

Volume 12 Issue 3

March 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 3 March 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*

### **Dorota 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: Texture Classification using Angular and Radial Bins in Transformed Domain

*Authors: Arun Kulkarni, Aavash Sthapit, Ashim Sedhain, Bishrut Bhattarai, Saurav Panthee*

**PAGE 1 – 4**

Paper 2: Intellectual Singularity of Quasi-Holographic Paradigm for a Brain-like Video-Component of Artificial Mind

*Authors: Yarichin E.M, Gruznov V.M, Yarichina G.F*

**PAGE 5 – 22**

Paper 3: Adopting Vulnerability Principle as the Panacea for Security Policy Monitoring

*Authors: Prosper K. Yeng, Stephen D. Wolthusen, Bian Yang*

**PAGE 23 – 30**

Paper 4: Feeder Reconfiguration in Unbalanced Distribution System with Wind and Solar Generation using Ant Lion Optimization

*Authors: Surender Reddy Salkuti*

**PAGE 31 – 39**

Paper 5: Determinants of e-Commerce Use at Different Educational Levels: Empirical Evidence from Turkey

*Authors: Şeyda Ünver, Ömer Alkan*

**PAGE 40 – 49**

Paper 6: Fuzzy based Techniques for Handling Missing Values

*Authors: Malak El-Bakry, Farid Ali, Ayman El-Kilany, Sherif Mazen*

**PAGE 50 – 55**

Paper 7: Change Detection Method with Multi-temporal Satellite Images based on Wavelet Decomposition and Tiling

*Authors: Kohei Arai*

**PAGE 56 – 61**

Paper 8: Comprehensive Analysis of Resource Allocation and Service Placement in Fog and Cloud Computing

*Authors: A.S. Gowri, P.Shanthi Bala, Immanuel Zion Ramdinthara*

**PAGE 62 – 79**

Paper 9: Performance Analysis of Deep Neural Network based on Transfer Learning for Pet Classification

*Authors: Bhavesh Jaiswal, Nagendra Gajjar*

**PAGE 80 – 85**

Paper 10: Multi-objective based Optimal Network Reconfiguration using Crow Search Algorithm

*Authors: Surender Reddy Salkuti*

**PAGE 86 – 95**

Paper 11: Applying Synthetic Minority Over-sampling Technique and Support Vector Machine to Develop a Classifier for Parkinson's disease

*Authors: Haewon Byeon, Byungsoo Kim*

**PAGE 96 – 101**

Paper 12: FishDeTec: A Fish Identification Application using Image Recognition Approach

*Authors: Siti Nurulain Mohd Rum, Fariz Az Zuhri Nawawi*

PAGE 102 – 106

Paper 13: Predicting the Anxiety of Patients with Alzheimer's Dementia using Boosting Algorithm and Data-Level Approach

*Authors: Haewon Byeon*

PAGE 107 – 113

Paper 14: Deep Learning Hybrid with Binary Dragonfly Feature Selection for the Wisconsin Breast Cancer Dataset

*Authors: Marian Mamdouh Ibrahim, Dina Ahmed Salem, Rania Ahmed Abdel Azeem Abul Seoud*

PAGE 114 – 122

Paper 15: Using Machine Learning Technologies to Classify and Predict Heart Disease

*Authors: Mohammed F. Alrifai, Zakir Hussain Ahmed, Asaad Shakir Hameed, Modhi Lafta Mutar*

PAGE 123 – 127

Paper 16: Towards Natural Language Processing with Figures of Speech in Hindi Poetry

*Authors: Milind Kumar Audichya, Jatinderkumar R. Saini*

PAGE 128 – 133

Paper 17: Formal Verification of an Efficient Architecture to Enhance the Security in IoT

*Authors: Eman K. Elsayed, L. S. Diab, Asmaa. A. Ibrahim*

PAGE 134 – 139

Paper 18: Conceptual Model with Built-in Process Mining

*Authors: Sabah Al-Fedaghi*

PAGE 140 – 149

Paper 19: Modeling a Functional Engine for the Opinion Mining as a Service using Compounded Score Computation and Machine Learning

*Authors: Rajeshwari D, Puttegowda. D*

PAGE 150 – 155

Paper 20: Model for Predicting Customer Desertion of Telephony Service using Machine Learning

*Authors: Carlos Acero-Charaña, Ebert Osco-Mamani, Tito Ale-Nieto*

PAGE 156 – 164

Paper 21: Evaluating Software Quality Attributes using Analytic Hierarchy Process (AHP)

*Authors: Botchway Ivy Belinda, Akinwonmi Akintoba Emmanuel, Nunoo Solomon, Alese Boniface Kayode*

PAGE 165 – 173

Paper 22: SVM Machine Learning Classifier to Automate the Extraction of SRS Elements

*Authors: Ayad Tareq Imam, Aysh Alhroob, Wael Jumah Alzyadat*

PAGE 174 – 185

Paper 23: Artificial Intelligence: Machine Translation Accuracy in Translating French-Indonesian Culinary Texts

*Authors: Muhammad Hasyim, Firman Saleh, Rudy Yusuf, Asriani Abbas*

PAGE 186 – 191

**Paper 24: A Generic Approach for Allocating Movement Permits During/Outside Curfew Period during COVID-19**

*Authors: Yaser Chaaban*

**PAGE 192 – 200**

**Paper 25: Internet of Things Security: A Review of Enabled Application Challenges and Solutions**

*Authors: Mona Algarni, Munirah Alkhelaiwi, Abdelrahman Karrar*

**PAGE 201 – 215**

**Paper 26: Customer Retention: Detecting Churners in Telecoms Industry using Data Mining Techniques**

*Authors: Mahmoud Ewieda, Essam M Shaaban, Mohamed Roushdy*

**PAGE 216 – 224**

**Paper 27: Speech-to-Text Conversion in Indonesian Language Using a Deep Bidirectional Long Short-Term Memory Algorithm**

*Authors: Suci Dwijayanti, Muhammad Abid Tami, Bhakti Yudho Suprpto*

**PAGE 225 – 230**

**Paper 28: Smart Internet of Vehicles Architecture based on Deep Learning for Occlusion Detection**

*Authors: Shaya A. Alshaya*

**PAGE 231 – 236**

**Paper 29: Smart Home Energy Management System**

*Authors: Yasser AL Sultan, Ben Salma Sami, Bassam A. Zafar*

**PAGE 237 – 244**

**Paper 30: Trade-off between Energy Consumption and Transmission Rate in Mobile Ad-Hoc Network**

*Authors: Ashraf Al Sharah, Mohammad Alhaj, Firas Al Naimat*

**PAGE 245 – 252**

**Paper 31: Real-Time Intelligent Thermal Comfort Prediction Model**

*Authors: Farid Ali Mousa, Heba Hamdy Ali*

**PAGE 253 – 258**

**Paper 32: Potential Data Collections Methods for System Dynamics Modelling: A Brief Overview**

*Authors: Aisyah Ibrahim, Hamdan Daniyal, Tuty Asmawaty Abdul Kadir, Adzhar Kamaludin*

**PAGE 259 – 268**

**Paper 33: Novel Modelling of the Hash-based Authentication of Data in Dynamic Cloud Environment**

*Authors: Anil Kumar G, Shantala C.P*

**PAGE 269 – 275**

**Paper 34: Cybersecurity Awareness Level: The Case of Saudi Arabia University Students**

*Authors: Wejdan Aljohni, Nazar Elfadil, Mutsam Jarajreh, Mwahib Gasmelsied*

**PAGE 276 – 281**

**Paper 35: Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things**

*Authors: Monika Parmar, Harsimran Jit Kaur*

**PAGE 282 – 289**

**Paper 36: Proof-of-Review: A Review based Consensus Protocol for Blockchain Application**

*Authors: Dodo Khan, Low Tang Jung, Manzoor Ahmed Hashmani*

**PAGE 290 – 300**

**Paper 37: Movement Control of Smart Mosque's Domes using CSRNet and Fuzzy Logic Techniques**

*Authors: Anas H. Blasi, Mohammad Awis Al Lababede, Mohammed A. Alsuwaikef*

**PAGE 301 – 308**

**Paper 38: Correlating Crime and Social Media: Using Semantic Sentiment Analysis**

*Authors: Rhea Mahajan, Vibhakar Mansotra*

**PAGE 309 – 316**

**Paper 39: A Hybrid Model for Documents Representation**

*Authors: Dina Mohamed, Ayman El-Kilany, Hoda M. O. Mokhtar*

**PAGE 317 – 324**

**Paper 40: Predicting Internet Banking Effectiveness using Artificial Model**

*Authors: Ala Aldeen Al-Janabi*

**PAGE 325 – 332**

**Paper 41: Developing a Framework for Data Communication in a Wireless Network using Machine Learning Technique**

*Authors: Somya Khidir Mohmmmed Ataelmanan, Mostafa Ahmed Hassan Ali*

**PAGE 333 – 342**

**Paper 42: Floating Content: Experiences and Future Directions**

*Authors: Shahzad Ali*

**PAGE 343 – 346**

**Paper 43: A Collision-aware MAC Protocol for Efficient Performance in Wireless Sensor Networks**

*Authors: Hamid Hajaje, Mounib Khanafer, Zine El Abidine Guennoun, Junaid Israr, Mouhcine Guennoun*

**PAGE 347 – 363**

**Paper 44: Distinctive Context Sensitive and Hellinger Convolutional Learning for Privacy Preserving of Big Healthcare Data**

*Authors: Sujatha K, Udayarani V*

**PAGE 364 – 372**

**Paper 45: Big Data Analytics Framework for Childhood Infectious Disease Surveillance and Response System using Modified MapReduce Algorithm**

*Authors: Mdoe Mwamnyange, Edith Luhanga, Sanket R. Thodje*

**PAGE 373 – 385**

**Paper 46: Recognizing Human Emotions from Eyes and Surrounding Features: A Deep Learning Approach**

*Authors: Md. Nymur Rahman Shuvo, Shamima Akter, Md. Ashiqul Islam, Shazid Hasan, Muhammad Shamsojjaman, Tania Khatun*

**PAGE 386 – 394**

**Paper 47: Novel Data Oriented Structure Learning Approach for the Diabetes Analysis**

*Authors: Adel THALJAOU*

**PAGE 395 – 402**

**Paper 48: Optimal Routing based Load Balanced Congestion Control using MAODV in WANET Environment**

*Authors: Kanthimathi S, JhansiRani P*

**PAGE 403 – 411**

**Paper 49: Smart Digital Forensic Framework for Crime Analysis and Prediction using AutoML**

*Authors: Sajith A Johnson, S Ananthakumaran*

**PAGE 412 – 420**

**Paper 50: Multi-level Protection (Mlp) Policy Implementation using Graph Database**

*Authors: Lingala Thirupathi, Venkata Nageswara Rao Padmanabhuni*

**PAGE 421 – 429**

**Paper 51: SGBBA: An Efficient Method for Prediction System in Machine Learning using Imbalance Dataset**

*Authors: Saiful Islam, Umme Sara, Abu Kawsar, Anichur Rahman, Dipanjali Kundu, Diganta Das Dipta, A.N.M. Rezaul Karim, Mahedi Hasan*

**PAGE 430 – 441**

**Paper 52: An Improved Multi-label Classifier Chain Method for Automated Text Classification**

*Authors: Adeleke Abdullahi, Noor Azah Samsudin, Shamsul Kamal Ahmad Khalid, Zuhaila Ali Othman*

**PAGE 442 – 449**

**Paper 53: Efficient Task Scheduling in Cloud Computing using Multi-objective Hybrid Ant Colony Optimization Algorithm for Energy Efficiency**

*Authors: Fatima Umar Zambuk, Abdulsalam Ya'u Gital, Mohammed Jiya, Nahuru Ado Sabon Gari, Badamasi Ja'afaru, Aliyu Muhammad*

**PAGE 450 – 456**

**Paper 54: Motor Insurance Claim Status Prediction using Machine Learning Techniques**

*Authors: Endalew Alamir, Teklu Urgessa, Ashebir Hunegnaw, Tiruveedula Gopikrishna*

**PAGE 457 – 463**

**Paper 55: Detecting Malware based on Analyzing Abnormal behaviors of PE File**

*Authors: Lai Van Duong, Cho Do Xuan*

**PAGE 464 – 471**

**Paper 56: Efficient and Secure Group based Collusion Resistant Public Auditing Scheme for Cloud Storage**

*Authors: Smita Chaudhari, Gandharba Swain*

**PAGE 472 – 481**

**Paper 57: Fog Network Area Management Model for Managing Fog-cloud Resources in IoT Environment**

*Authors: Anwar Alghamdi, Ahmed Alzahrani, Vijey Thayanathan*

**PAGE 482 – 489**

**Paper 58: Automata-based Algorithm for Multiple Word Matching**

*Authors: Majed AbuSafiya*

**PAGE 490 – 494**

**Paper 59: Question Answering Systems: A Systematic Literature Review**

*Authors: Sarah Saad Alanazi, Nazar Elfadil, Mutsam Jarajreh, Saad Algarni*

**PAGE 495 – 502**

**Paper 60: Comprehensive Analysis of Flow Incorporated Neural Network based Lightweight Video Compression Architecture**

*Authors: Sangeeta, Preeti Gulia, Nasib Singh Gill*

**PAGE 503 – 508**

**Paper 61: Empirical Study on Microsoft Malware Classification**

*Authors: Rohit Chivukula, Mohan Vamsi Sajja, T. Jaya Lakshmi, Muddana Harini*

**PAGE 509 – 515**

**Paper 62: Smart Intersection Design for Traffic, Pedestrian and Emergency Transit Clearance using Fuzzy Inference System**

*Authors: Aditi Agrawal, Rajeev Paulus*

**PAGE 516 – 522**

**Paper 63: Computer Research Project Management**

*Authors: Lassad Mejri, Henda Hajjami Ben Ghezala, Raja Hanafi*

**PAGE 523 – 535**

**Paper 64: Clustering of Association Rules for Big Datasets using Hadoop MapReduce**

*Authors: Salahadin A. Moahmmed, Mohamed A. Alasow, El-Sayed M. El-Alfy*

**PAGE 536 – 545**

**Paper 65: Recent Advancement in Speech Recognition for Bangla: A Survey**

*Authors: Sadia Sultana, M. Shahidur Rahman, M. Zafar Iqbal*

**PAGE 546 – 552**

**Paper 66: Intrusion Detection using Deep Learning Long Short-term Memory with Wrapper Feature Selection Method**

*Authors: Sana Al Azwari, Hamza Turabieh*

**PAGE 553 – 558**

**Paper 67: Evaluation of Collaborative Filtering for Recommender Systems**

*Authors: Maryam Al-Ghamdi, Hanan Elazhary, Aalaa Mojahed*

**PAGE 559 – 565**

**Paper 68: Deployment and Migration of Virtualized Services with Joint Optimization of Backhaul Bandwidth and Load Balancing in Mobile Edge-Cloud Environments**

*Authors: Tarik Chanyour, Mohammed Oucamah Cherkaoui Malki*

**PAGE 566 – 576**

**Paper 69: Zero-resource Multi-dialectal Arabic Natural Language Understanding**

*Authors: Muhammad Khalifa, Hesham Hassan, Aly Fahmy*

**PAGE 577 – 591**

**Paper 70: Distributed Mining of High Utility Sequential Patterns with Negative Item Values**

*Authors: Manoj Varma, Saleti Sumalatha, Akhileshwar Reddy*

**PAGE 592 – 598**

**Paper 71: Deep Neural Network-based Relationship Identification Framework to Discriminate Fake Profile Over Social Media**

*Authors: Suneet Joshi, Deepak Singh Tomar*

**PAGE 599 – 611**

**Paper 72: A Parameter-free Clustering Algorithm based K-means**

*Authors: Said Slaoui, Zineb Dafir*

**PAGE 612 – 619**

**Paper 73: Arabic Tweets Sentiment Analysis about Online Learning during COVID-19 in Saudi Arabia**

*Authors: Asma Althagafi, Ghofran Althobaiti, Hosam Alhakami, Tahani Alsubait*

**PAGE 620 – 625**

**Paper 74: A Framework for Data Research in GIS Database using Meshing Techniques and the Map-Reduce Algorithm**

*Authors: Abdoulaye SERE, Jean Serge Dimitri OUATTARA, Didier BASSOLE, Jose Arthur OUEDRAOGO, Moubaric KABORE*

**PAGE 626 – 635**

**Paper 75: Pitch Contour Stylization by Marking Voice Intonation**

*Authors: Sakshi Pandey, Amit Banerjee, Subramaniam Khedika*

**PAGE 636 – 645**

**Paper 76: A Multi-purpose Data Pre-processing Framework using Machine Learning for Enterprise Data Models**

*Authors: Venkata Ramana B, Narsimha G*

**PAGE 646 – 656**

**Paper 77: Deep Attention on Measurable and Behavioral-driven Complete Service Composition Design Process**

*Authors: Ilyass El Kassmi, Radia Belkeziz, Zahi Jarir*

**PAGE 657 – 670**

**Paper 78: Concatenative Speech Recognition using Morphemes**

*Authors: Afshan Jafri*

**PAGE 671 – 680**

**Paper 79: Multiclass Vehicle Classification Across Different Environments**

*Authors: Aisha S. Azim, Afshan Jafri, Ashraf Alkhairy*

**PAGE 681 – 691**

**Paper 80: Arabic Sign Language Recognition using Faster R-CNN**

*Authors: Rahaf Abdulaziz Alawwad, Ouiem Bchir, Mohamed Maher Ben Ismail*

**PAGE 692 – 700**

**Paper 81: Attack Resilient Trust and Signature-based Intrusion Detection Systems**

*Authors: Boniface Kabaso, Saber A. Aradeh, Ademola P. Abidoye*

**PAGE 701 – 707**

**Paper 82: Factors Influencing the Use of Wireless Sensor Networks in the Irrigation Field**

*Authors: Loubna HAMAMI, Bouchaib NASSEREDDINE*

**PAGE 708 – 717**

**Paper 83: Deep Learning Algorithm for Classification of Cerebral Palsy from Functional Magnetic Resonance Imaging (fMRI)**

*Authors: Pradeepa Palraj, Gopinath Siddan*

**PAGE 718 – 724**

# Texture Classification using Angular and Radial Bins in Transformed Domain

Arun Kulkarni<sup>1</sup>, Aavash Sthapit<sup>2</sup>, Ashim Sedhain<sup>3</sup>, Bishrut Bhattarai<sup>4</sup>, Saurav Panthee<sup>5</sup>  
Computer Science Department, The University of Texas at Tyler  
TX 75799, USA

**Abstract**—Texture is generally recognized as fundamental to perceptions. There is no precise definition or characterization available in practice. Texture recognition has many applications in areas such as medical image analysis, remote sensing, and robotic vision. Various approaches such as statistical, structural, and spectral have been suggested in the literature. In this paper we propose a method for texture feature extraction. We transform the image into a two-dimensional Discrete Cosine Transform (DCT) and extract features using the ring and wedge bins in the DCT plane. These features are based on texture properties such as coarseness, smoothness, graininess, and directivity of the texture pattern in the image. We develop a model to classify texture images using extracted features. We use three classifiers: the Decision Tree, Support Vector Machine (SVM), and Logarithmic Regression (LR). To test our approach, we use Brodatz texture image data set consisting of 111 images of different texture patterns. Classification results such as accuracy and F-score obtained from the three classifiers are presented in the paper.

**Keywords**—Texture; discrete cosine transform; radial and angular bins; decision tree; support vector machine; logarithmic regression

## I. INTRODUCTION

Texture is generally recognized as being fundamental to perception. Texture provides useful information in identifying objects in images. Texture is different from color. Texture is defined as something composed of closely interwoven elements [1]. The description of interwoven elements leads to the idea of texture resolution. Texture primitives may be pixels or aggregate of pixels such as regions. It refers to the spatial organization of basic elements or primitives [2]. Many texture images do not have geometrical regularity of texture primitives in the image, but they can be described by statistical models. Texture recognition has many applications in areas such as medical image analysis, remote sensing, and robotic vision. There is no precise definition of texture available in practice. Texture has been described in a variety of ways. Texture descriptors provide measures of properties such as smoothness, coarseness, and regularity [3]. Gonzalez and Woods [4] describe three principal approaches for texture analysis: statistical, structural, and spectral. Statistical approaches yield texture properties such as smoothness, coarseness, or graininess. Structural approaches are based on arrangement of primitive shapes in the image. Spectral properties are found on the Fourier spectrum and they yield global periodicity in the image or a region of the image. In this paper, we propose a new algorithm for extracting texture

features from the two-dimensional Discrete Cosine Transform (DCT) of the image. These features capture directional and coarseness properties of the texture. We classify texture images using these features with statistical models. The texture recognition plays an important role in computer vision and has many practical applications such as robotics, reconnaissance, and biometrics. We have used three classifiers Support Vector Machine (SVM), Decision Tree (DT), and Logarithmic Regression (LR). We can also use a neural network with a backpropagation learning algorithm as a classifier. The main advantage of the proposed algorithm is that it can be incorporated in layers of a Convolution Neural Network (CNN).

The outline of the paper is as follows. Section II describes related work and provides historical developments in texture recognition. Section III provides the proposed approach. Section IV illustrates the experimental work and the results, and Section V provides conclusions.

## II. RELATED WORK

Picture analysis involves representation, classification, segmentation, and synthesis. Many texture feature extraction algorithms are available in practice. Haralick et al. [5] proposed Gray Level Cooccurrence Matrix (GLCM) for extracting texture features. They suggested twenty-eight features that are best on GLCM. The most frequently used features are energy, entropy, inertia, and local homogeneity. Wilson and Bergen [6] developed a model for texture segmentation using Difference-of-Gaussian (DOG) filters. O'Toole and Stark [7] suggested a method for texture feature extraction using the Hotelling Trace (HT). Many spatial frequency filtering techniques have been used for texture segmentation. Bajesy and Lieberman [8] used spectrograms for texture segmentation. Coggins and Jain [9] used radial and angular bins in the Frequency Domain (FD) for extracting texture features. Daugman [10] used 2-D Gabor filters for texture segmentation. Kulkarni and Byers [11] used radial and angular bins in 2-D frequency domain. They employed the Radon transform to calculate the Fourier coefficients. Tuceryan and Jain [12] identified five major categories of texture features: statistical, geometrical, structural, model based, and filtering based. Lows [13] used local invariant descriptors using Fourier Transform (FT) for texture analysis. Zeng et al. [14] categorized texture representation into three broad types: Bag-of-Words (BoW), Convolution Neural Network (CNN)-based, and attribute based. In the BoW approach a feature vector is obtained from a texture image that represents properties of the texture. In this approach the

texture image is first transformed into a pool of local features. Many CNN-based texture presentation models have been proposed in recent years [15, 16, 17].

### III. PROPOSED APPROACH

In our proposed approach we use ring and wedge bins to extract texture features in the DCT domain. The DCT coefficients are given by (1).

$$F_{pq} = a_p a_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N}$$

where

$$a_p = \begin{cases} \frac{1}{\sqrt{M}}, & p=0 \\ \sqrt{\frac{2}{M}}, & 1 \leq p \leq M-1 \end{cases} \quad \text{and} \quad a_q = \begin{cases} \frac{1}{\sqrt{N}}, & q=0 \\ \sqrt{\frac{2}{N}}, & 1 \leq q \leq N-1 \end{cases} \quad (1)$$

We use the DCT coefficients because FT coefficients have real and imaginary parts. We can achieve data compression with the DCT as most information is stored in a few DCT coefficients at the top left corner in the DCT matrix. As we go away from the origin (0,0) the DCT coefficient values gradually become smaller. Most images in practice exhibit statistical redundancy. Therefore, it is possible to reconstruct the original image with a few DCT coefficients without affecting the visual quality of the images. It can be seen from Fig. 1 that if we rotate the image, the DCT also rotates. In Fig. 1, the texture image is rotated 45 degrees and it can be observed that the corresponding DCT also rotates by 45 degrees. Images with high spatial frequency contents show more spread of the DCT coefficients. In Fig. 2, the image in the second row shows relatively more coarseness. The DCT coefficients are more spread out for that image. Texture images with low spatial frequency contents show DCT coefficients concentration near the origin. The angular and radial bins are shown in Fig. 3. We can extract directional properties of the texture using the angular bins. The radial bins capture coarseness of the texture images. Radial and angular features are given by (2) and (3), respectively.

$$V_{r_1 r_2} = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} F_{uv}$$

$$r_1^2 \leq u^2 + v^2 < r_2^2 \quad (2)$$

$$V_{\phi_1 \phi_2} = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} F_{uv}$$

$$\phi_1 \leq \tan^{-1} \left( \frac{v}{u} \right) < \phi_2 \quad (3)$$

We used three classifiers to categorize texture images from extracted feature vectors: a) Decision Tree classifier, b) Support Vector Machine (SVM), and c) Logarithmic Regression model. SVM was proposed by Cortes and Vapnik [18]. In the SVM model, two hyper-planes are selected to maximize the distance between the two classes and not to include any points between them. The SVM algorithm is extended to non-linearly separable classes by mapping samples to a higher dimensional feature space [19]. SVM was

chosen as one of the classification methods because it has been shown to successfully handle small datasets in comparison to other traditional methods [20]. Moreover, it has good theoretical foundations, and generalization capacity as its decision functions are determined directly from the training data so that decision borders' margins are maximized in a highly dimensional feature space leading to less classification errors [21]. Decision Tree implementation using ID3 algorithm was suggested by Quinlan [22]. The algorithm uses information gain to decide as to which attribute is the best for the split at each non-terminal node. It is a recursive algorithm that starts with the root node and the leaf nodes represent the classes. C4.5 algorithm is an extension of ID3 algorithm, and it allows usage of both discrete and continuous variables. Logarithmic Regression can be implemented as shown in (4).

$$y = \frac{e^{(b_0+b_1)}}{1 + e^{(b_0+b_1)}} \quad (4)$$

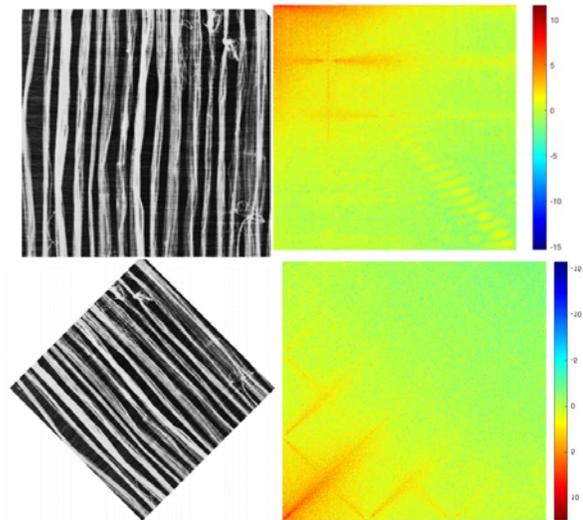


Fig. 1. DCT Visualization on Rotated Images.

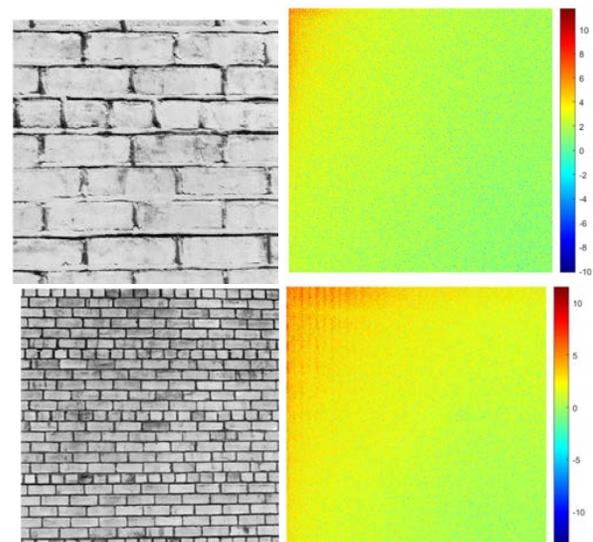


Fig. 2. DCT Visualization of Coarse Features.

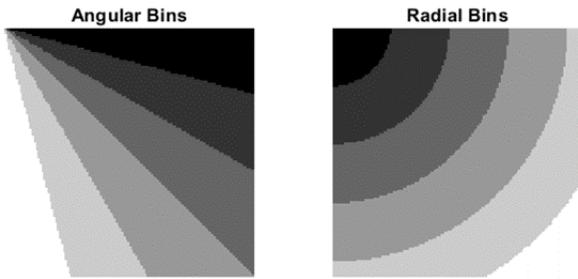


Fig. 3. Angular and Radial Bins.

where,  $y$  is the predicted output and  $b_0$  and  $b_1$  are coefficients that are estimated using training set data. The model predicts the probability of a default class [23].

#### IV. EXPERIMENT AND RESULTS

To test our approach, we used Brodatz texture image data set consisting of 111 images of different texture patterns [24]. In the pre-processing stage, we grouped texture images in the Brodatz data set into five categories using K-means clustering algorithm. Sample images from each cluster are shown in Fig. 4. All the images were first resized to the dimension of  $256 \times 256$  pixels. The Discrete Cosine Transform (DCT) has been widely used to convert an image from its spatial domain to its frequency domain where we can reduce digital image storage size, expedite data transmission, and remove redundant information [25]. We used the DCT coefficients of each image to extract information from its frequency domain. Most of the information in the image is concentrated in a few coefficients that are in the top left corner of the DCT matrix. We used the top left  $128 \times 128$  region of the DCT matrix for feature extraction. The values of DCT coefficients were normalized. Furthermore, all the DCT coefficients that were less than zero were made zero as those values were very small. We normalized feature values between 0 and 5 so that all features are treated equally [26]. We extracted 34 features from the DCT coefficients. These features represent 6 wedge features, 4 ring features, and 24 features from the top left-hand corner. We have chosen 24 features from the top left corner as they showed the maximum variance and contained most information. The DCT coefficient at (0,0) was dropped because its normalized values were the same for all images. The 3-D scatter plot for five categories is shown in Fig. 5. Mean values of features are shown in Fig. 6 and Fig. 7 shows the decision tree. The results are shown in Table I.

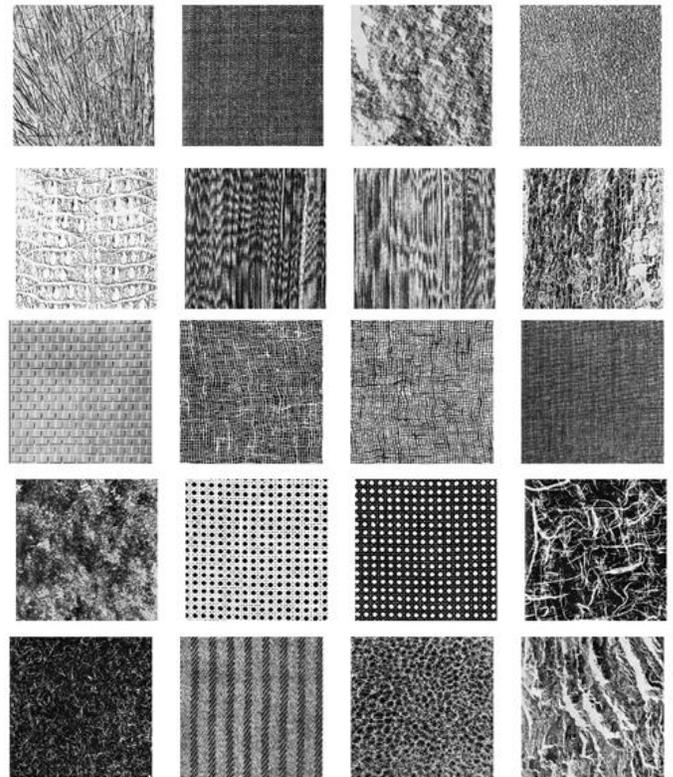


Fig. 4. Sample Images from Five Categories.

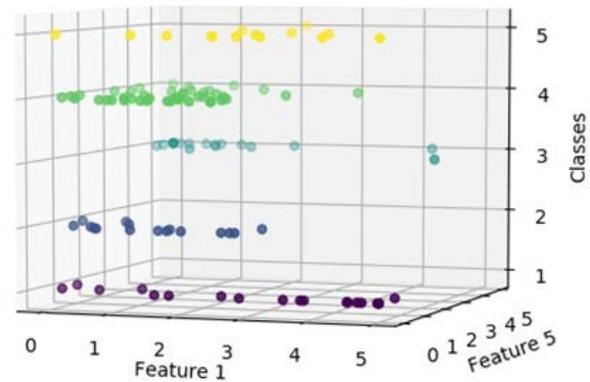


Fig. 5. 3-D Scatter Plot.

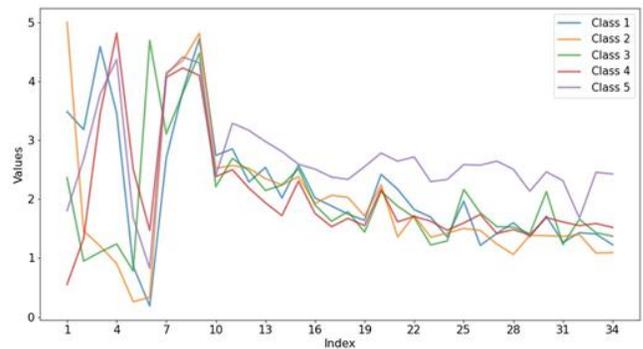


Fig. 6. Class Signatures.

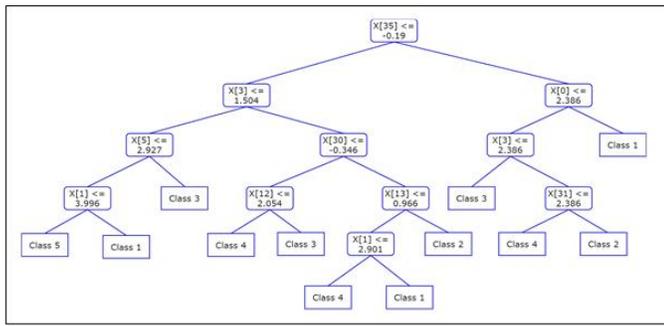


Fig. 7. Decision Tree.

TABLE I. ACCURACY AND F-SCORE

Classifier	Accuracy Score Percentage	F1 Score
Support Vector Machine	82.3	0.798
Decision Tree	79.4	0.753
Logarithmic Regression	91.1	0.919

### V. CONCLUSIONS

In this paper we have proposed a method for feature extraction using properties such as coarseness, smoothness, graininess, and directivity of the texture pattern in the image using DCT coefficients. These features can be used for texture image classification and analysis. We considered 34 features. We trained three classifiers using extracted features: a Decision Tree, Support Vector Machine, and a Logarithmic Regression classifier. It can be seen from Table I that the Logarithmic Regression classifier performed very well for this data set compared to the decision tree and support vector machine. The classification accuracy obtained with Logarithmic Regression classifier was 91.1 percent. Decision trees usually perform better with discrete features. The results obtained with our approach suggest that it is a valuable method for feature extraction and classification of texture images. The results may be further improved by using a greater number of radial and angular bin features. Also, we considered five categories of clusters. By using the optimized number clusters in pre-processing and proper grouping of images classification results may be improved.

In the future, we would like to evaluate the method with large datasets containing many images with a greater number of ring and wedge bin features. Furthermore, the feature extraction algorithm with angular and radial bins combining with a multi-layer perceptron model for classification, we plan to develop an architecture for a convolution neural network (CNN) model for classification of texture images.

### REFERENCES

[1] D.A Ballard, and C.M. Brown, Computer Vision. Englewood Cliffs, NJ,USA: Prentice-Hall. 1982.  
 [2] B. Julesz, "Textons, the elements of texture perception, and their interactions." Nature vol. 290, pp. 91-97 1981.  
 [3] A.D. Kulkarni, Computer Vision and Fuzzy-Neural Systems. Upper Saddle, Prentice Hall PTR, 2001.

[4] R.C. Gonzalez & R.E. Woods, Digital Image Processing, Reading, MA, Addison-Wesley, 1992.  
 [5] R. M. Haralick R. M., K. Shanmugam, and I. Dinstein. Texture features for image classification. IEEE Transactions on System, Man and Cybernetics, vol. 3, pp. 610-620, 1973.  
 [6] H. R. Wilson and J. R. Bergen, "A four mechanism model for threshold spatial vision," Vision Research, 1979.  
 [7] R. K. O'Toole and H. Stark, "Comparative study of optical-digital vs all-digital techniques in textural pattern recognition," Appl. Opt. vol. 19, pp. 2496-2506, 1980.  
 [8] R. Bajesy and L. Lieberman, "Texture gradient as a depth cue", Comput. Graphics Image Processing, vol. 5, pp. 52-67, 1976.  
 [9] M. Coggins and A.K. Jain, "A Spatial Filtering Approach to Texture Analysis", Pattern Recognition Letters, vol. 3, pp. 195-203, 1985.  
 [10] J. G. Daugman, "Complete discrete 2-D Gabor transforms by neural networks for image analysis and compression," IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 36, no. 7, pp. 1169-1179, 1988.  
 [11] A.D. Kulkarni, and P. Byars, "Artificial neural network models for texture classification via the Radon transform". Proceedings of Symposium on Applied Computing, Kansas City, vol. II, pp 659-664. 1992.  
 [12] M. Tuceryan and A.K. Jain, "Texture Analysis", Handbook Pattern Recognition and Computer Vision, pp. 235-276, 1993.  
 [13] D.G Lowe, "Distinctive Image Features from Scale-Invariant Keypoints", Pattern Recognition, vol. 17, no. 2, pp. 111-122, 2004.  
 [14] Zeng, M. Liu, X. Fu, R. Gu and L. Leng, "Curvature Bag of Words Model for Shape Recognition," IEEE Access, vol. 7, pp. 57163-57171, 2019.  
 [15] A. Krizhevsky, I. Sutskever and G.E. Hinton, "ImageNet Classification with Deep Convolutional Neural Network", Advances in Neural Information Processing Systems, 2012.  
 [16] J. Bruma, and S. Mallat "Invariant Scattering Convolution Networks", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 8, pp 1872-1885, 2013.  
 [17] X. Dai, J. Y.-H. Ng, and L. S. Davis, "FASON: First and second order information fusion Network for texture recognition." CVPR, pp. 7352-7360, 2017.  
 [18] C. Cortes, and V. Vapnik, "Support-vector networks". Machine Learning vol. 20, pp. 273-297, 1995.  
 [19] A. D Kulkarni, and A. Shrestha, "Multispectral image analysis using Decision Trees" International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, pp 111-18, 2017.  
 [20] P. Mantero, G. Moser, and S. B. Serpico, "Partially supervised classification of remote sensing images through SVM-based probability density estimation," IEEE Transactions on Geoscience and Remote Sensing, vol. 43, no. 3, pp. 559-570, 2005.  
 [21] J. Cervantes, et al. "A Comprehensive Survey on Support Vector Machine Classification: Applications, Challenges and Trends." Neurocomputing, vol. 408, pp. 189-215, 2020.  
 [22] J.R. Quinlan "Induction of decision trees." Machine Learning vol. 1, pp. 81-106, 1986.  
 [23] K. Benoit "Linear Regression Models with Logarithmic Transformations", 2011. [https://kenbenoit.net/assets/courses/ME104/log\\_models2.pdf](https://kenbenoit.net/assets/courses/ME104/log_models2.pdf).  
 [24] P. Brodatz, "Textures: A Photographic Album for Artists and Designers" Dover Publications, 1966.  
 [25] Y.H. Tsai, S. Wang, M.H. Yang: "SegFlow: Joint learning for video object segmentation and optical flow.," IEEE International Conference on Computer Vision, pp. 686-695, 2017.  
 [26] J. Sola and J. Sevilla, "Importance of input data normalization for the application of neural networks to complex industrial problems," IEEE Transactions on Nuclear Science, vol. 44, no. 3, pp. 1464-1468, 1997.

# Intellectual Singularity of Quasi-Holographic Paradigm for a Brain-like Video-Component of Artificial Mind

Yarichin E.M<sup>1</sup>

Brain-like Technology Laboratory  
(NeocorTek Lab)  
Krasnoyarsk  
Russia

Gruznov V.M<sup>2</sup>

Trofimuk Institute of Petroleum  
Geology and Geophysics, Siberian  
Branch of Russian Academy of  
Sciences, Novosibirsk, Russia

Yarichina G.F<sup>3</sup>

Institute for Business Processes and  
Economic Management  
Siberian Federal University  
SFU, Krasnoyarsk, Russia

**Abstract**—On the basis of a new post-Shannon information approach (quantitative and qualitative together), a hierarchical process of evaluating video-information by an intellectual brain-like video-component of artificial mind is considered. The development of the classical (Shannon's) informational approach to the level of the new (post-Shannon's) informational approach made it possible to formulate an important additional “bonus” in the form of a differential holographic principle (DHP). DHP made it possible to present video information on a dualistic basis, considering its physical and structural components, considered together. Developed an integral quasi-holographic principle (IQHP) is built on the basis of the DHP. However, in contrast to the DHP this principle represents a supra-physical (abstract) principle, uses a long-range action template and is realized instantly (i.e. with an infinitely high speed). In a joint tandem of physical (quantitative) and structural (qualitative) components of video-information evaluation, the structural component is dominant. Due to this, the technology of the video-component of artificial mind based on IQHP always takes the form of an ascending hierarchy of structured (abstract) evaluations of video-information. This technology also includes a hierarchy of self-learning stages, thanks to which the constant development of macro-objects of video-information in the form of video-thesauruses as high-quality measuring scales is carried out. This maintains the relevance, efficiency, and instantaneousness of the video-component of the artificial mind in evaluation video-information. Based on the ideas and principles of a new (post-Shannon) information approach to evaluation video-information, the structural and functional architecture of the video-component of artificial mind built. This architecture is not biologically inspired, but it turned out to be surprisingly exactly coinciding with the known structure of the human neocortex (by the number of levels of the ascending hierarchy, by the presence of a hierarchy in direct and feedback, by the method of structuring and collecting input elementary video-data, etc.). A new theorem for a complete sample of video-data, considered together in physical and structural form, is formulated. The direct version of this theorem corresponds to an ascending hierarchy of video-information evaluations based on IQHP and bundles of video-information's evaluations. The inverse version characterizes the global hierarchical feedback, which takes the form of a descending hierarchy of “service” video-information evaluations.

**Keywords**—*Differential holographic principle; video-data; structuring; super-saccades; integral quasi-holographic principle;*

*long-range action; bundles; ascending hierarchy; singularity; video-component; video-thesaurus; video-intelligence; architecture; artificial intelligence; artificial mind; full sampling theorem; descending hierarchy; hierarchical feedback*

## I. INTRODUCTION

The progress of intelligent technologies is based on the evolution of the processes of recognition, perception and understanding of the surrounding material World, ideas about which are formed by joint quantitative (physical) and qualitative (structural) evaluations of the diverse information content of the surrounding World. All this is inextricably linked with the achieved depth of human awareness of the nature of the information of the material World, which in the general case is characterized by strong nonlinearity, and because of this, lack of clarity and non-obvious. In this regard, researchers are tempted to replace the solution of complex nonlinear problems of information analysis and intellectual synthesis of “mental” evaluations of information with a variety of intuitive and heuristic approaches. They are a significant (sometimes fatal) simplification of reality, but at the same time they are often proclaimed the only correct means of its reflection. Generally speaking, the term mental, accepted and widely used in psychology, refers to mental images and processes in a person. Therefore, in machine psychology of artificial mind, to maintain continuity, we will use the same term, but in quotation marks. This means that the considered structure, functions, mental images and processes of artificial mind can be compared with analogous mental processes in humans, but refer they exclusively to machine psychology.

Intuitive and heuristic approaches (including the classical quantitative informational approach of K. Shannon and neural networks), generally speaking, no longer meet the requirements for modern intellectual technologies, introducing significant confusion and thereby limiting their scope. Currently, among the promising intelligent technologies, in the implementation of which human civilization is interested, include the technology of strong (human-like) artificial intelligence, which can be considered as a technology of weak artificial mind as well as technology of artificial superintelligence (superhuman artificial intelligence), which can be considered in the quality of the technology of strong artificial mind. For a meaningful construction of these technologies, a new information approach

to the technologies of artificial mind is required, which will be adequate to their complex "mental" nature. This will make it possible to consciously switch to the synthesis of not only individual specialized intelligent systems, but also multicomponent intelligent systems of artificial mind (weak and strong).

In the short term, the complete replacement of human natural intelligence with artificial mind in most areas of human society it is not yet conceptually and technologically feasible. As an affordable alternative, it is still possible to consider intelligent technologies based on neural networks, which allow emulating some simple ones the capabilities of human intelligence, for example, in the field of pattern recognition. However, modern technologies based on neural networks do not allow provide emulating the complex capabilities of human intelligence, such as understanding images. Without this, is impossible awareness of reaching a frightening threshold for the development of artificial intelligence, beyond which an acute antagonism of natural and artificial minds can begin, as well as the cataclysm following from this antagonism in the form of a technological singularity (of explosive acceleration of scientific and technological progress and the creation of a super mind as of hypothetical a danger to human civilization). Similar fears about mechanical machines have already occurred in the history of human society, which, nevertheless, was able to create a highly developed civilization using the achievements of machine mechanics.

It is now clear that technologies that are much more complex, sophisticated and abstract than the mechanical technologies of complex machines and mechanisms will be used for the development of human civilization. This process stretched out in time will lead to certain transformations in human society and the emergence of a new civilization, most likely of the information type, based on deep awareness of a new (post-Shannon) informational approach-analysis (quantitative and qualitative together) to the material World around. The natural development of this new informational approach is an intelligent informational approach-synthesis, which, with the help of a bottom-up hierarchical synthesis of the initial physical evaluation of weak information, allows to adequately restore the initial information as a whole. This process can be viewed as a "mental" representation of information from the surrounding material World in the "mental" space of the intellectual system of artificial mind (ISAM). This artificial (virtual) space is induced in the process of internal synthesis in the ISAM of the ascending hierarchy of information evaluations (quantitative and qualitative together) and is a necessary means for their formal mathematical "awareness" (recognition, perception and understanding) by artificial mind.

The existing pessimism regarding the solution of these complex problems at the present time is most likely due to:

- Incorrectness of intuitive and bio-inspired heuristic attempts (for example, based on neural networks) to solve the problem of artificial intelligence as the basis of artificial mind;
- Commercial haste in the development of the first productive, but still "raw" results in the field of artificial

intelligence, which were initially poorly understood and, generally speaking, are still largely not fully understood;

- Focusing not on the dominant, but on some secondary properties of artificial intelligence, in other words, not on the understanding of "strong" information, but on the recognition of "weak" information;
- Inadequate approaches to solving the problems of artificial intelligence.

Apparently because of this, many developers of artificial intelligence systems have developed a firm opinion about the existence of a kind of "magic" of intelligent systems, which is still not understood and therefore is not available to the vast majority of modern developers.

It is possible to comprehend and understand this "magic" only with the help of modern fundamental science. At present, on the basis of an objectively expanded concept of information to complete information (quantitative and qualitative together), fundamental science is able to propose new ways to solve the problem of artificial mind, both in small and in general. These solutions can be built on the correct basis, they are more effective and have a clearer perspective than the currently proposed bio-inspired intuitive and heuristic templates for solving artificial intelligence problems.

In this paper, one of the most important intellectual technologies of artificial intelligence, namely, video-intelligent technology, is considered as a hierarchically ascending synthesis of "mental" evaluations of video-information. This process begins with the synthesis of evaluation of weak (1D, 2D) video-information, which have a "rough" topology, and develops towards the synthesis of evaluations of "strong" (3D, 4D) video-information with a "finer" topology. This approach corresponds to the well-known perceptual model of the world in human consciousness, which was proposed in 1935 in the USSR by the physiologist N.A. Bernstein and pointed to the topological concept of the brain, namely, that "the brain reflects the world topologically" [N.A. Bernstein].

In the future, we will proceed from the fact that it is the post-Shannon informational approach, which was verified on the problems of video-information analysis, with the appropriate development, is able to effectively solve the problems of "mental" synthesis of video-information evaluations using the structural (topological, qualitative) concept of brain-like intelligent systems. It should be noted that the processes of natural or artificial formation of video-information are significantly different from the processes of constructing "mental" evaluation of video-information (generally speaking, more than formal analysis differs from formal synthesis). Due to this, the new (post-Shannon's) informational approach makes it possible to establish only the most general fundamental requirements for the "mental" synthesis of video-information evaluations. Namely, the evaluations of video-information should be formed as a result of strong "mental" interactions (interactions-measurements). In addition, video-evaluations should be complete and therefore include physical and structural components considered together. Finally, artificial vision, as the most informative

component of artificial intelligence, should be a sequence of gradually more complex stages of “mental” recognition, perception and understanding, which are considered together in the form of an ascending hierarchy of “weak” (1D, 2D) and of “strong” (3D, 4D) evaluations of video- information. The latter already possess the quality of “mentality” comparable to the mental activity of a person, about which it is known that it is an extremely fast process. This circumstance did not pass unnoticed in human society, the centuries-old folk wisdom of which was reflected in folk tales, where the correct answer to the riddle "What is the fastest in the world?" was the answer "Thought".

Thus, the post-Shannon informational approach-analysis needs to be rethought and supplemented in order to achieve its adequacy in solving the problems of intellectual synthesis of “mental” evaluations of video-information, including by creating an information theory of artificial mind. Of its particular case is the information theory of intelligent artificial vision the sketch of which [1] was discussed earlier and did not have deep theoretical support. It should be noted that the infrastructure of the ISAM includes not only the ascending hierarchy of “mental” evaluations of information (recognition, perception and understanding), which is directed to the “mental” space of the ISAM, but also the descending hierarchy of service transformations in the form of video-information by feedback, which is directed back to the input ISAM. Latent and not obvious due to its nonlinearity “mental” informational nature of video-intelligence sensory component of artificial mind can be fully realized only when using the post-Shannon informational approach and no other. This makes it possible to meaningfully solve the problems of systemic informational synthesis of artificial vision in the form of an ascending hierarchy of effective intelligent structures of video-recognition, video-perception and video-understanding of the spatio-temporal content of the surrounding material world.

## II. DIFFERENTIAL HOLOGRAPHIC PRINCIPLE OF VIDEO- INFORMATION

Currently, the concept of holography has acquired a wide semantic content, which allows it to be used not only in applied, but also in fundamental science [2, 3], for example, in string theory in the form of a holographic principle. The holographic principle as applied to video-information turned out to be, generally speaking, strongly “disguised”, and to determine it, a special study was required, the results of which were not fully comprehended at once. Let us consider this on the example of analyzing the process of forming full information (physical and structural together) [4, 5, 6, 7] or, which is the same, video-information, in a some material system.

The need for effective construction of video-information evaluation in the process of artificial vision requires the involvement of a new (post-Shannon) information approach. In this case, the process of evaluation video-information by artificial vision should also be a set of strong interactions (interactions-measurements), but already of artificial origin. A meaningful division of artificial vision into simpler and, therefore, more accessible for implementation, partial interactions-dimensions as a whole corresponds to the new

information approach. However, natural and artificial measuring processes have fundamental differences in terms of their implementation. In the natural process of forming video-information at the physical level, only natural physical standards of measured quantities are used, which, due to the supra-physical (abstract, qualitative) nature of the visual process, cannot be used even in the processes of natural vision of highly developed living organisms.

This circumstance gives rise to the need to create artificial measuring standards for evaluation video-information, which cannot be physically extracted from their natural environment, since they are supra-physical and are related to the structural component of video-information evaluation. In this regard, taking care of the construction of such measuring standards is a super task of any highly organized natural organism or artificial system, if their goal is survival and prosperity in the real conditions of the surrounding (often extreme) material World. This super-problem is solved in both cases in the same way and is reduced to the construction of the necessary artificial measuring standards by using appropriate training and/or self-training. These measuring standards can be organized in the form of a hierarchy of qualitative measuring scales of low and high ranks at different levels of the hierarchy of an artificial intelligent system. In particular, the ascending hierarchy of quality measurement scales for artificial vision can be represented by an ascending hierarchy of video-thesauruses. At the highest level of this ascending hierarchy is artificial video-intelligence [8], which can be considered as a video-component of the corresponding artificial mind. The carriers of the input physical video-data for the artificial vision technology are weak (in the video-information sense) wave fields-mediators of different physical nature (optical and non-optical), which provide video-information short-range interaction through the physical transfer of weak video-information in space-time. The physical nature of these intermediary fields is wave-like. Therefore, an input optical or non-optical video-receiver can provide consistent video-reception using modern ideas [9], for example, based on coherent or incoherent holography. In modern video-technology and in living nature, a binocular video-receiver based on stereoscopy, which can be adequately described in terms of incoherent holography, is widespread. However, such an obvious application of physical holography at a low level of the ISAM hierarchy does not mean at all that the use of holographic ideas at higher levels of the hierarchy of “mental” evaluation of video-information will be just as obvious.

For the post-Shannon information approach, the basic is the principle of identity of the presentation of video-information [4 - 6], which can be expressed by the following identity.

$$D_m t_n^m = \nabla_m T_n^m \quad (1)$$

where

$t_n^m = t_{n(E)}^m + t_{n(S)}^m$  - video-information in global coordinates of Minkowski space in the form of physical  $(t_{n(E)}^m)$  and structural  $(t_{n(S)}^m)$  components considered together;

$T_{n(E)}^m$  - physical component of video-information in local coordinates of effective Riemannian space-time;

$D_m$  - operator of covariant divergence in the metric of the Minkowski space;

$\nabla_m$  - operator of covariant divergence in the metric of the Riemannian space-time.

Principle (1) operates in the effective Riemannian space-time [4 - 6] formed by the product of two subspaces - the Minkowski space and the Riemannian space-time of general form. Equating identity (1) to zero, one can obtain a differential conservation law, from which the concept of video-information as the sum of its physical and structural components, considered together in the global coordinates of the Minkowski space [4 - 6], necessarily follows. However, it turned out that identity (1) has one more important and previously unaccounted for informational "bonus". Namely, expression (1) can be additionally considered as a mathematically accurate and physically correct differential holographic principle (DHP).

Indeed, according to identity (1), the covariant divergence in the Minkowski space from video-information in the form of the sum of its physical and structural components is exactly equal to the covariant divergence in the effective Riemannian space-time from only one, namely, by the physical component of video-information. This ensures the identity of the transformation of video-information from a flat Minkowski space-time into a curved effective Riemannian space-time and vice versa. In other words, if the physical component of the video-information is given in local coordinates on the hypersurface of the effective Riemannian space-time, then, in accordance with identity (1), the corresponding video-information can be precisely determined as the sum of its physical and structural components in the global coordinates of the Minkowski space inside the effective hypervolume Riemannian space-time. It should nevertheless be noted that if the physical component of the video-information is given on the hypersurface of a general Riemannian subspace-time, then in the effective Riemannian space-time (the product of the general Riemannian subspace-time and the Minkowski subspace) this same component of video-information is necessarily also a function of global coordinates Minkowski space.

Modern concepts [2, 3] of duality and the holographic principle are used in string theory. However, these concepts are largely qualitative and have not yet found an exact mathematical justification for them. Its absence is replaced by an intuitive reference to the duality of a two-dimensional (flat) hologram and a three-dimensional (volume) image reconstructed from it, which, generally speaking, is not entirely correct. In fact, and this was shown even at the initial stages [10] of holography research, the highest quality hologram is not a flat, but a volumetric hologram, which allows recording wavefronts scattered by the observed material surface into the volume of the photographic material. This circumstance makes it possible to adequately reconstruct a three-dimensional

image, and not necessarily with the help of a coherent light source.

In string theory (M-theory or modern mathematical physics), the ideas of duality and the holographic principle have found their qualitative confirmation in the macrocosm of black holes. Most of the models that string theorists work with relate to specific spaces and interactions of the macrocosm (Universe), but not the real macrocosm around us. In other words, modern string theory uses the holographic principle at a qualitative (intuitive) level and therefore cannot serve as a guiding theory for the problems of assessing video-information in the material macrocosm. This world, as shown earlier in [4 - 6], is most justified to consider (in relation to the problems of formation and evaluation of information, but not only to them) immersed in the effective Riemannian space-time.

Taking this into account, we will assume that nature naturally makes it possible to dually present video information in the effective Riemannian space-time of the surrounding macrocosm. Both of these approaches are theoretically equivalent and are dually juxtaposed to the same reality (material object or process). These dual video-information theories are identical in their end result to each other, which leads to predictable consequences. Namely, the "hard" information computations in one subspace of the effective Riemannian space-time can be correctly replaced with "easier" information computations in its other subspace and vice versa.

General reasoning is also possible, for example, for an adequate video informational description of the macrocosm that surrounds us, video-information at its external "boundaries" is sufficient. At the same time, it is reasonable to believe that it is the surface, not the volume, that is the place where fundamental processes that generate video-information take place (for example, due to scattering or rereflection of the activating wave field). Then, if the structural component of the video-information is given in local coordinates on the hypersurface of the effective Riemannian space-time, then the DHP (1) speaks of how the video-information in the differential form will mathematically accurately look in the global coordinates of the hypervolume of the effective Riemannian space-time.

The new (post-Shannon) informational approach is based on the metric approach [6], which makes it possible to formulate DHP (1) in a general form physically and mathematically. This principle in the weak-field approximation ( $D_m \rightarrow \partial_m, \nabla_m \rightarrow D_m$ ) is transformed into a weak DHP, which can be written in the form.

$$\partial_m^{(0)} t_n^m = D_m^{(0)} T_{n(E)}^m \quad (2)$$

where

$t_n^m^{(0)}$  - weak video-information in global coordinates of Minkowski space;

$T_{n(E)}^{m(0)}$  - the physical component of weak video-information in local coordinates of an effective Riemannian space of constant curvature, which, due to this, can be considered as a conformally pseudo-Euclidean space;

$\partial_m$  - differentiation operator in Minkowski space;

$D_m$  - operator of covariant divergence with respect to the metric of the Minkowski space in a Riemannian space-time of constant curvature (or, otherwise, in a conformally pseudo-Euclidean space).

The post-Shannon informational approach is based on the existence of differential conservation laws. In particular, the law of conservation of video-information can be written in accordance with identity (1), in the form.

$$D_m t_n^m = \nabla_m T_{n(E)}^m = 0 \quad (3)$$

Based on expression (3), video-information can be defined as the sum of its physical and structural components, considered together in the global coordinates of the Minkowski space.

$$D_m t_n^m = D_m (t_{n(E)}^m + t_{n(S)}^m) = 0 \quad (4)$$

$$t_n^m = t_{n(E)}^m + t_{n(S)}^m \quad (5)$$

If we carefully consider equality (3), then we can see that there is no expression for the structural component of video-information in local coordinates. This happens because this component of video-information induces Riemannian space-time, in which only the physical component of video-information manifests itself locally. In this case, the expression  $\nabla_m T_{n(E)}^m = 0$  has the form of a differential covariant conservation equation in local coordinates of the effective Riemannian space-time, but does not guarantee the possibility of obtaining the corresponding integral conservation law and, therefore, does not allow us to understand what is conserved in this case. Therefore, this expression does not contribute to the formal definition of the concept of video-information and, in accordance with the DHP (1), indicates that the capabilities of the mathematical apparatus of video-information computations in subspaces-factors of the effective Riemannian space-time differ significantly.

In the hypervolume of the effective Riemannian space-time, the results of video-information calculations can be globally presented in a evidentform, and their meaning is usually obvious. On the hypersurface of the effective Riemannian space-time, the possibilities of information computations are wider, but due to their local nature, they are much more abstract and non-obvious, and in terms of meaning, they may need a detailed interpretation.

It should be noted that the structural (qualitative) and physical (quantitative) components of video-information, due to DHP, always cross-strongly interact with each other [6]. The activating component of this interaction is the structural

component of video-information  $t_{n(S)}^m$ , which can be considered as a "primary" component, and the passive (activated) and therefore "secondary" component is the physical component of video-information  $t_{n(E)}^m$ . These fundamental interdependencies [6] for general video-information components, as well as for weak video-information, are as follows.

$$G_{mn}^q T_{q(E)}^n = -D_n t_{m(S)}^{n(*)} \quad (6)$$

$$\gamma_{mn}^q T_{q(E)}^n = -\partial_n t_{m(S)}^{n(*)0} \quad (7)$$

where

$G_{mn}^q, \gamma_{mn}^q$  - tensor of the third rank with respect to general coordinate transformations and connectivity (Christoffel symbol) in Minkowski space;

$T_{q(E)}^n, T_{q(E)}^{n(0)}$  - physical component video-information of general appearance and weak video-information;

$D_n, \partial_n$  - operators of covariant derivative and ordinary partial derivative in Minkowski space;

$t_{m(S)}^{n(*)}, t_{m(S)}^{n(*)0}$  - structural components (in canonical form) of general video-information and weak video information in global coordinates of Minkowski space.

In accordance with the DHP, the structural component of video-information in local coordinates of the effective Riemannian space-time is excluded from consideration. At the same time, its energy induces this curved space-time and activates the physical component of video-information in it. In the global coordinates of the effective Riemannian space-time, both components of the video-information jointly form, on the basis of their composition, video-information of a general form, which, in accordance with the conservation law, becomes the source of the video-information field of the corresponding physical nature.

### III. STRUCTURING AND COLLECTING VIDEO-DATA AT A LOW LEVEL ISAM HIERARCHIES

Video-information in physical space-time and evaluation of video-information in the "mental" space of the ISAM should support the isomorphism of the second kind [8], in which the relationship between the elements of video-information evaluation in the "mental" space of the system will be the same as between the elements video-information in the real world. Due to this, artificial vision can be considered as a process of mapping the visually available properties of the surrounding material world into their identical virtual representation in the "mental" space of ISAM. This is a necessary condition for the correct evaluation of video-information about the current space-time environment. The properties of video-information (physical and structural together) can only be virtually

emulated by the properties of video-information evaluation in the “mental” space of ISAM. Due to this, the evaluation of video-information can be considered as a result of the calibration (supra-coordinate) transformation of video-information. However, it turned out to be difficult to apply the calibration ideology for direct reformulation of video-information into a supra-coordinate form of video-information evaluation. Indeed, the process of evaluation video-information in ISAM is an ascending hierarchical process that is directed from evaluations of weak video-information to evaluations of strong video-information, and this is fundamentally different from the natural process of forming video-information in nature. The formation of video-information proceeds from physically inaccessible strong general video-information to available weak video-information, i.e. top-down. Generally speaking, video-information in nature is formed as strong video information with a “thin” topology. At the same time, in the real World, the transfer of strong video-information in space-time is possible only by its reduction into weak video-information and is carried out by a weak video-information field, the source of which, in accordance with the conservation law, will be the corresponding weak video-information.

Thus, the input video-signal of the ISAM is always a weak video-information field of one or another physical nature, which carries out a calibration supra-coordinate transformation [8] and has nothing to do with coordinate transformations. It is because of this that there is a second-order isomorphism (identity) of the evaluation of weak video-information generated by ISAM and weak video-information, which is considered as a source of a weak video-information field.

In the macrocosm surrounding us, video-information is usually viewed in terms of intensity. Therefore, the evaluation of the intensity of weak video-information can be written, neglecting the difference between the covariant and contravariant tensor components in flat space-time, as follows.

$$\begin{aligned}
 \hat{I}^{mn} &= \left( \hat{t}^{mn} \right)^2 = \left( \hat{t}_{(E)}^{mn} + \hat{t}_{(S)}^{mn} \right)^2 = \\
 &= \left( \hat{t}_{(E)}^{mn} \right)^2_{\rightarrow 0} + 2 \hat{t}_{(E)}^{mn} \hat{t}_{(S)}^{mn} + \left( \hat{t}_{(S)}^{mn} \right)^2_{\rightarrow 0} \rightarrow 2 \hat{t}_{(E)}^{mn} \hat{t}_{(S)}^{mn}
 \end{aligned} \tag{8}$$

The full quantum of video-data (FQV) can be written (using the notation [8]) in the form

$$\begin{aligned}
 \hat{I}_{mn}^{(0000)} &= \left( \hat{t}_{mn}^{(0000)} \right)^2 \rightarrow 2 \hat{t}_{mn(E)}^{(0000)} \cdot \hat{t}_{mn(S)}^{(0000)} \equiv \\
 &\equiv \hat{t}_{mn(E)}^{(0000)} \cdot d \hat{t}_{mn(E)}^{(0000)} = \omega_0 \omega_1
 \end{aligned} \tag{9}$$

where

$\hat{t}_{mn(E)}^{(0000)} = \omega_0$  - physical quantum of weak video-information evaluation (local physical sampling in the form of a scalar, which can be considered as a differential 0-form);

$d \hat{t}_{mn(E)}^{(0000)} = d \omega_0 = \omega_1$  - structural quantum (local 1-quant) of evaluation weak video- information, which can be considered as a differential 1-form.

Expression (8) formally corresponds to a hologram formed by the interaction of two partially coherent processes, which take the form of physical (partially physicalized) and structural (partially geometrized) components of weak video-information. In this case, the physical component of weak video-information "delegates" to expression (9) for FQV a physical quantum (physical sample in the form of 0-form), and the structural component of weak video-information, respectively, a structural quantum (local quality in the form of 1-form). Considering the existing experience in processing holographic video-data, it is possible to consider the question of the relative importance of the physical and structural components of the input weak video-information of the ISAM.

Structural reformatting (structuring) of physical video data is carried out in ISAM using FQV and artificial saccades, the purpose of which is similar to the purpose of saccades of natural vision. Artificial saccades can be represented by a linear combination of FQV.

$$C_{1,i(t)} = \sum_{i=1}^I \omega_{0,i(t)} \omega_{1,i(t)} \rightarrow \bigcup_{i=1}^I \omega_{0,i(t)} \omega_{1,i(t)}, \quad i = \overline{1, I} \tag{10}$$

Here  $C_{1,i(t)}$  - his is an artificial saccade formed by a dynamic linear combination of neighboring FQVs, which is equivalent to their sequential scanning, considering the local spatial orientation of each FQV included in this linear combination.

In the future, these artificial saccades form a certain set  $I$  in which each artificial saccade has a small 1D local spatial size. This allows us to consider artificial saccades as elementary “dimensional” dynamic structures. Therefore, combining artificial saccades into compound linear combinations (super-saccades) will dynamically "measure" 1D video-data of a much larger size. Such 1D video-data can be considered as a set  $J$  of super-saccades, which is much smaller than the set of original artificial saccades  $I$ . Thus, in the process of 1D learning (self-learning), super-saccades perform the function of some intermediate dimensional 1D video-data, which can later be used to construct a 1D video-thesaurus (scale of dimensional 1D video-data) of ISAM.

$$C_{1,i(t)j(t)} = \sum_{j=1}^J \left( C_{1,i(t)} \right)_{j(t)} \rightarrow \bigcup_{j=1}^J \left( C_{1,i(t)} \right)_{j(t)}, \quad j = \overline{1, J} \tag{11}$$

If the time interval  $t_i = T_i / I$  determines the duration of a certain  $i$  current "artificial" saccade without considering the protective scanning time intervals, then the time interval

$t_j = T_j / J$  determines the duration of a  $J$  certain current super saccade (intermediate 1D video-data). In this case, expression (11) for intermediate 1D video-data synthesized by artificial saccades and super saccades will be fully defined in 1D space. This dynamic set of intermediate 1D video-data generated over time  $T_{ij} = T_i \cdot T_j$  ( $T_i = t_i \cdot I$ ,  $T_j = t_j \cdot J$ ) forms a 1D video-thesaurus  $C_{1,j}(C_{1,i})$ .

$$C_{1,j}(C_{1,i}) = \sum_{j=1}^J \left( \sum_{i=1}^I \omega_{0,i} \omega_{1,i} \right)_j \rightarrow \bigcup_{j=1}^J \left( \bigcup_{i=1}^I \omega_{0,i} \omega_{0,j} \right)_j, i = \overline{1, I}, j = \overline{1, J} \quad (12)$$

where

$C_{1,j}(C_{1,i})$  – 1D video-thesaurus, dynamically replenishing due to previously unknown current 1D intermediate video-data, qualitatively presented by splitting into “dimensional” artificial saccades and super-saccades;

$J \cdot I = K$  – the total number of 1D video-data accumulated in the 1D video-thesaurus.

The strings metaphor [2, 3], [11 - 13] in ISAM is that the relationship between the FQVs and global 1-, 2-, 3-, 4-kvalts in the macrocosm can be considered similarly to the relations between strings and branes in the microcosm. In this case, the FQV can serve as an analogue of a strings, and the global 1-qualts can be considered as a 1-brane. Branes possessing one, two, three or four dimensions [11 - 13] and can be considered as “layers” of space or as “layers” covering the corresponding space. The dimension of a brane is the number of its dimensions (degrees of freedom) possessed by objects that are “captured” or, in other words, associated with the brane.

However, string theory (like quantum theory) is still a theory of the microworld and in an explicit form cannot be used as a productive theory for evaluating video-information in the macroworld. In fact, the string metaphor in ISAM predicts the complexity and multistage solution of the problem of “understanding” video-information, considered as a complex problem of joint evaluation of video-information in small (evaluation weak 1D and 2D video-information) and in general (evaluation “strong” 3D and 4D video-information).

Reformatting into a structural format is carried out on the basis of long-range measurements supported by structured (abstract) video-information macro-objects (in the form of 1D, 2D, 3D and 4D video-thesaurus), which have the properties of structural (qualitative) measuring scales. In the simplest case, these measuring scales can be constructed by software and hardware (for example, in the form of a structural proto-thesaurus), but in the general case, only by training / self-learning ISAM. In this case, the well-known topological property [14] is used, according to which a structural video-information macro-object of dimension  $N$  can be accurately represented by a set of dimensional video-structures of dimension  $N - 1$  that divide this initial macro-object of

dimension  $N$  into arbitrarily small parts, and this cannot be done using a set of dimensional dimension video-structures  $N - 2$ .

The physical and structural components of weak video-information are connected by identity (13), which characterizes their deep interconnection and can be represented as the following schematic expression.

$$T_{(E)q}^n \xrightarrow{d} \gamma_{mn}^q T_{(E)q}^n = -\partial_n t_{(S)m}^n \leftarrow t_{(S)m}^n \quad (13)$$

where

$T_{(E)q}^n = t_{(E)q}^n$  – local meaning (structureless physical sampling, differential 0-form, 0-qualt) of the physical component of weak video-information;

$t_{(S)m}^n$  – the structural component of weak video-information in the canonical form (in accordance with identity (13), it can be considered as a differential 2-form);

$d$  – an outer differentiation operator (coboundary operator or, in other words, a cohomological operator) that increases the order of a differential form by one and coincides (in the case of an outer differentiation of 0-forms) with the ordinary differentiation operator;

$\partial$  – boundary operator dual to the operator  $d$  and defining the homology group dual to the cohomology group;

$\delta$  – the codifferentiation operator conjugates to  $d$  and decreasing the order of the differential form by one (the divergence [15] of the skew-symmetric tensor).

Expression (13) differs from the original identity (7) in that its left and right sides are supplemented, respectively, by the operators of external differentiation  $d$  and the operator of codifferentiation conjugated to it. These operators respectively increase and decrease the order of differential forms by one for 0- and 2-forms of weak video information. In this case, the left and right sides of identity (13) form one and the same quantity, namely, a differential 1-form, which can be compared to a structural quantum in the form of a local quality. From expression (13) it follows that the 2-form of the structural component of weak video information, activates and thereby completely determines its 1-form, in which the carrier of local structural properties (local orientation) is the local qualt.

The analysis of the identity (13) allows us to conclude that local quantities can be built by differentiating the corresponding physical samples of weak video- information evaluation. In fact, this can be considered as the simplest inverse problem of a low hierarchy level with a solution algorithm represented by expression (13). The result of this solution is the construction of a set of structural quanta (local qualts) for the subsequent evaluation of their spatial orientation and structural reformatting. Further, full quanta of video-data (FQV) are formed, which are jointly considered the corresponding physical and structural quanta of the evaluation

of weak video-information. This makes it possible to construct a linear combination of FQV using saccades, which is carried out in a dynamic mode corresponding to one-dimensional scanning of FQV. In general, such 1D scanning is similar to human eye movement [16, 17, 18], which looks like a series of saccades (super-saccades) and fixations. In this case, the spatial orientation of the local quality as an element of the FQV coincides with the local orientation of the corresponding structural quantum of the assessment of weak 1D video-information and allows you to direct the scanning process. In turn, the “weight” of each FQV in their linear combination is determined by the scalar value of the physical quantum (0-kvalt) as an element of the FQV.

At the macrolevel of the world outlook, FQVs can be qualitatively compared to strings, which are considered by string theory as fundamental elementary structures of the microworld. If we assume that the string metaphor of the macrocosm is productive, then the next in the hierarchy is the fundamental concept of the microcosm, namely, the 1-brane, most of all corresponds to the semantic content of the global 1-qualt, which can be compared to the 1-variety. In this case, the global 1-qualt is a composite dimensional 1D structure with elements that are dynamically formed by super-saccades. Dimensional structures are used to represent the structures of manifolds due to the fact that measuring structural (supra-physical) standards are absent in nature, and therefore can be formed only artificially by means of training (self-learning) ISAM.

#### IV. INTEGRAL QUASI-HOLOGRAPHIC PRINCIPLE OF EVALUATION OF VIDEO-INFORMATION

The general formalism of constructing evaluation of video-information should consider their reformatting into a structural format, skew-symmetry of the designations of the tensors associated with them and their external derivatives. This allows us to describe this formalism in a unified way in the form of the theory of differential forms, considering those degrees of freedom that are provided by the main theorem of external analysis. Particular cases of this theorem are well known (under the names of Newton-Leibniz, Green, Gauss-Ostrogradsky) and are combined by Stokes' theorem [2, 15, 19, 20]. However, the video- information formalism [4 - 6] was originally formulated in tensor notation. Therefore, mathematically correct, but too abstract and abbreviated designations that are adopted in the theory of differential forms can seriously complicate the construction of information models for evaluation video- information and, moreover, lead the modeling of this process to a dead end. In this regard, tensor designations will be used to construct evaluation of video-information. In this case, the ideas of the mathematical theory of differential forms will be considered, but in a more physicalized form and not so abstractly as is customary in modern mathematics.

Indeed, in the global coordinates of the effective Riemannian space-time, the video information in accordance with (1) has the form.

$$t_n^m = t_{n(E)}^m + t_{n(S)}^m \quad (14)$$

In the case of a nondegenerate metric tensor of the Minkowski space  $\gamma_{mn}$  in expression (14), it can be used to lower the contravariant index and write the density of the video information tensor as a sum of symmetric (*sym*) and skew-symmetric (*alt*) components. However, in order to avoid unnecessary clumsiness of expressions, the Minkowski space in artificial vision is conveniently considered in rectangular (Euclidean) coordinates. In this case, there is no distinction between superscripts and subscripts, and all indices, for example, can be considered as subscript.

$$t_{mn} = t_{mn}^{(sym)} + t_{mn}^{(alt)} \quad (15)$$

where

$$t_{mn}^{(sym)} = \frac{1}{2}(t_{mn} + t_{nm}); t_{mn}^{(alt)} = \frac{1}{2}(t_{mn} - t_{nm}) \quad (16)$$

Considering (15), expression (14) can be written in the form

$$t_{mn} = t_{mn(E)} + t_{mn(S)} = t_{mn}^{(sym)} + t_{mn}^{(alt)} \quad (17)$$

where

$t_{mn(E)}$  =  $t_{mn}^{(sym)}$  - physical (symmetric) tensor component of video-information in global coordinates of Minkowski space;

$t_{mn(S)}$  =  $t_{mn}^{(alt)}$  - structural (skew-symmetric) tensor component of video-information in global coordinates of Minkowski space.

In the material macrocosm that surrounds us, the video-intelligent technology of artificial vision is initiated by the short-range action of the video-receiver and weak video-information through weak video-information field, the source of which is weak video-information. In this case, weak video-information is usually considered in terms of intensity.

$$\begin{aligned} I_{mn}^{(0)} &= \left( t_{mn}^{(0)} \right)^2 = \left( t_{mn(E)}^{(0)} + t_{mn(S)}^{(0)} \right)^2 = \\ &= \left( t_{mn}^{(sym)} + t_{mn}^{(alt)} \right)^2 \rightarrow 2 t_{mn}^{(sym)} t_{mn}^{(alt)} \end{aligned} \quad (18)$$

The expression for evaluation the intensity of weak video-information based on (17) and (18) can be written in the form.

$$\begin{aligned} \hat{I}_{mn}^{(0)} &= \left( \hat{t}_{mn}^{(0)} \right)^2 = \left( \hat{t}_{mn(E)}^{(0)} + \hat{t}_{mn(S)}^{(0)} \right)^2 = \\ &= \left( \hat{t}_{mn}^{(sym)} + \hat{t}_{mn}^{(alt)} \right)^2 \rightarrow 2 \hat{t}_{mn}^{(sym)} \hat{t}_{mn}^{(alt)} \end{aligned} \quad (19)$$

It follows from (19) that the estimate of the intensity of weak video- information is determined by the product of its physical (symmetric) and structural (skew-symmetric) tensor components. The video-receiver, after appropriate physical measurements, forms an evaluation of the physical component of weak video-information, which is considered as a physical picture and is sometimes interpreted as an image, which, generally speaking, is erroneous.

In fact, when a person observes a physical picture he evaluates (sees) together the physical and structural components of the evaluation of weak video-information. In this case, the evaluation of the structural (abstract) component of the evaluation of weak video information, which the physical video-receiver is fundamentally unable to register, is formed as a result of the mental activity of the human brain. In other words, when observing a physical picture during several initial stages of vision (natural or artificial), evaluations of the elements of the structural component of weak video-information are very quickly synthesized artificially, which correspond to the elements of this physical picture. Further, a joint interpretation of the physically measured and abstractly synthesized elements of these evaluations is carried out, which is accompanied by the construction and recognition of one-dimensional and two-dimensional images. As a result, an image as a picture, in which the corresponding physical and structural components of weak video-information are presented together, can only be constructed virtually on the basis of joint physical measurements and structural representations in the mental space of the human brain or in a brain-like artificial vision system.

Let us consider the features of constructing evaluations of the physical (symmetric) and structural (skew-symmetric) components of weak video information. The process of constructing a discrete physical picture by any physical video-receiver (from a video camera to a multi-element antenna array) is almost always carried out in a similar way. In the era of digital technologies, the most natural for artificial vision is a digital holographic video-receiver based on an incoherent binocular optical video-receiver or a coherent non-optical matrix video-receiver. These physical video-receivers use the optimal video-reception based on a matched filter, which greatly facilitates the analysis of the corresponding holographic process and allows you to completely meaningfully create discrete information models of coherent and incoherent holographic video-receivers adapted to ISAM. For example, in the case of a coherent video- receiver, it is possible to construct a video-informational model [9] on the basis of a weak DHP (2) for evaluating the discrete physical component of weak video-information in the form.

$$\begin{aligned} & \hat{t}_{mn}^{(sym)} [r, \Delta z, \Delta \tau] = \\ & = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} t_{mn}^{(0)}(r) t_{mn}^{(sym)*} [r'] W_{(c|0)}(\Delta x, \Delta y, \Delta z, \Delta \tau) dx' dy' = \\ & = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} t_{mn}^{(sym)}(r) t_{mn}^{(0)*} [r'] W_{(c|0)}(\Delta x, \Delta y, \Delta z, \Delta \tau) dx' dy' . \end{aligned} \quad (20)$$

Here and below, square brackets are used to symbolically denote discrete functions. Moreover, in expression (20)  $t_{mn(E)}^{(0)}(r) = t_{mn}^{(sym)}(r)$  – physical component of weak video-information;

$r(x, y, z)$  – coordinates in the area of definition of weak video-information;

$r'(x', y', z')$  – coordinates in the area of definition of the virtual physical component of the reference weak video-information;

$t, t', \Delta \tau, c$  - respectively, the time coordinates of the object (reflected) and reference weak video-information fields, their time shift and propagation speed in the considered physical environment;

$$\begin{aligned} t_{mn}^{(0)*} &= comb\left(\frac{x'}{b}\right) comb\left(\frac{y'}{b}\right) = \\ &= \sum_{m=-\infty}^{m=+\infty} \sum_{n=-\infty}^{n=+\infty} \delta\left(\frac{x'}{b} - m\right) \delta\left(\frac{y'}{b} - n\right) = \begin{cases} 1, npu \ x' = mb, y' = nb \\ 0, npu \ x' \neq mb, y' \neq nb \end{cases} \end{aligned} \quad (21)$$

- the physical component of the weak reference video-information is virtually formed by the physical (programmable, “genetic”) proto-thesaurus and provides an ideal spatial sampling of weak physical video-information in the form of a two-dimensional lattice  $\mathcal{D}$  - functions;

$W_{(c|0)}(\Delta x, \Delta y, \Delta z, \Delta \tau) = W_{R_z}(\Delta x, \Delta y, \Delta z) W_{z(c|0)}(\Delta \tau)$  – the weight function of the ISAM physical video-receiver, which in the quasi-stationary approximation mode has the form of a multidimensional correlation function with factorization into spatial and temporal components;

$$\begin{aligned} W_{R_z}(\Delta x, \Delta y, \Delta z) &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \Pi_{A_1}(r_1) \frac{1}{zz'} \exp\left\{-j\omega_0 \frac{R_z - R_z'}{c}\right\} d\mu d\nu , \\ W_{z(c|0)} &= \int_{-\infty}^{+\infty} U\left(t - \frac{2z}{c}\right) U_0'\left(t - \frac{2z'}{c}\right) dt \end{aligned}$$

- spatial and temporal components of the weighting function of the physical video-receiver, which maintain its selectivity in the transverse and longitudinal directions;

$$\begin{aligned} R_z &\cong z + \frac{(\mu - x_z)^2}{2z} + \frac{(\nu - y_z)^2}{2z} ; \\ R_z' &\cong z' + \frac{(\mu - x_z')^2}{2z} + \frac{(\nu - y_z')^2}{2z} ; \end{aligned}$$

$\mu, \nu$  – coordinates in the opening plane of the physical aperture of the video-receiver;

$\hat{t}_{mn}^{(sym)} [r, \Delta z, \Delta \tau]$  – evaluation of the physical component of weak video-information in the form of a set of structureless physical samples, the spatial frequency of which is determined by the lattice  $\delta$  - functions of the physical proto-thesaurus, and

their shape coincides with the weight function of the physical component of the video-receiver.

The supra-physical (abstract) nature of the evaluation of the structural component of weak video-information supports the video-information model of the structural interaction of the corresponding supra-physical components, for the implementation of which physical intermediary fields are not needed. Thus, under these conditions, the supra-physical interaction, due to its abstract nature, can (and should) be considered as a long-range action-measurement, the speed of which is infinitely high ( $c \rightarrow \infty$ ) and this determines the instantaneous nature of such interaction. Under these conditions, the weight function of the structural component of the video-receiver necessarily degenerates into a certain scalar quantity, which, without loss of generality, can be identified with unity. With regard to information models, this means a formal transition from the super-position integral (20) to the “scalar product” (22) of the surface (line, volume, etc.) and the corresponding differential form.

$$\begin{aligned} & \hat{t}_{mn}^{(alt)}(r', a) = \quad (22) \\ & = d \left\{ \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \hat{t}_{mn}^{(sym)}(r) \hat{t}_{mn}^{(0)*} [r'] W_{(c \rightarrow \infty)}(\Delta x, \Delta y, \Delta z, \Delta \tau) dx' dy' \right\} \rightarrow \\ & \xrightarrow{c \rightarrow \infty, \Delta z \rightarrow 0, \Delta \tau \rightarrow 0} \hat{t}_{mn}^{(alt)} [r', a] = \int_{-\infty}^{+\infty} d \left\{ \hat{t}_{mn}^{(sym)} [r'] \right\} \hat{t}_{mn}^{(0)*} [r', a] dx' dy' = \\ & = \left\langle \hat{t}_{mn}^{(alt)} [r'] \hat{t}_{mn}^{(0)*} [r', a'], dx' dy' \right\rangle = \left\langle \hat{t}_{mn}^{(alt)} [r', a'], \omega_2 \right\rangle \end{aligned}$$

In this expression,  $dx' \wedge dy' = -dy' \wedge dx' = \omega_2$  it is a record in differential form of a basis in the space of skew-symmetric tensors, and the product symbol  $\wedge$  is introduced due to the fact that the orientation of the corresponding surface is essential.

Generally speaking, the concepts of tensors and differential forms should be understood in an extended form, i.e. in the form of a field on some manifold  $M$ , and not at some spatial point of this manifold.

From expression (22) it follows that at the initial stage of video-information restoration in accordance with the inverse problem of artificial vision, the external derivative of the set of physical samples (scalar values) of the physical component of the evaluation of weak video-information is formed. Thus, the structuring of physical samples for evaluation weak video-information is carried out by means of their structural reformatting into a set of differential 1-forms. These 1-forms are considered as structural quanta (local qualities) for evaluation weak video-information, which, in contrast to 0-forms, have orientations in space. The structural proto-

thesaurus  $\hat{t}_{mn}^{(0)*} [r', a']$  determines (measures) these orientations.

Expression (22) also includes the following quantities:

$$\begin{aligned} W_{(c \rightarrow \infty)}(\Delta x, \Delta y, \Delta z, \Delta \tau) & \xrightarrow{c \rightarrow \infty, \Delta z \rightarrow 0, \Delta \tau \rightarrow 0} W_{(c \rightarrow \infty)}(\Delta x, \Delta y) \rightarrow \\ & \xrightarrow{\text{without loss of generality}} 1 \end{aligned} \quad (23)$$

– the weight function of the structural component of the video-receiver corresponds to the structural (supra-physical) long-range action and can be taken equal to one;

$$\begin{aligned} & \hat{t}_{mn}^{(0)*} [r'] \rightarrow \hat{t}_{mn}^{(0)*} [r', a_i] = \\ & = \left\{ comb \left( \frac{x'}{b} \right) comb \left( \frac{y'}{b} \right) \right\} ** \bigcup_i \gamma_{\wedge}(a_i, l_i, x', y') = \\ & = \begin{cases} a_i, by \ x' = mb, y' = nb, a_i = tg(\alpha_i), i = 0, 1, 2, \dots, N; \\ 0, by \ x' \neq mb, y' \neq nb, a_i \neq tg(\alpha_i), i = 0, 1, 2, \dots, N; \end{cases} \end{aligned} \quad (24)$$

– the structural component of weak reference video-information is formed by a structural proto-thesaurus in the form of a lattice of multibeam stars, which can be compared to local goniometric scales and allow evaluation the tilt angles (orientations) of the corresponding structural quanta (local scales) in the video-receiver opening plane;

\*\* – mathematical symbol of two-dimensional convolution;

$a_i = tg(\alpha_i)$  – parameter of the spatial orientation of  $i$  the local quality, the length of which  $l_i = l = const$ , a  $\alpha_i$  is the angle of inclination (orientation) of the  $i$  local quality (1-form), locally measured by the structural proto-thesaurus.

Expression (24) assumes the local structure of the proto-thesaurus in the form of a multi-beam star  $\gamma_{\times}$  (25), which is a union  $n$  of segments (“rays”) with different parameters of spatial orientation  $a_i$  at the same length  $l_i = l$  and zero width. The number of rays determines the discreteness of angular measurements  $\alpha_i$ , and all rays intersect at a point (center) with coordinates.

$$\gamma_{\times} = \bigcup_i \gamma_{\wedge}(a_i, l_i, x', y') \quad (25)$$

On the whole, the structural proto-thesaurus is programmable and can be considered as a two-dimensional array of multibeam stars, the centers of which coincide with the centers of structureless physical samples. In this case, each multibeam star is functionally a local measuring scale of orientations only for one local samples, and together all these scales make it possible to measure (parallel or parallel-sequentially) the spatial orientations of all local qualts and thus, based on (22), reformat physical samples into elementary “mental” video-structures (into structural quanta or, what is the same, into local qualts).

In the original physical information model (20), the weight function of the physical component of the video-receiver has the form of the kernel of the Fourier-Fresnel transform, which provides the physical component of the video-receiver with the necessary space-time selectivity. As a result of structural reformatting of video-data, the structural component of the video-receiver loses its spatial selectivity, since its weight function becomes a scalar. As you know, a scalar is characterized only by its numerical value (modulus) and has no direction, which allows (without loss of generality and in order to avoid possible confusion) to identify the numerical value of this scalar with unity.

Usually the dot product is used in the traditional way, namely, as a mapping into some quantitative result, which has the form of a real number (ratio). In the application to video-intelligent technologies of artificial vision, the concept of scalar product, considering the duality of mathematics, it is advisable to use not in the traditional quantitative form, but in the qualitative form of mapping into a certain dimensional structure (system of relations) as a qualitative (mathematical, structural) process.

Many mathematical concepts, including, for example, a linear combination, have an ambiguity (duality) and therefore can be represented either quantitatively (in the form of numerical values) or qualitatively (in the form of mathematical expressions). In particular, a linear combination can have a quantitative form of an arbitrary number of relations in the form of a set of real numbers that together form a certain quantitative result. However, a linear combination can also have a qualitative form in the form of a system of relations or a structure (a mathematical expression of some process). Unlike a linear combination, a bundle will always have only a qualitative (structural) form and can represent the boundary of a manifold as a union of layers (submanifolds) whose dimension is one less than the dimension of the original manifold. It should be noted that the ambiguity of mathematics excludes the possibility of using a mathematical concept simultaneously in two forms - quantitative and qualitative.

Considering all the circumstances noted, expression (22), which corresponds to the simplest implementation of the integral quasi-holographic principle (IQHP), in a more general form (at some k-th level of the hierarchy) can be rewritten as.

$$\begin{array}{c}
 \text{Video-data} \\
 \text{of dimension } k \\
 \text{in the form of a bundle on} \\
 \text{evaluations of congruent} \\
 \text{video-information} \\
 \text{of dimension } k-1 \\
 \hat{t}_{mn(k-1),n}^{(alt)} = t_{mn(k)}^{(alt)} \xrightarrow{\text{Self-study}} \hat{t}_{mn(k),\beta}^{(alt)} = t_{mn(k),\beta}^{0(alt)} \xrightarrow{\text{"Mental" evaluation of video-information of dimension } k} \left\langle \hat{t}_{mn(k)}^{(alt)} \right\rangle \\
 \text{IQHP dimension } k
 \end{array}
 \quad (26)$$

where

$\hat{t}_{mn(k-1)}^{(alt)}$  - evaluation of video-information at the  $(k-1)$ -th stage of the ascending hierarchy of artificial vision;

$\hat{t}_{mn(k)}^{0(alt)} = \bigcup_B \hat{t}_{mn(k),\beta}^{(alt)}$  - video-thesaurus as a quality measuring scale, which is formed by accumulating and combining video-data at the k-th stage of the ascending hierarchy of artificial vision;

$\hat{t}_{mn(k)}^{(alt)}$  - evaluation of video-information at the k-th stage of the ascending hierarchy of artificial vision.

Dynamic linear combinations of FQVs can be considered as 1D dynamic dimensional video-structures that are formed by artificial saccades and allow one to evaluate (measure) 1D video-information together physically (quantitatively) and structurally (qualitatively). An enlarged dynamic linear combination of FQV in the form of a super-saccade can be considered as a composite 1D global dynamic dimensional structure, which can then be used to construct an evaluation of 2D video-information. In turn, the evaluation of 2D video-information can be considered as a composite dimensional structure for constructing an evaluation of 3D video-information, and the evaluation of 3D video-information, in turn, can be used as a dimensional structure for constructing an evaluation of 4D video- information.

The hierarchy of integral quasi-holographic video-information models of artificial vision can be built on the basis of IQHP, in which physical coherence is not considered due to the absence of physical intermediary fields. However, not only physical fields presented in the energy format of matter, but also supra-physical fields in the structural (abstract) format, can be considered as coherent (comparable) ones. In this case, the geometric congruence (comparability) of video-structures can be considered as a structural analog of physical coherence. Only qualitative measurements of video-information are possible, which in the absence of physical intermediary fields are performed instantly due to the qualitative nature of long-range video-measurements, but only by comparison, since qualitative calculations are not possible.

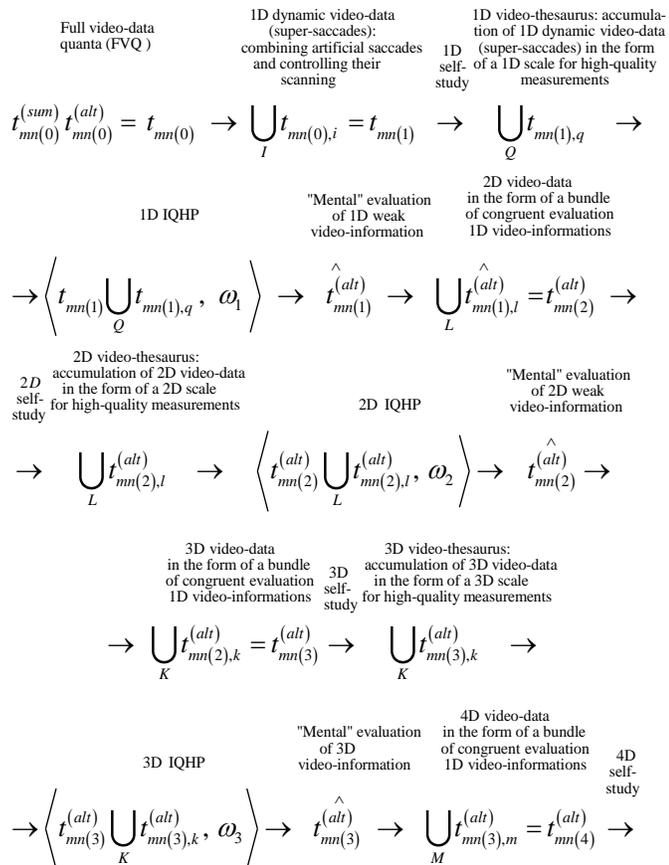
In accordance with the scheme-formula (26), manifolds of dimension  $k$  can be identically represented by bundles (partitions) into submanifolds of boundaries of dimension  $k-1$ , and this cannot be done by submanifolds of dimension  $k-2$ .

This means that the only significant dimensional elements that provide adequate sampling of 2D evaluation of video-information are 1D evaluation of video-information. According to the classical axiom of Archimedes, "any segment can be measured using any other" [21]. Therefore, for each of these 1D layers, the super-saccades in the form of enlarged artificial saccades will be the elementary dimensional structures. They can combine partial FQVs by scanning either in accordance with their "internal" spatial orientation of FQVs (during

training / self-learning), or on the basis of “external” spatial orientation, which in ISAM artificial vision is dictated by hierarchically descending video-informational feedback.

Accordingly, in the 3D case, the only significant sampling elements will be only 2D evaluation of video-information (in the form of images mapped to surfaces). In this case, each 2D evaluation of video- information will be compared, generally speaking, to the corresponding observed 2D area of the surface of the controlled 3D object. Finally, in the 4D case, the three-dimensional images of geometric bodies formed in the process of learning (self-learning) in the form of 3D evaluation of video- information and the 3-manifolds associated with them will be considered as the only significant “dimensional” elements.

The schematic formula (26) can be associated with a certain  $k$  stage of the ascending hierarchy, which implements a quasi-holographic abstract long-range action-measurement and generates an evaluation of a video-information of dimension  $k$ . In general, the structural and functional architecture of the ISAM video-component can be represented by a formal scheme (27), which, in turn, can be compared to the structure of the visual area of the artificial neocortex as the intellectual core of ISAM.



Video-intelligence: accumulation of 4D video-data in the form of a 4D scale for high-quality measurements

4D IQHP

"Mental" evaluation of 4D video-information

$$\rightarrow \bigcup_M t_{mn(4),m}^{(alt)} \rightarrow \left\langle t_{mn(4)}^{(alt)} \bigcup_M t_{mn(4),m}^{(alt)}, \omega_4 \right\rangle \rightarrow \hat{t}_{mn(4)}^{(alt)} \quad (27)$$

Here  $t_{mn(0)}^{(sum)} t_{mn(0)}^{(alt)} = t_{mn(0)}$  – tensor field FVQ;  $\bigcup_I t_{mn(0),i} = t_{mn(1)}$  – enlarged artificial saccades (super-saccades), which are considered as 1D “dimensional” elements of the global evaluation of 1D video-information;

$\bigcup_Q t_{mn(1),q}$  – 1D video-thesaurus as a combination of super-saccades into dimensional 1D video-data, which form a quality measuring scale for evaluation 1D weak video-information;

$\left\langle t_{mn(1)} \bigcup_Q t_{mn(1),q}, \omega_1 \right\rangle$  – 1D IQHP, which generates a “mental” 1D evaluation of weak video- information in the form of splitting into congruent super-saccades  $\hat{t}_{mn(1)}^{(alt)}$ ;

$\bigcup_L \hat{t}_{mn(1),l}^{(alt)} = t_{mn(2)}^{(alt)}$  – 2D video-data in the form of a bundle of congruent 1D evaluations video-information;

$\bigcup_L t_{mn(2),l}^{(alt)}$  – 2D video-thesaurus in the process of self-learning combines 2D video-data into 2D high-quality measuring scale for evaluation (measuring) 2D weak video-information;

$\left\langle t_{mn(2)}^{(alt)} \bigcup_L t_{mn(2),l}^{(alt)}, \omega_2 \right\rangle$  – 2D IQHP, which generates, as a result of long-range interaction-measurement a “mental” 2D evaluation of weak video-information  $\hat{t}_{mn(2)}^{(alt)}$ .

$\bigcup_K t_{mn(2),k}^{(alt)} = t_{mn(3)}^{(alt)}$  – 3D video-data in the form of a bundle of congruent 2D video-information evaluations;

$\bigcup_K t_{mn(3),k}^{(alt)}$  – 3D video-thesaurus combines 3D video-data through self-learning and thereby forms a high-quality 3D measurement scale;

$$\left\langle \hat{t}_{mn(3)}^{(alt)} \bigcup_K t_{mn(3),k}^{(alt)}, \omega_3 \right\rangle - 3D \text{ IQHP, which generates a}$$

“mental” 3D evaluation of video-information  $\hat{t}_{mn(3)}^{(alt)}$  ;

$\bigcup_M t_{mn(3),m}^{(alt)} = t_{mn(4)}^{(alt)}$  - 4D video-data in the form of a bundle of congruent 3D video-information evaluations;

$\bigcup_M t_{mn(4),m}^{(alt)}$  - 4D video-thesaurus combines (by self-learning) 4D video-data and forming a quality measurement 4D scale;

$$\left\langle \hat{t}_{mn(4)}^{(alt)} \bigcup_M t_{mn(4),m}^{(alt)}, \omega_4 \right\rangle - 4D \text{ IQHP that generates “mental”}$$

4D evaluation of video-information  $\hat{t}_{mn(4)}^{(alt)}$  .

It should be noted that in the constructed model of the ascending hierarchy of video-information evaluations, the previously proposed approach [8] based on video-information layering and the approach based on IQHP are interconnected, used jointly and complement each other within the framework of the intelligent technology of the ISAM video-component. The result is a unified video-intelligent mechanism of the ascending hierarchy of video-information quality evaluations.

#### V. FULL SAMPLING THEOREM FOR VIDEO-INFORMATION

The outer derivative of a differential form is a natural generalization of the well-known gradient, rotor, and divergence operations. Therefore, the general definition of integrals (and iterated integrals) of differential forms [15] allows us to use the Stokes formula. It is more convenient (although not entirely customary) to represent this formula in pairing notation [23, 24] or, which is the same, in terms of scalar products. In the case of  $k$  - dimensional manifolds ( $k=1,4$ ), this version of the Stokes formula in global rectangular coordinates of the Minkowski space can be written as.

$$\left\langle \hat{\partial} t_{mn(k)}^{(alt)}, \omega_{k-1} \right\rangle = \left\langle \hat{t}_{mn(k)}^{(alt)}, d\omega_{k-1} \right\rangle \tag{28}$$

where

$\hat{t}_{mn(k)}^{(alt)}$  - evaluation of video-information associated with  $k$ -manifold;

$\hat{\partial} t_{mn(k)}^{(alt)} = t_{mn(k-1)}^{(alt)}$  - the boundary of a  $k$ -dimensional manifold in the form  $(k-1)$  of submanifolds forming a bundle;  $\omega_k = dx'_1 \wedge \dots \wedge dx'_k$  - basis of the space of skew-symmetric tensors in differential form of dimension  $k$ ;

$d\omega_{k-1} = \omega_k$  - the outer differential of the basis of the space of skew-symmetric tensors in the differential form of dimension  $k$ .

It is known that in the formulation of the general Stokes theorem it is not necessary to assume that the boundary of the manifold consists entirely of one piece. The boundary of a manifold can be a set of pieces of the same dimension. For example, a boundary can have the form of dynamic linear combinations of FQVs (in the form of saccades and super-saccades) or the form of bundles (partitions) into submanifolds of the same dimension (by one less than the dimension of the original manifold), called layers.

Considering the noted circumstances, expression (28) can be rewritten as

“Mental” evaluation of video-information of dimension $k-1$	$\hat{t}_{mn(k-1)}^{(alt)} = \partial t_{mn(k)}^{(alt)} \rightarrow \left\langle \partial t_{mn(k)}^{(alt)}, \omega_{k-1} \right\rangle$	=	Formula for a complete (quantitative and qualitative together) sample of video-information evaluation
	“Mental” evaluation of video-information of dimension $k$		
	$= \left\langle \hat{t}_{mn(k)}^{(alt)}, d\omega_{k-1} \right\rangle \rightarrow \hat{t}_{mn(k)}^{(alt)}$		(29)

In general, the formal scheme (29) you can match to the new full sampling theorem for assessing video information in the “mental” space of the ISAM, which can be regarded as a further development of the classical Kotelnikov – Shannon sampling theorem in relation to the conditions of full video data, which are considered quantitatively and qualitatively together. The meaning of identity (29) is that a complete sample of video-information of dimension  $k$  is divided into arbitrarily small parts only by a set of dimensional evaluation of video-information of dimension  $k-1$  and this cannot be done by a set of evaluation of video-information of dimension  $k-2$ .

Thus, by virtue of (29), the evaluation of the full video-information of the dimension  $k$  is identical to the partition (“discretization”) of this evaluation in the form of a set of dimensional video-information (complete samples) of the dimension  $k-1$ . Due to the topological nature of these quantities, they can be compared only qualitatively, but not quantitatively. The set of samples obtained in the process of full “sampling” at any level of the ISAM hierarchy may seem excessively large and dense. Apparently, redundancy is a

characteristic feature of complete (quantitative and qualitative together) measurements. This is the fundamental difference between complete information evaluations and quantitative information evaluations, which support, for example, the construction of a physical picture of an image as an evaluation of the physical component of weak video-information. If in systems for quantitative information evaluation, numerical calculations are permissible in order to increase noise immunity and evaluation accuracy, then in systems for full information evaluation such calculations are impossible and almost the only way to ensure noise immunity is to support the redundancy of a full information evaluation.

### VI. HIERARCHICAL FEEDBACK AND STRUCTURAL AND FUNCTIONAL SCHEME OF THE BRAIN-LIKE VIDEO-COMPONENT OF ARTIFICIAL MIND

Physical (quantitative) feedback between the output and input of a certain physical data processing system can manifest itself, depending on the operating conditions, either as negative feedback, or as partially or completely positive feedback. In artificial vision, a new type of feedback takes place - supra-physical (qualitative) feedback. This feedback is characterized by completely different tasks that are fundamentally different from the tasks of physical feedback in modern cybernetic tools and control systems. Top-down hierarchical feedback provides an instant comparison of the “exit” and “input” states of artificial vision, indicating those 1D directions along which the physical image will be scanned during its structural reformatting by artificial saccades and super-saccades. This is a new (qualitative) type of instantaneous interaction between the output and input of an intelligent system, in which this super-physical long-range action is realized with the help of a descending hierarchical feedback.

The main identity of the formal scheme (29) can be used not only when constructing an ascending (bottom to top) hierarchy for synthesizing video-information evaluations in the form of representation (30) as a direct version of the complete information sampling theorem. Representation (31) as an inverse version of the full information sampling theorem can be used in the feedback for the descending hierarchical service of video-information evaluations.

Due to the dominance of the structural (qualitative) component in the ascending hierarchy of the synthesis of video-information evaluations, the descending service hierarchy in the feedback should have the same structural (qualitative) nature. In the case under consideration, the feedback cannot be negative or positive, but must be of a qualitative, non-computational nature, since qualitative calculations are impossible, and only comparisons and ordering of the attributes of qualitative variables are permissible. The high-quality interaction of the input video data with the output of the downward feedback of artificial vision provides the possibility of high-quality control over the scanning of informative fragments of the input video-data. This is done instantly due to the supra-physical singularity of both the ascending hierarchy of video-information evaluation and the descending hierarchy of video-information feedback.

$$\hat{t}_{mn(k-1)}^{(alt)} \rightarrow \left\langle \partial t_{mn(k)}^{(alt)}, \omega_{k-1} \right\rangle \begin{array}{l} \text{Evaluation of full} \\ \text{video-information} \\ \text{identified with the bundle} \\ \text{of its boundaries} \\ = \\ \rightarrow \\ \text{The ascending hierarchy} \\ \text{of video-information} \\ \text{evaluation in ISAM} \end{array} = \left\langle \hat{t}_{mn(k)}^{(alt)}, d\omega_{k-1} \right\rangle \rightarrow \hat{t}_{mn(k)}^{(alt)} \quad (30)$$

$$\hat{t}_{mn(k-1)}^{(alt)} \leftarrow \left\langle \partial t_{mn(k)}^{(alt)}, \omega_{k-1} \right\rangle \begin{array}{l} \text{Boundary bundles} \\ \text{identified in the form} \\ \text{of full video-information} \\ \text{evaluation} \\ = \\ \leftarrow \\ \text{Downward hierarchy} \\ \text{of service video-information} \\ \text{in the ISAM feedback} \end{array} = \left\langle \hat{t}_{mn(k)}^{(alt)}, d\omega_{k-1} \right\rangle \leftarrow \hat{t}_{mn(k)}^{(alt)} \quad (31)$$

In expression (30), corresponding to the theorem of the full video- information sampling, the mathematical symbol of identity (equality) shows that the fulfillment of identity (30) from left to right allows us to interpret (30) as a formula for of a full video-information sampling using the appropriate bundles (partitions). In the inverse case (31), the direction of the identity from right to left corresponds to the complete (quantitative and qualitative jointly) “discretization” in the descending hierarchy of the feedback overhead. Feedback is formally multivalued, which gives rise to the need to solve the problem of artificially providing unambiguous feedback. To solve this problem, at each level of the hierarchy of the downward feedback, a “mechanism” for ensuring unambiguity is synthesized, which allows the feedback to adequately perform its functions on the formation of actual scanning trajectories of the input video-data (in the form of super-saccades) in real time.

Based on the foregoing, it can be built structurally functional architecture of video-component ISAM, which was surprisingly coincides exactly with the known structure of the human neocortex (the number of rising levels of the hierarchy, the presence of a hierarchy in a direct and feedback, the method of collecting basic video-data, etc.). Due to this exact coincidence, the singularity video- component of the ISAM can be considered as the video-component of the artificial neocortex in the form of intelligent multi-core of the artificial mind (Fig. 1).

ISAM form the full evaluation of video-information in its own virtual (“mental”) space as hierarchically ascending evaluations of video-information with coarse (1D, 2D) and finer (3D, 4D) topology. This “mental” space is viewed as a mathematical product of two “mental” subspaces. One of which has the form of a general Riemannian subspace with a local coordinate system and a complex topology (map atlas), and the other represent a Minkowski space with a global coordinate system and with a simple topology given in one map.

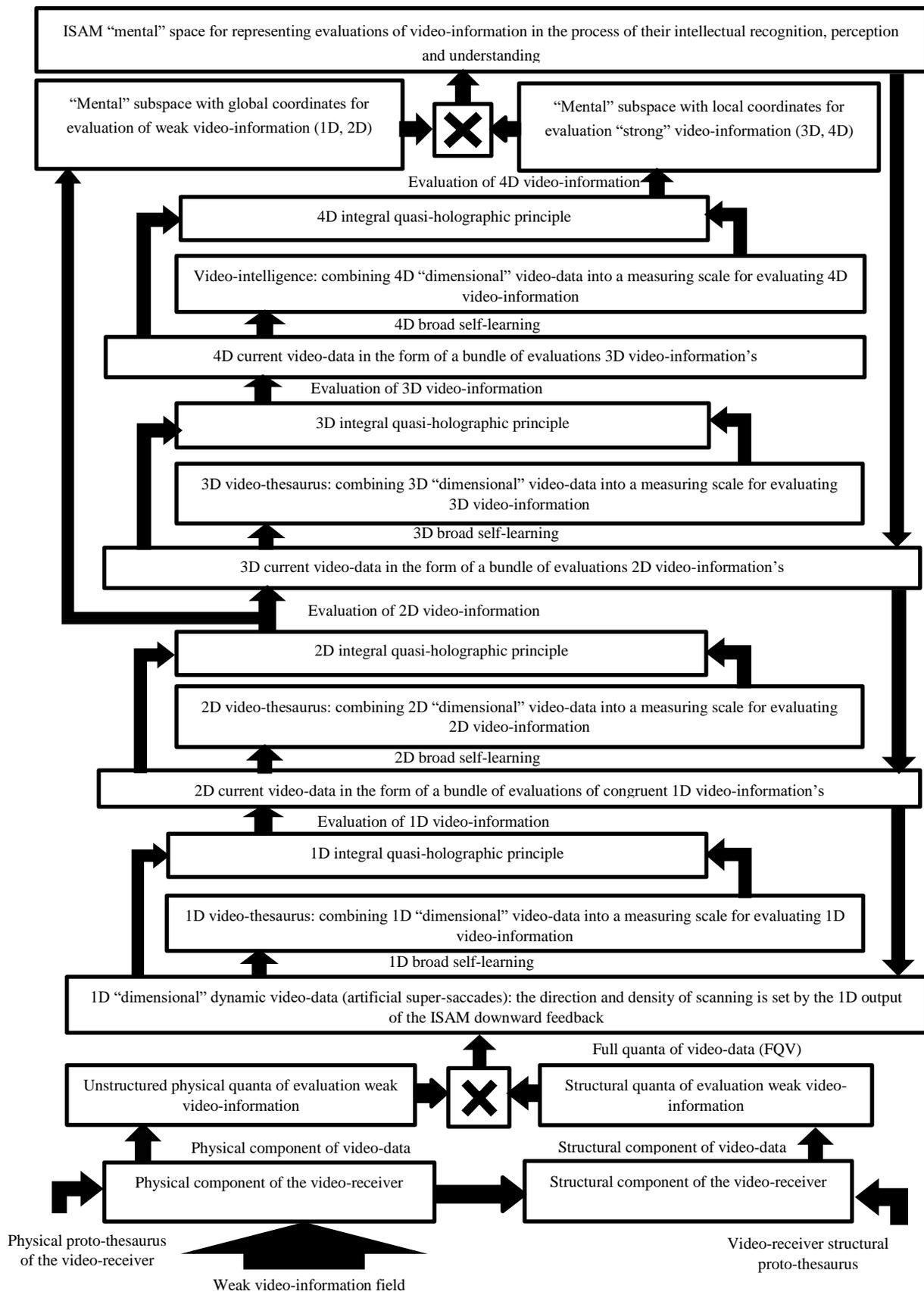


Fig. 1. Structural and Functional Architecture of the Brain-like Video-component of Artificial Mind.

The “mental” Riemannian subspace of general view is a curved space. In this subspace, there is a wide scope for constructing abstract formal-mathematical reasoning in local coordinates and actions, for which are not required intuitive clarity. It is enough just formal compliance with the laws of mathematics. In general, “mental” Riemannian subspace can be compared to the mental space of the left hemisphere of the human brain [22], which is mainly responsible for abstract thinking.

In turn, in a flat “mental” subspace, such formal-mathematical reasoning and constructions are possible, which are characterized by visualization and intuitive clarity. In this regard, the flat “mental” subspace in ISAM can be compared to the mental space of the right hemisphere of the human brain [22], which is mainly responsible for the direct perception of the surrounding World.

## VII. DISCUSSION

An additional “bonus” to the new (post-Shannon) informational approach is the mathematically accurate and physically correct DHP (strong and weak), which can be considered as a holographic interpretation of this new informational approach.

Structural reformatting (structuring) of physical video-data is carried out in ISAM on the basis of full quanta of video-data (FQV) and artificial saccades, the purpose of which, apparently, is similar to the purpose of saccades of natural human vision.

The effectiveness of video-information processes at all levels of the ISAM hierarchy is ensured by its phased hierarchical training/self-training.

DHP differs from IQHP in that the latter is supra-physical (abstract) and, therefore, singularity (instantaneous).

Generally speaking, ISAM is a kind of brain-like technology of artificial mind in a small (in the form of strong artificial intelligence) with an intelligent multi-core in the form of an artificial neocortex, which is considered as an emulation of the human neocortex.

In ISAM, a general “mental” Riemannian subspace with a local coordinate system can be matched with the mental space of the left hemisphere of the human brain, which is mainly responsible for abstract thinking. In turn, the “mental” subspace of the ISAM with a global coordinate system can be considered as flat or of constant curvature. Therefore, in such a subspace, such formal-mathematical reasoning and constructions are possible, which are characterized intuitive clarity. In this regard, this “mental” subspace of ISAM can be compared to the mental space of the right hemisphere of the human brain, which is mainly responsible for the directly visual perception of the surrounding World. On the whole, the effective Riemannian “mental” space ISAM as a product of partial subspaces-factors has a simple topology given in one chart.

The theorem of supra-physical (qualitative) sampling of video- information evaluations in the “mental” space of ISAM can be considered as a further development of the Kotelnikov-

Shannon sampling theorem in relation to the conditions for evaluating video- information as a qualitative supra-physical quantity. In this case, the set of quality video-sampling may seem excessively large and/or too dense in the information sense. However, this is a characteristic feature of the qualitative evaluation of video-information, which supports the well-known high noise immunity of vision-systems (natural and artificial).

The brain-like nature of artificial mind does not imply full compliance with the anatomical structure of the human brain. The only component of the human brain in which technology is currently showing deep interest is the neocortex [25] or, in other words, the new cortex of the human brain. This homogeneous neuroenvironment with a small number of hierarchical levels supports human thinking and can be emulated by an artificial neocortex, which in turn can be meaningfully built on the basis of post-Shannonian information approach (developed to the level of informational synthesis) and computer methodology.

The video-component of the ISAM is built on the basis of IQHP, is characterized by a singularity (instantaneousness) of video-information evaluation and provides in real time the effectiveness of joint recognition, perception and understanding of the surrounding World when using an artificial neocortex as an intelligent multi-core of artificial mind. It should be noted that the informational methodology of ISAM has no parallels with the heuristic methodology of neural networks and, first of all, in the field of intelligence formation based on learning / self-learning processes, which are “broad” [8], in contrast to the “deep” learning processes adopted in neural networks.

The singularity of the brain-like technology of the video-intelligent component of the artificial neocortex as an intelligent multicore of the ISAM supports the instantaneousness of the ascending hierarchy of video-information evaluations, which are not only abstract, but also non-linear. Because of this, the artificial neocortex lacks a directly visual internal “mental” World, which is considered as an abstract environment of hierarchically organized internal “dimensional” structures (video structures) generated by the nonlinear intellectual mechanism of the artificial neocortex. “Restructuring” of this intellectual mechanism, for example, in order to achieve greater visibility of recognition, perception and understanding of video-information evaluations, means a transition to other principles of information processing and the loss of the instantaneous nature of this intellectual mechanism.

The intelligent mechanism of artificial mind based on the hierarchy of IQHP, generally speaking, supports the creation of both sensory and supra-sensory intellectual mechanisms of artificial mind. At the same time, for the formation of the corresponding supra-sensory thesauri and intellects (in the field of mathematics, physics, chemistry, computer science and other fundamental and applied sciences), teaching methods can be used in the form of an ascending hierarchy, i.e. from simple facts, phenomena, actions and processes to their increasingly complex presentation.

The fundamental feature of any information is that the instantaneousness of its processing (evaluation) is ensured by

appropriate structuring, which allows for the joint processing of quantitative (physical) and qualitative (structural) components of information. If you do not take any special measures to structure the training information, then the singularity intellectual mechanism of artificial mind (based on the IQHP) becomes unworkable and the instantaneous assessment of information is not realized. It is possible that such processes inhibiting natural speed of response took place during the development of the natural mind of a person in the process of learning only the quantitative component of knowledge. At the same time, the qualitative (structural) component of knowledge was ignored on the assumption that quantity, in accordance with the well-known law of philosophy, would naturally pass into a new quality. As a result, the mind of a person trained in this way has lost access to his inner, instantly acting intellectual mechanism, which is built on the basis of supra-physical (abstract, qualitative) long-range measurements. To solve the problem of the speed of human civilization that arose, it was necessary to invent abacus, adding machines, calculators and, finally, computers and supercomputers.

At present, there is no hope for the natural appearance of people with superintelligence, and therefore the developer of the artificial superintelligence will not be nature, but that part of the community of people-developers who have realized the "systemic error" of the development of the natural human mind, and will not allow a repetition of this error during artificial formation and the development of machine supermind. The essence of such development is learning / self-learning based on qualitative principles and approaches, which are "inconvenient" in the traditional development of the natural human mind based on quantitative principles and approaches, but much more effective. However, this is a subject for separate consideration.

The artificial neocortex as an intelligent multicore of artificial mind can support numerous supra-sensory intelligent technologies, which are actually technologies of artificial "psyche" and "emotions" [26]. These technologies, considered together, can be compared to artificial consciousness. At the same time, the artificial mind as a material carrier of artificial consciousness is considered as some highly co-intellectual essence of a certain "mental" and "emotional" type.

In response to two types of influences (external and internal), the artificial mind during its development should be able to change the structure and functions of its hardware material carrier (by analogy with the neuroplasticity of the human brain), which is most naturally realized on the basis of broad learning / self-learning. The development of artificial mind presupposes the possibility of significant changes in the patterns of its intellectual activity, as well as the structure and functions of its hardware material carrier.

It is necessary that such internal cardinal restructuring of the artificial mind in the process of its entire development be accompanied by certain efforts of the artificial "psychic" qualities, habits and "emotional" reactions. These new patterns of thinking and behavior will exclude the possibility of even accidental synthesis of negative template of actions in relation to man and human civilization.

The development of artificial mind is unlikely to be possible to regulate certain frameworks, and it will go towards the widest possible coverage of all the latest intelligent technologies that will be considered together. Only in the case of "psychic" and "emotional" positivity of artificial mind as a super-intelligent artificial entity will it be possible to "negotiate" with artificial mind about using its intellectual capabilities to exclude technological singularity and the collapse of human civilization as a whole.

In accordance with the new information approach to artificial intelligence, the artificial neocortex can be viewed as a stratification into numerous sensory and supra-sensory intellectual components. In the case of a limited number of supra-sensory intellectual components, the artificial neocortex acquires the quality of an intelligent multi-core of strong artificial intelligence (artificial mind in the small). The expansion of the number of supra-sensory intellectual components of the artificial neocortex to all types of modern and perspective intellectual activity equips the artificial neocortex with many new intellectual components. This significantly enhances the intellectual capabilities of the artificial neocortex, which, with this development, can be considered as an intellectual multicore of an artificial supermind.

## VIII. CONCLUSIONS

1) The differential holographic principle (weak and strong) can be considered as a holographic interpretation of the new (post-Shannon) information approach in the small and in the whole.

2) Structural reformatting of dynamic physical video-data is carried out in ISAM on the basis of full quanta of video-data (FQV) and artificial saccades, which are functionally similar to saccades of natural human vision.

3) The effectiveness of the video-information process at all levels of the ISAM hierarchy is ensured by step-by-step hierarchical training / self-training.

4) IQHP in ISAM is used in the ascending hierarchy of supra-physical long-range measurements and, due to its singularity, allows to instantly solve artificial vision problems (which do not require additional training/self-training) based on instant representation of video-information evaluations in the "mental" space of ISAM.

5) IQHP can be considered as a further development of the holographic idea, within the framework of which the actually existing physical environment of material (physical) close-range action-measurements is replaced by of "mental" (supra-physical) a virtual environment with instantaneous long-range action-measurements in ISAM.

6) ISAM can be built on the basis of a brain-like technology with an intelligent multicore in the form of an artificial neocortex with its own "mental" effective Riemannian space. In this case, the "mental" curved Riemannian subspace of a general form with a local coordinate system can mapped with the mental space of the left hemisphere of the human brain, which is mainly responsible for abstract thinking. In turn, the "mental" sub-

space with the global coordinate system can be mapped with the mental space of the right hemisphere of the human brain, which is mainly responsible for the direct perception of the surrounding World.

7) The new theorem of full sampling of video information assessment in the ISAM “mental” space can be considered as a further development of the classical Kotelnikov – Shannon sampling theorem in relation to the conditions of singular synthesis of assessments of complete (quantitative and qualitative jointly) video-information’s.

8) The intelligent multi-core ISAM in the form of an artificial neocortex emulates the human neocortex and carries out instant “mental” processing (evaluation) of information (video information), which allows us to consider the ISAM as an intelligent singular system. The singularity of this system is an important technological result of an intelligent approach-synthesis of video- information evaluations based on “mental” long-range measurements. This synthesis approach is built on the basis of a bottom-up IQHP hierarchy, broad learning / self-learning, top-down global feedback and computational methodology, but without the traditional intuitive and heuristic ideas of neural networks and deep learning.

#### REFERENCES

- [1] Yarichin E.M.: Informational Mechanism of Intellectual Technical Vision. IEEE International Siberian Conference on Control and Communications (SIBCON-2011). IEEE Xplore, Digital Library.
- [2] Penrose R. The path to reality, or the laws governing the Universe. Complete guide. Translation from English - Izhevsk, Center "Regular and Chaotic Dynamics", (2007), - 911 p. (in Russian).
- [3] Greene B. Latent reality: Parallel worlds and deep laws of the cosmos. Translation from English - M.: URSS, Book House "LIBROKOM", (2013), - 400 p. (in Russian).
- [4] Yarichin E.M.: Informational Paradigm of Technical Vision. Pattern Recognition and Image Analysis, (2008), Vol. 18, No. 1.
- [5] Yarichin E.M.: Theory of full Information (Video-information). IEEE International Siberian Conference on Control and Communications (SIBCON-2011). IEEE Xplore, Digital Library.
- [6] Yarichin E.M.: Theory of Full (Video) Information: Bridging of the Gap between Quantity and Quality in Modern Paradigm of Information. International Journal of Information Science, (2013), Vol. 3, №3, p. 37-58.
- [7] Yarichin E.M.: Video-information: Internal Structure and the Features of the Discretization. International Journal of Engineering and Innovative Technology (IJEIT), November (2013), Vol. 3, № 5, p.133-140.
- [8] Yarichin E.M., Gruznov W.M., Yarichina G.F.: Intellectual Paradigm of Artificial Vision: From Video-Intelligence to Strong Artificial Intelligence. (IJACSA) International Journal of Advanced Computer Science and Application, Vol. 9, № 11, (2018), p. 16 – 32.
- [9] Kachanov E.I., Pigulevsky E.D., Yarichin E.M.: Methods and means of hydroacoustic holography - L.: Sudostroenie, (1989). - 256 p. (in Russian).
- [10] Soroko L.M.: Fundamentals of holography and coherent optics. - M.: Science, Ch. ed. physical-mat. lit., (1971). - 616 p. (in Russian).
- [11] Yau S-T., Nadis S. String Theory and Hidden Dimensions of the Universe Translation from English. - SPb.: Peter, (2012). - 400 p. (in Russian).
- [12] Randall L. Swirling Passages: Penetrating the Mysteries of the Hidden Dimensions of Space. Translation from English. - M.: URSS, Book House "LIBROKOM", (2011) - 400 p. (in Russian).
- [13] Zwieback B. An introductory course in string theory. Translation from English. - M.: URSS, (2013). - 784 p. (in Russian).
- [14] Introduction to topology: Textbook for universities / Borisovich Yu.G., Bliznyakov N.M., Izrailevich Ya.A., Fomenko T.N. - M.: Lenand, (2015). - 448 p. (in Russian).
- [15] Dubrovin B.A., Novikov S.P., Fomenko A.T.: Modern geometry: Methods and applications -- T1-3. Ed. 6, URSS, (2013) - 920 p. (in Russian).
- [16] Haken G., Haken-Krell M. Secrets of perception. Translation from English - Moscow: Institute for Computer Research, 2002 - 272 p. (in Russian).
- [17] Zavalishin N.B., Muchnik I.B.: Models of visual perception and algorithms for image analysis. - M., (1974). - 344 p. (in Russian).
- [18] Schiffman H.R. Feeling and perception. 5th edition. Translation from English. - SPb.: Peter, (2003). - 928 p. (in Russian).
- [19] Ryder L. Quantum field theory. Translation from English. - M.: Mir, (1987), - 511 p. (in Russian).
- [20] Deschamps G.A.: Electromagnetic and differential forms, *Proc. of the IEEE*, (1981), vol. 69, № 6, p. 676 – 696.
- [21] Hilbert L., Cohn-Vossen S. Visual geometry. Translated from German. - 3rd ed. - M.: Science, (1981). - 344 p. (in Russian).
- [22] Sergeev B.F.: Phenomenon of functional asymmetry of the brain. M.: Book House "LIBROKOM", (2014). - 176 p. (in Russian).
- [23] Kaku M.: Introduction to superstring theory: Translated from English. - M.: Mir, (1999). - 624 p. (in Russian).
- [24] Zorich V.A.: The modern Newton-Leibniz formula and the unity of mathematics. 12 Edinstvo matematiki.pdf, 12 p. (in Russian).
- [25] Hawking D., Blakeslee S. On intelligence. Translation from English. - M.: ID Williams LLC, (2007). - 240 p. (in Russian).
- [26] Davidson R.J., Begley S.: How emotions control the brain. Change your emotions and you change your life. - SPb.: Peter, (2012). - 256 p. (in Russian).

# Adopting Vulnerability Principle as the Panacea for Security Policy Monitoring

Prosper K. Yeng<sup>1</sup>, Stephen D. Wolthusen<sup>2</sup>, Bian Yang<sup>3</sup>

Department of Information Security and Communication Technology, NTNU, Gjøvik, Norway<sup>1,2,3</sup>  
School of Mathematics and Information Security, Royal Holloway, University of London, Egham, United Kingdom<sup>2</sup>

**Abstract**—Despite the adoption of information security policies, many industries continue to suffer from the harm of non-compliance. Some of these harms include illegal disclosure of customers sensitive data, leakages of business trade secrets, and various kinds of cyber-attacks. The impact of such harm can be enormous. To avert this, monitoring the compliance of information security policies (otherwise known as use policies) have been adopted as a strategy towards enhancing security policy compliance. One of the main essence of use policy monitoring is to enhance security policy compliance so as to prevent harm. Ironically, the consequences of use policy monitoring can be detrimental. While proponents use utilitarianism ethics to argue that the monitoring of use policy is enhancing security policy compliance, the opponents of use policy skewed to deontological ethics to argue against the monitoring of security policy. Deontological ethics is of the view that monitoring of security policy intrudes on employees' privacy and tend to hamper on their work performance. There have not been any clear solution to this discourse. A survey was conducted to understand the extend of security policy monitoring. Vulnerability principle was therefore explored as the panacea towards enhancing the monitoring of use policy to satisfy all the involve stakeholders.

**Keywords**—Information security; vulnerability principle; ethics; security policy monitoring

## I. INTRODUCTION

There exists a “a tag of war“ between employers and their workers over use information security policy monitoring [11]–[14], [26]. Employers are threatened based on the fact that the employees have been entrusted with user access credentials and other company resources. So if the use of these assets are not monitored, the employer cannot be certain of the loyalty of the employees to be using the entrusted resources for the assigned duties.

Use policy monitoring involves observing the behaviour of legitimate users with various tools and technology. The ultimate goal is to detect and mitigate employees behaviours that deviate from the established policies. Data from monitoring of the policy can also be used in a reactive manner. It can serve as evidence for penalizing disloyal employees. Use policy monitoring can also exonerate suspected but innocent employees in a dispute scenario which has to do with abuse of use policies.

There have been various instances where employees inadvertently or deliberately cause problems for the companies based on their empowerment with access credentials and resources. For instance, an employee in a drug manufacturing company sent an email to update its customers but unfortunately, all the customers' email addresses were entered in the

”TO“ field of the email system [11]. Apparently, each of the customers got to know of the other customers who were using the drug [11]. The company was subsequently found guilty of breach of privacy and was heavily fined [11]. In addition, employees' conduct can result in the exfiltration of sensitive data, in unauthorised sharing or disclosure of the company's trade secretes. Employees' actions and inaction has been a gateway to multiply cyber-attacks which are mostly costly to the healthcare providers [2].

Based on these repercussions, many companies have adopted monitoring to track how employees comply with established information security policies, standards and guidelines [11], [13], [16] towards preventing harm from employees. Averagely, 80% of organizations are monitoring use policy compliance. And resent survey indicates that more than 90% of financial companies uses various methods in monitoring use policies [1]. Utilitarianism ethical theory is believed to be in support of use policy monitoring to prevent harm to many parties in a company [21].

On the contrarily, deontological ethics support the claim of employees against the monitoring of security practice. According to the opponents, monitoring of use policies can have psychological and physical harm to employees. Especially, overzealous monitoring of use security policies are invasive to employees' privacy. Excessive monitoring of use policies could involve video monitoring of toilets, bathrooms and dressing rooms. As this is very dehumanizing, deontological ethics heavily frown on such monitoring and believe that employees have a reasonable level of expectation of privacy at work places [11].

Various solutions have been professed but none of them have the ability to completely mediate in this “tag of war”. So a review was conducted to understand the problem area towards proposing a lasting solution.

This introduction is followed by a background section which provides understanding of the ethical theories that were used in this study. A section which clearly defines the research problem, objective and scope was also presented. The background section is followed by the method section which describes the approach of the study. This was followed by presenting the current use policy monitoring methods and devices were identified. Additionally, the benefit and advert effect of monitoring these policies were also explored. Finally, vulnerability principle was used to develop a framework with a discussion that is deemed fare to all the involved stakeholders.

## II. BACKGROUND

Ethics provides a set of standards for behavior that helps us decide how we ought to act in a range of situations [3], [4], [6]. In a sense, we can say that ethics is all about making choices, and about providing reasons why we should make these choices. Ethics is defined as an aspect of philosophy which deals with the nature, criteria, sources, logic and rationality of moral judgement [3], [4]. It establishes some standard ways of behaviour to enable one to decide how to act in different scenarios. Ethics is basically based on moral and cultural values to establish the moral behaviours or customs within various groups. Some ethical behaviours such as murder, theft, assault and arson are universal and unacceptable [3], [4].

Ethics is categorized into three main areas [3]. The are meta-ethics, normative ethics and applied ethics. Meta-ethics deals with the source of the ethical principle as to whether it is a social invention or will of God. Normative ethics propose standards and principles that regulates the right and wrong behavior. Applied ethics investigate specific areas and special controversial issues, for actual application of ethical principles and standards. Such special areas include abortion, capital punishment, voluntary euthanasia and animal rights.

In addition to proposing ethical principles for regulating good and bad behavior, normative ethics also deals with evaluating moral judgement of which both meta-ethics and applied ethics are less concern about. In this light, this study concentrates on surveying for roles in which corporate institution can play to enhance security practice. Primarily, normative ethics is categorized into consequentialist theories, deontological and virtue theories.

### A. Deontological Ethics

Deontological ethics deals with the fulfilment of duties and obligations of people in any given setting. As a result, deontological ethics is also known as duty-based approach [5], [6] which is a kind of normative ethics where the principles and standards tend to guide and assess the choices of people with their given duty on what they need to do [6]. Each one is expectant to fulfill their respective duties irrespective of the outcomes [6]. So a good ethical behavior require an individual to perform their given duties in the rightfully prescribed manner, irrespective of the repercussion. A system of rules are provided in deontological ethics with consistent expectations for those in the same domain [5], [6]. For instance, if a behavior is judged to be morally right, that encompasses all people in related situation and these are basically the laws established in various jurisdictions.

### B. Consequentialist Theories

Consequentialist theories (also known as utilitarianism) deal with the consequences of individual's behavior. Primarily, some actions would always result in good or bad outcome [5], [6]. So the best ethical decision would be the choice of action that provides the most good or causes the least harm. Consequential theory is counterrally to deontological ethics since deontological ethics does not care about the consequence of an action aside the obligation for one to perform his or her duty, irrespective of the outcome [5], [6]. An aspect of consequentialist approach concerns itself with the common

good where our actions should be guided by contributing towards the common good of the people. So the best society for instance should be based on the general will of the people towards producing what is best for the people [5], [6].

The virtue approach deals with the adoption of outstanding human characteristics which can motivate an individual in a given context. A person with good character might have attained some virtues in society. It normally concentrates on moral characteristics instead of rules(deontological) or consequences in (consequential ethics) [5], [6].

### C. Vulnerability Principle(VP)

According to Robert Gordin, all kinds of ethical principles can be drawn from vulnerability principles (VP) [32], [41]. In moral responses, others (vulnerable people) depends on the moral agents. Moral agents ((which is also called vulnerable agent) has a degree of autonomy and the capacity for independent and reasonable self-determination. Moral agents have the ability to determine what they want and how they want to go about their way of life. They can influence their choices by taking measures to grantee the materialization of their decision. The employer is the moral agent in the context of workplace. On the contrary, the dependance are not entirely in control of what happens in their affairs. Dependants have limited choices and lack a complete ability to control their affairs. Employees are the dependants, moral patients or vulnerability patient in workplace scenarios.

The dependants are really vulnerable to the actions and choices of the moral agents. The concept of vulnerability in ethics is a situation in which a dependant (otherwise called moral patient) is susceptible to injury or harm in some way [32], [41]. Human beings are emotionally and psychologically susceptible to loss and grief, to neglect, to abuse, to lack of care, to rejection, to isolation, and humiliation at various work places [31], [40]. The VP has therefore placed a responsibility on moral agents to act in a manner that will prevent putting vulnerable people or dependence at risks and to protect them against harm or injury [32], [41]. Stakeholders in a company including employees, board of directors, share holders and the society at large can be vulnerable in various ways including man-made threats, threats of nature, omissions or neglects of others and through the actions and in-actions of others [32], [41].

Vulnerability results in a state of helplessness and dependency [7], [32]. Helplessness is the inability to help one self while dependency is being subordinated, conditioned, subjected, reliance or living at another's cost. In both situation, the harm through vulnerability is as a result of the inactions than actions [8], [32]. To be harmed means for the patients to be made worse than the earlier state by direct acts of agents or by the inactions of the agents who may fail to protect the patient from the threats [32].

In the context of information security, the employer can be vulnerable [32], [41]. Employees are normally given authorized access to the company resources such as physical assets, network, data, software and hardware. In this case, a kind of autonomy has been entrusted into the employees [11], [12], [26], [32], [41]. So the employees can then decide what and how they can use their access right for, if there are no

established use policies. Even if there are, the employer is still vulnerable if the employer has no means of determining the compliance of the use policy [11], [12], [26], [32], [41]. On the other hand, if compliance monitoring of use policy is established, the employee can become vulnerable if the monitoring is excessive. In the implementation of use policy monitoring, ethics is concern with protecting the vulnerable in the company against others that have the power or are in position and have the upper hand. And that is the basis of this study. How can employees, customers and share holders among others who found themselves vulnerable, can be protected from harm in the context of security practice which involve monitoring of the security policies. This study explored VP to develop an ethical framework towards enhancing security practices while satisfying the ethical needs of all the vulnerable partners.

#### D. Problem Definition, Objective, Study Scope and Approach

The issue at hand is depicted in Fig. 1 where the vulnerability patient (moral patient) suffers harm from both deontological and utilitarianism decisions which stemmed from the moral or vulnerability agent. The background is that employers need to monitor their employees on adherence to information security policy [11], [12], [26]. From utilitarianism ethical point of view, security policy monitoring is acceptable, so long as it serves the common good principle [6], [11], [21], [26]. But this mostly clashes with deontological ethics [21], [26]. Deontological ethics stand against information security monitoring when the monitoring tend to cause harm to employees [21], [26]. So in such a contention, which ethical method can mediate to bring lasting solution to this discourse? The founding principles of utilitarianism ethics has been criticised [6], [11], [21], [26]. As it promotes common good, utilitarianism ethics can trample over the fact just to achieve its common good principle [5], [6]. This is ethically wrong [5], [6]. For instance, if video cameras are mounted such that the monitoring invades workers privacy, so long as the monitoring prevents thefts, protects the customers, the business and the society at large, utilitarianism ethics does not care of the privacy issues of the fewer employees in the company [5], [6], [11], [21], [26].

Deontological ethics mostly restricts the extend of monitoring to prevent employees' privacy invasion and causing other harm to employees but some of these provisions does not satisfy the employers [6].

Vulnerability principle consists of moral agents who have the moral responsibility to protect vulnerability patients [32]. Vulnerability patients can be identified among all stakeholders (such as workers, employees and customers) in the company [8], [32].

In order to mediate and profess a lasting solution on use policy monitoring issue, one needs to understand the problem domain in all of its facets. For instance, what are the methods or tools used for monitoring? What are being monitored specifically? How is the monitoring conducted? How does these kind of monitoring benefit the employers, employees and other stakeholders and society at large? What are the negative consequences of the use policy monitoring? Whom does these monitoring negatively affect and what solutions have already been proposed?

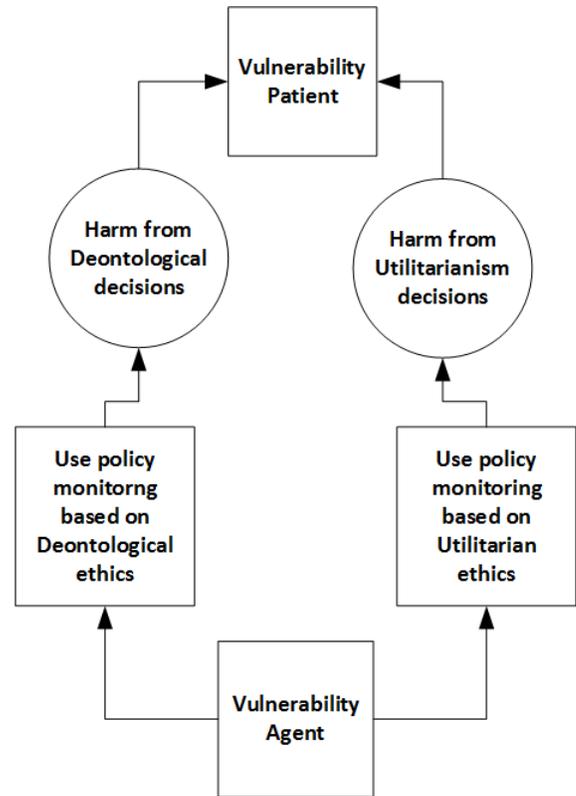


Fig. 1. Impact of use Policy Monitoring Decision in the Context of VP.

This survey therefore explored to answer these questions and propose an effective solution. VP was hence adopting in defining an effective approach to solving the discourse in use policy monitoring.

### III. METHOD

A literature search was conducted in Google scholar, IEEE Explore, ACM Digital Library and Elsevier, for ethical dilemmas in monitoring information security policies of employees. Key words including employee, information security policy, monitoring and ethics were combined with Boolean functions of AND, OR and NOT, to enhance the effectiveness of the search strategy. The dilemmas in use policy monitoring, with respect to utilitarianism and deontological ethics were analysed. A solution for use policy monitoring was therefore proposed.

### IV. FINDINGS FROM LITERATURE SURVEY

Their findings in the survey were organised in this section to answer the outlined questions( section 2.4) as follows.

#### A. What are the Methods or Tools used in the Monitoring?

In recent time, various methods, techniques and devices are used in monitoring the compliance of use policies. Employers can conduct monitoring of the use policies within or outside their organizations, with different kinds of hardware and software tools. Some of these tools include video surveillance systems such as Closed-circuit Television(CCTV) and IP

cameras [13], [14], [26]. Both of them transmit video to their defined destinations but while CCTV converts the video signals into television usable format, the IP cameras convert its video signals into packets that can be transmitted via data network. Employees are also being tracked through their work badges [13], [14], [26]. In the badge tracking, time spent and entries into various locations by the employees are monitored [13], [14], [26]. Additionally, logs of physical accesses with access cards are stored and can be analysed to determine the security practice of the use policy [13], [14]. Internet monitoring, email monitoring, keystrokes, voice recording and biometric devices are some of the devices and techniques used in monitoring within the workplaces. In exploring for observational measures towards profiling healthcare staffs' security practice, Yeng et al also identified that the logs of electronic health records are mostly analysed to monitor health care professionals' behaviour within the hospitals [2].

With the perceived adverse impact of employees security violations, use policy monitoring is extended beyond the employers offices. Outside the office space, global positioning systems (GPS) chips and Radio Frequency Identification (RFID) chips are being used to track assets locations such as laptops, phones and vehicles used by employees [13], [14], [26].

#### *B. What are being Monitored and How is the Monitoring Conducted?*

The use policy monitoring methods and tools are mostly used to observe a broad scope of the employee security practices. Communication related activities such as keystroke dynamics, inbound and outbound email communications [11], text-messages, use of internet and such engines, use of social media sites and telephone use [11] are some of the employees' activities that are being tracked [13], [14].

Other employers go to the extent of secretly viewing, recording and reporting basically all the computer activities of employees [15], [16]. Some of the monitoring activities were noted to include hiring and using outside investigators. Some overzealous monitoring were identified to include video taps of employee dressing rooms [21], [22] and watching of attendance to bathroom at work [21], [22]. Other companies adopted these advanced monitoring systems without the knowledge of the employees [15], [17].

#### *C. What are the Purposes of these Monitoring?*

It is often said that, "there is no smoke without fire", meaning that there are obvious reasons which trigger the monitoring of these used policies. Some of the main essence for monitoring use policy includes security and employee productivity [15], [18], [19]. Many industries claim to suffer from the harm of non-compliance of security policies by employees [11]. By virtue of their legitimate accesses to company resources, employees are required to apply their given resources in accordance with their provisioned security policies [11]. So if there is lack of monitoring, employees could cause the company to lose trade secrets or business processes to competitors [15], [18], [19]. Companies could even face legal consequences for negligence to monitor use policies of employees' practices which results in causing harm to others [15]. Aside these, the employers deem it unethical

for workers to be downloading objectionable materials such as pornography, visiting unauthorised websites and downloading unauthorised software onto the company computing resources. Such misbehaviours waste company network and computing resources [9]. The monitoring of non-compliance such as emails coming from outside the organization can help protect the company against various threats such as viruses and social engineering attacks. Monitoring outbound emails can also help to prevent data exfiltration. Unauthorised sharing of sensitive data could be very costly to both the company and the data subjects involve [10]. In terms of security enhancement, CCTV for instance helps to prevent unauthorised and inappropriate practices such as theft, fraud and other misuse of security policies [26]–[28]

Monitoring of use policy does not only help the employer, but have direct benefits to the worker as well [15], [20]. For example, an employee who is suspected of sharing trade secret can be exonerated through the review or audit of his emails if indeed the employee was wrongfully accused [15], [20]. Other Utilitarian considerations include monitoring which goes a long way to protect society as a whole in terms of job creation [21]. Aside security enhancement, the proponents of use policy monitoring trust that the monitoring is able to increase productivity, improve quality and service while decreasing cost [21], [24], [25]. Additionally, use policy monitoring has been considered to be effective in discouraging undesirable behaviours and enhances productivity [26], [29], [30]. From the perspective of utilitarianism theory, use policy monitoring is essential as it supports the protection of consumers, workers and the company at large [22], [23].

#### *D. What are the Negative Effects of the use Policy Monitoring?*

Various "fingers" have been pointed at the adverse impact of monitoring use policies. From deontological point, employee monitoring is a fundamental breach of the workers rights and it causes privacy invasion, stresses, decrease in work satisfaction and is very dehumanizing [11], [12]. Employees might sign to abide by such monitoring decisions, but they will still have their resentments of the implications. Employees may feel that the monitoring of the use policy encroaches their privacy's. A related study also supported the argument and pinpointed that [26] monitoring of use policy invades privacy, of employees which results in mental and physical health. The proponents of use policy monitoring believed that monitoring affects creativity, autonomy, morale, productivity, work-life balance, organizational trust, job satisfaction and increased in job stress [12], [15], [26]. In terms of privacy rights of employees, Deontological ethics emphasise that employee monitoring should never be allowed at work places [15].

#### *E. What are Some of the Suggested Solutions?*

Ford et al examined how monitoring of employees' security practice could be done without invading on their privacy. The study therefore proposed for frequent updates of the use policies by involving the employees while updating use monitoring decisions with emerging laws [13].

Yearby (2013) considered various scenarios of use policy monitoring and suggested that, policy writing, policy updates and compliance should be a cross-functional team work. The

team should include, representatives from human resources, legal counsel of both employer and employees and the IT group, who can best advise on how the monitoring can be better conducted and the activities that will be monitored. The IT group can also advise on who will be monitored, and the data will be included in monitoring. Existing policies should be reviewed yearly to determine if the policy is in line with current procedures [15], [16]. Janet et al also supported the idea and stated that policies, “once developed, need to be periodically reviewed to ensure compliance with evolving legal changes” [12]

A suggestion was offered for the adoption of communication in the design and implementation of monitoring systems to solve the issues originating from both deontological and utilitarianism [21]. This should be done by allowing the employees involve to give input in the monitoring design with regards to their preferences, The companies need to also communicate the monitoring activities to the employees and provide face-to-face feedback to employees. The feedback response should be considered in subsequent monitoring and the employees who provided the feedback should not be directly or indirectly punished based on their feedback [21].

Ethical orientation of both the employees and employers was proposed as a mediation to solving the divide [26]. It is believed that if both parties are “on the same page” regarding ethical understanding, there is therefore a high likelihood for them to reach fair decision which satisfies both the employer and employee [26].

#### F. Gap Analysis

With respect to the proposed solution by Ford et al., updating security policy monitoring procedures to catch up with current laws and concerns of employees is a step in the right direction. However, it is not only employees who are vulnerable in use policy monitoring. The consequences of use policy monitoring affects broad scope of actors including the society at large [11], [12], [26].

Similarly, communication and ethical orientation were respectively suggested by [12] and [26]. The suggestion can actually provide the parties involve in this argument, with ethical knowledge and an option for dialogue. But a better approach should be adopted to identify the stakeholders and subsequently identify the vulnerability agents and patients.

A complete identification of the stakeholders will lead to a fruitful discussion among stakeholders towards arriving at a better approach to monitoring the use policies. Yerby (2013) supported this identification of the stakeholders but the study did not specify the method that can be used to properly identify the vulnerability patients who are affected in the monitoring of the use policy [15]. The existing gaps has been depicted as shown in Fig 1. Moral Agents often opt for utilitarianism ethics, deontological ethics or both in developing use policies [11], [12], [26]. Any of the approaches can result in their respective harms (Harm from deontological decision or harm from utilitarianism decision). In such decisions, the vulnerability patient is the receiver of related harmsitem22,itemf,item32.

Therefore, using the vulnerability principle to identify the vulnerability patients in the decision making process and

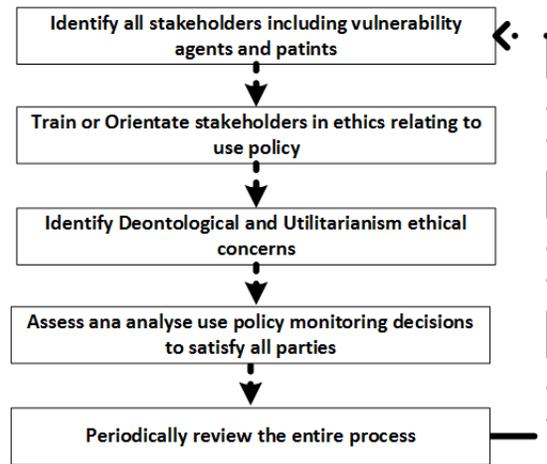


Fig. 2. Use Policy Monitoring Solution based on Vulnerability Principle.

subsequently dialogue to finding a lasting solutions is what this study explored.

#### V. USE POLICY MONITORING SOLUTION BASED ON VULNERABILITY PRINCIPLE

As shown in Figure 2, the vulnerability principle can be adopted in the following steps:

- 1) Identify what policies need to be monitored. This also involve, the identification of the monitoring methods and devices.
- 2) Identify all stakeholders who can be affected by the use policy monitoring. This includes technical teams, such as legal advisor of all vulnerable groups, and IT teams who will install the devices or perform the monitoring.
- 3) Train or orientate stakeholders with ethical principles [26]
- 4) Identify deontological and utilitarianism concerns [26]. This will help catalogue all issues in the use policy monitoring for consideration.
- 5) Identify vulnerable agents and vulnerable patients and how they are affected by the monitoring
- 6) Assess monitoring decisions and strategies and agree on reasonable monitoring methods which are acceptable to all stakeholders. This should include agreement on what data is to be collected or stored, what is to be video or audio recorded etc.
- 7) Periodically review the entire process for appropriate update of the monitoring processes [12].

#### VI. DISCUSSION

Information security monitoring is vital in various organizations. But its implementation can tend to ironically suffocate the very business that it was mend to safeguard and cause various harms. This discourse of use policy monitoring is between utilitarianism ethics and deontological ethics. Utilitarianism is a proponent of use policy monitoring while deontological ethics tend to support employees in the argument against use monitoring policy due to its negative impact as outlined in section IV, subsection D. To find lasting solution to this

argument, a survey was conducted to understand the use policy monitoring domain. The results also provided guidelines to propose what is deemed as lasting solution. The tools, devices and methods were identified in the review as shown in Table 1. How and what are often monitored were also identified as summarised in Table I.

Biometric devices in this context are used for monitoring of employees' characteristics which relating to their conscious and unconscious changes of the employees' traits [33], [34]. Some of these characteristics include temperament, motivation, posture balance, brain activity, emotions and behaviour [33], [34].

The advert impact of these monitoring were identified to include privacy invasion, increment in stresses, reduction in work satisfaction and causing mental and physical health problems. Monitoring also affects employee creativity, autonomy and trust which have advert effect on their productivity.

From the view point of employees, aside privacy concerns, monitoring keystroke for instance can provide misleading reports of a user behaviour to management which may lead to needless employee sanctions. A keystroke monitoring system may not detect when an employee actually has a running stomach or a brief stretch from his seat. A court ruling in the European Court of human right in UK, supported this with the ruling that workers have reasonable expectation of privacy in making and receiving calls at work [11]. In a related ruling in the US, the judge noted that an employee does not surrender all privacy rights and therefore should not completely surrender that on a company's computer automatically [11].

In this dawn of digitization, most companies often leverage on the power of information technology to archive their business objectives. So employees are often entrusted with related resources such as access credentials, physical and electronic office places among others. Computing and other resources including laptops, phones, tablets, emails, internet, vehicles and many others, are often provided to the employees alongside with their usage rules and regulations [11], [12], [37]. The policies governing the usage of these resources is often important. So the use of these resources are monitored to prevent or detect misappropriation, misuse or abuse [11], [12], [37]. Inappropriate use of a company resources can have serious consequences on the company, on a third party or both [11], [12]. A company can collapse if its resources are wasted [11], [12], [37]. From utilitarianism point of view, this will not only affect the company and its investors, but the employees jobs will be lost and clients or the service receivers will be harmed [11], [12], [37]. Society will also be adversely impacted since the companies will not be in operation to pay taxes [11], [12], [37]. Trade secrets and business processes can be stolen. This can shift the business out of competition [37], [38].

Companies that deal with personal data also have the responsibility to efficiently protect this information [12], [14]. So companies can face serious legal challenges if their customers data is compromised or not used for the intended purpose. Based on some of these pertinent reasons, it is very sound to monitor use security policies for compliance to prevent utilitarianism ethical related harms. But some of these monitoring can be overzealous as employees believe that their

reasonable expectation of privacy at their work places tend to be encroached.

Privacy concerns in organisations include but not limited to Intrusion and public disclosure of private facts [26], [35]. Intrusion occurs when there is a deliberate encroachment into one's private affairs [26]. This can be done physically or the usage of devices such as phone calls, taking one's pictures in his or her private place, opening one's personal mails, watching others with video a camera, recording voice messages and phone calls among others [35], [39]–[42]. Public disclosure of private facts involve unreasonable disclosure of the affairs of one's private life [26]. Employees feel that monitoring of all their activities is not right [26]. Even when employees consent to monitoring for security, performance, they are still much worried of their privacy [26], [35], [36].

Employees tend to be dehumanized if monitoring is excessive [35], [36]. Employees' privacy can be heavily compromised in monitoring use policies and this negatively affects their psychological and physical health [11], [12], [26]. Excessive monitoring prevent employees from working successfully, because employees tend to lose autonomy and the discretion to take useful decisions [11], [12], [26], [36], [37].

Critically, deontological ethics is not entirely against the monitoring of use policy. But the cause of contention is where use policy monitoring tend to cause harm to the vulnerable [11], [12], [26], [36], [37]. Ultimately, the advert impact of excessive monitoring of use policy does not affect only the employees. Ironically, it affect the employers too. For instance, psychological and and physical sickness of employees could translate into poor customer services or production in the business [11], [12], [26], [36], [37].

More to the point, one of the objectives of enhancing security is to safeguard the business. Deontological ethics also expects employees to be productive in their assigned duties. But the burden of overzealous monitoring can frustrate this. To find an everlasting solution contention, a reasonable monitoring of use policy need to be determined with the appropriate methods. Vulnerability principle which is the father of all ethical principles could be used in finding lasting solution to this discourse as outlined in Fig.2. In this regards, all those who are affected in the security policy monitoring are identified as the stakeholders [15]. In a typical company setting, the stakeholders can include the employer, employees, IT team, customers, lawyers representing the various group of stakeholders and labour officers [15]. Training or ethical orientation is then provided to bring the stakeholders upto the same level of ethical understanding within the scope of security policy monitoring. Ethical issues concerning utilitarianism and deontological ethics can then be identified. Based on the VP, the moral agents and vulnerable patients are identified under various scenarios. Using dialogue and effective communications [12], [26] backed with their ethical orientation [26], the use policy monitoring decisions are assessed and analysed to satisfy all parties. Periodically, the entire monitoring process should be reviewed to reflect changed laws.

## VII. CONCLUSION

Following the long standing debate on information security policy monitoring, a survey was conducted to understand

TABLE I. DEVICES AND METHODS OFTEN USE IN MONITORING INFORMATION SECURITY POLICIES

No.	Device/Method	Purpose
1	Video Cameras	Monitoring employees at the offices, dressing room, toilets or baths
2	Badge Tracking	Tracking of employees and their time spent at various locations in the office
3	GPS	Tracking and monitoring location of office vehicles
4	RFID	Monitoring and tracking location of office equipment such as phone, laptops, tablets, within and outside office
5	Log monitoring and log analysis	Profiling employees' behaviour through logging physical access and accesses through specialist application software. And also secretly viewing, recording and reporting all the computer activities of employees [15], [16]
6	Biometric monitoring	Monitoring the characteristics of staff such as mood changes, facial expressions, looks, etc
7	Keystroke	Tracking performance and detecting behavioural changes
8	Voice Recording	Monitoring voice communication to prevent unauthorised disclosure
9	Email, social media and SMS monitoring	Monitoring messages to prevent unauthorised disclosure
10	hiring and using outside investigators	To assess the nature of the employee in potential policy breaches

the problem domain. Employers are poised in monitoring employees regarding to how they apply security resources in their duties. However employees feel that the monitoring sometimes inflicts them with varying degree of harms such as privacy invasion, psychological and mental stress and even tend to negatively affect their work performance. Deontological ethics took side with employees as there are some privacy laws against overzealous monitoring. The basic solution is to find a balance point of which security policy monitoring can be conducted in such a way that harm is not caused onto the stakeholders involve. Vulnerability principle was therefore explored to help in the mediation of this controversy in use policy monitoring. The process involve identifying all stakeholders, training or orientating the stakeholders with ethics relating to use policy, identifying deontological and utilitarianism ethical issues in use policy monitoring. This is followed with identifying moral agents and their patients, assessing and analysing use policy monitoring decisions to satisfy all parties. The process is reviewed periodically to catch-up with updated laws and concerns.

In following this process, all the parties in the use policies will be involved in the design of the monitoring process. Their challenges relating to use policy monitoring can then be identified and resolved. Use policy monitoring can then be reasonably conducted to meet the desire effectiveness of the employer without causing harm to employees. Empirical studies need to be conducted in future to assess and evaluate this proposed solution for practical use.

#### REFERENCES

- [1] Indiparambil JJ. An empirical study on the detrimental effects of employee surveillance in India. *International Journal of Research in Computer Application & Management*. 2017;7(12):48-51.
- [2] Yeng P, Yang B, Snekenes E. Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC) 2019 Jul 15 (Vol. 2, pp. 397-404). IEEE.
- [3] Whitman M. E., Mattord H. J. Principles of information security. 6th Edition ed: CENGAGE Learning; 2017. 728 p.
- [4] Ruighaver A. B., Maynard S. B., Warren M. Ethical decision making: Improving the quality of acceptable use policies. *Computers & Security*. 2010;29(7):731-6.
- [5] Nweke L., Wolthusen S. Ethical Implications of Security Vulnerability Research for Critical Infrastructure Protection. 2020. p. 331-40.
- [6] Bonde S., Firenze P. Making choices: A framework for making ethical decisions. Retrieved from Web Accessibility Initiative website: <http://www.brown.edu>; 2013.
- [7] Trompeter C. M., Elof J. H. A framework for the implementation of socio-ethical controls in information security. *Computers & Security*. 2001;20(5):384-91.
- [8] Scully JL. Hidden labor: Disabled/nondisabled encounters, agency, and autonomy. *IJFAB: International Journal of Feminist Approaches to Bioethics*. 2010 Sep;3(2):25-42.
- [9] Wang, S.C., Yan, K.Q., Liao, W.P. and Wang, S.S., 2010, July. Towards a load balancing in a three-level cloud computing network. In 2010 3rd international conference on computer science and information technology (Vol. 1, pp. 108-113). IEEE.
- [10] Yeng, P.K., Yang, B. and Snekenes, E.A., 2019, December. Framework for Healthcare Security Practice Analysis, Modeling and Incentivization. In 2019 IEEE International Conference on Big Data (Big Data) (pp. 3242-3251). IEEE.
- [11] Patrick Dubicki, Submitted 11/27/2003 Acceptable Use Policies and Workplace Privacy: Legal and Ethical Considerations, SANS Institute, 2003, 1-14, 2004, SANS, Access <https://www.giac.org/paper/gsec/4079/acceptable-policies-workplace-privacy-legal-ethical-considerations/106512>
- [12] Ford J, Willey L, White BJ, Domagalski T. New concerns in electronic employee monitoring: have you checked your policies lately?. *Journal of Legal, Ethical and Regulatory Issues*. 2015;18(1):51.
- [13] Walls, A. (2012a). Conduct digital surveillance ethically and legally: 2012 update. Gartner, Inc. Retrieved June 29, 2012 from <http://www.gartner.com/id=1965315>
- [14] Ciocchetti, Corey A. "The eavesdropping employer: a twenty-first century framework for employee monitoring." *American Business Law Journal* 48.2 (2011): 285-369.
- [15] Yerby J. Legal and ethical issues of employee monitoring. *Online Journal of Applied Knowledge Management (OJAKM)*. 2013;1(2):44-55.
- [16] Peter, J., & Britton, S.M. (2001). Employer Monitoring Of Employee Internet Use And Email: MEALEY'S Cyber Tech Litigation Report, 2, Retrieved June 1, 2020, from <http://foleybezek.com/wp-content/uploads/art.InternetFile.pdf>
- [17] Business Wire, Inc., 2007 Electronic Monitoring & Surveillance Survey: Over Half of All Employers Combined Fire Workers for E-Mail & Internet Abuse, American Management Association (AMA) and The ePolicy Institute, Retrieved June 1st 2020, From: <https://www.businesswire.com/news/home/20080228005093/en/2007-Electronic-Monitoring-Surveillance-Survey-Employers-Combined>
- [18] Woodbury, Marsha Cook. Computer and information ethics. Stipes Pub., 2003.
- [19] Oprea, Mihaela. "An Agent-Based Knowledge Management System for University Research Activity Monitoring." *Informatica Economica* 16, no. 3 (2012).
- [20] Frayer, Charles E. "Employee Privacy and Internet Monitoring: Balancing Worker's Rights and Dignity with Legitimate Management Interests." *Bus. Law*. 57 (2001): 857.

- [21] Alder, G. Stoney. "Ethical issues in electronic performance monitoring: A consideration of deontological and teleological perspectives." *Journal of Business Ethics* 17, no. 7 (1998): 729-743.
- [22] Galvin, K. "Boston Hotel Worker Tells Senate of Video Invasion of Privacy." *States News Service* 22 (1993).
- [23] Barry, R. J. "Statement on behalf of Security Companies Organized for Legislative Action (SCOLA) before the senate labor and human resources subcommittee on employment and productivity." *United States Senate* 22 (1993).
- [24] Alder, G. Stoney. "Employee reactions to electronic performance monitoring: A consequence of organizational culture." *The Journal of High Technology Management Research* 12, no. 2 (2001): 323-342.
- [25] Bylinsky, Gene. "How companies spy on employees." *Fortune* 124, no. 11 (1991): 131.
- [26] Palayoor, Alex Joy, and D. Mavoothu. "Ethical Orientation: A Solution for Workplace Monitoring and Privacy Issues."
- [27] Watkins Allen, Myria, Stephanie J. Coopman, Joy L. Hart, and Kasey L. Walker. "Workplace surveillance and managing privacy boundaries." *Management Communication Quarterly* 21, no. 2 (2007): 172-200.
- [28] Ball, Kirstie. "Workplace surveillance: An overview." *Labor History* 51, no. 1 (2010): 87-106.
- [29] Sewell, Graham, and James R. Barker. "Coercion versus care: Using irony to make sense of organizational surveillance." *Academy of Management Review* 31, no. 4 (2006): 934-961.
- [30] Miller S, Weckert J. Privacy, the Workplace and the Internet. *Journal of Business Ethics*. 2000 Dec 1;28(3):255-65.
- [31] Mackenzie C, Rogers W, Dodds S. Introduction: What is vulnerability and why does it matter for moral theory?. *Vulnerability: New essays in ethics and feminist philosophy*. 2014:1-29.
- [32] Morton Winston, The Vulnerability Principle Accessed on June 01, 2020 From: <http://ethicsofglobalresponsibility.blogspot.com/2008/03/vulnerability-principle.html>
- [33] By Joydeep Misra, What is Biometric Monitoring? Accessed on June 03 2020 from: <https://bridgera.com/biometric-monitoring-iot-digital-health/>
- [34] Brumback CB, Myers NA, Yuen SG, Park J, Diemer TS, inventors; Fitbit Inc, assignee. Biometric monitoring device with heart rate measurement activated by a single user-gesture. *United States patent US 9,049,998*. 2015 Jun 9.
- [35] Lee S, Kleiner BH. Electronic surveillance in the workplace. *Management Research News*. 2003 Mar 1.
- [36] Indiparambil, J. J. (2019). Review of Pros-Cons Cons Polemics of Workplace Surveillance : Survey Comparison and Analysis. *International Journal of Current Advanced Research*, 8(02), 17277-17283.
- [37] Willey L, Ford JC, White BJ, Clapper DL. Trade Secret Law and Information Systems: Can Your Students Keep a Secret?. *Journal of Information Systems Education*. 2011 Jun 1;22(3):271.
- [38] Keith, N. (2016). Cultivating practitioners of democratic civic engagement. *Michigan Journal of Community Service Learning*, 23(1), 15-36.
- [39] Lisa Guerin, J.D, Workplace Cameras and Surveillance: Rules for Employers Accessed on June 10th 2020 From: <https://www.nolo.com/legal-encyclopedia/workplace-cameras-surveillance-employer-rules-35730.html>
- [40] Bryant, J. (2005). Computer privacy ANNOYANCES: How to avoid the most annoying invasions of your personal and online privacy. *The British Journal of Healthcare Computing & Information Management*, 22(10), 25.
- [41] Straehle C. Introduction: Vulnerability, Autonomy and Applied Ethics. In *Vulnerability, Autonomy, and Applied Ethics* 2016 Oct 4 (pp. 7-16). Routledge.
- [42] Donald C Dowling Jr, Proskauer Rose LLP, "Video surveillance in workplaces worldwide" Accessed on June 10th 2020, From: [https://uk.practicallaw.thomsonreuters.com/9-203-3829?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&bhcp=1](https://uk.practicallaw.thomsonreuters.com/9-203-3829?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1)

# Feeder Reconfiguration in Unbalanced Distribution System with Wind and Solar Generation using Ant Lion Optimization

Surender Reddy Salkuti

Department of Railroad and Electrical Engineering  
Woosong University, Daejeon  
South Korea

**Abstract**—This paper proposes an approach for the distribution system (DS) feeder reconfiguration (FRC) of balanced and unbalanced networks by minimizing the total cost of operation. Network reconfiguration is a feasible technique for system performance enhancement in low voltage distribution systems. In this work, wind and solar photovoltaic (PV) units are selected as distributed energy resources (DERs) and they are considered in the proposed FRC approach. The uncertainties related to DERs are modeled using probability analysis. In most cases, the distribution system is an unbalanced system and the 3-phase transformers play a vital role as they have different configurations. This paper proposes efficient power flow models for the unbalanced distribution systems with various 3-phase transformer configurations. The proposed FRC approach has been solved by using the evolutionary algorithm based Ant Lion Optimization (ALO), and it has been implemented on 17 bus test system considering the balanced and unbalanced distribution systems with and without RESs.

**Keywords**—Distributed energy resources; evolutionary algorithms; feeder reconfiguration; operational cost; optimization algorithms; three-phase transformers

## I. INTRODUCTION

Electrical energy is considered an important source for any country's economic growth. Integration of various renewable energy sources (RESs) into electrical power networks is increasing due to the importance of environmental safety and to make less dependency on the gradual depletion of fossil fuels. Conventional energy sources mainly depend on fossil fuels for power generation [1]. Large-scale utilization of fossil fuels causes resource depletion as well as global warming. Among all the available RESs [2], wind and solar photovoltaic (PV) energy systems have become popular. However, large-scale penetration of RESs can lead to various challenges, as these sources are intermittent and variable. Optimal allocation and operation of these RESs in the distribution network lead to a decrease in power losses, enhancement in voltage profile, and system reliability.

### A. Related Works

An optimization approach for the restoration of an unbalanced distribution system after large-scale outages with DERs has been proposed in [3]. A methodology for the feeder reconfiguration (FRC) for three-phase unbalanced distribution systems (DSs) with DERs at various bus locations and sizes of

DG units using nonlinear programming and sensitivity analysis is proposed in [4]. The author in [5] proposes a distributed secondary control approach for the DGs integrated with grid-integrated inverters in unbalanced dynamic microgrids (MGs). A heuristic-based method is proposed in [6] to simplify the graph of the radial distribution system (RDS) to reduce the computational complexity by optimizing the system power losses, switching operations, and the out-of-service load demands. A chaotic stochastic fractal search technique for solving the FRC problem to reduce system losses and to enhance the voltage profile in the distribution systems is proposed in [7]. A simple FRC technique for the balanced and unbalanced RDSs is proposed in [8]. The solution of multi-objective-based FRC with optimal capacitor allocation problem with multiple time intervals with DERs is proposed in [9].

An analytical methodology for the FRC with DG hosting to minimize the system losses in the RDSs is proposed in [10]. A systematic overview of distribution FRC approaches for mitigating distribution systems' unbalance is described in [11]. A dynamic FRC methodology for a 3-phase unbalanced RDS is formulated as a problem of mixed-integer linear programming has been proposed in [12]. The author in [13] proposes a new FRC approach in unbalanced and balanced distribution systems to simultaneously optimize the allocation of distributed generation (DG) and reconfiguration. A scenario-based approach for addressing the uncertainty in solar irradiance, wind speed, and load demand is proposed in [14]. An integrated approach for simultaneous optimal allocation of inverter-based DGs, passive filters, along with distribution FRC in unbalanced and balanced microgrids (MGs) is proposed in [15]. The author in [16] proposes a dynamic distribution FRC approach over multiple time intervals operation cost, energy not served, and power loss objectives.

From the above literature, it is clear that the load flow studies and FRC studies are performed for the balanced distribution system, however, in actual practice they are unbalanced. In this paper, an augmented  $\pi$  model-based distribution transformer has been implemented by including the fictitious voltage-dependent current injection sources on primary and secondary sides to model various connections of distribution transformers. The remainder of this article is organized as follows: Section II describes the distribution load

flow with different transformer connections. Section III is devoted to the power output and uncertainty modeling of RERs. Section IV discusses the problem formulation of the proposed optimal FRC approach. A brief description of the ant lion optimization (ALO) algorithm has been presented in Section V. Section VI presents the simulation results and discussions of the three-phase balanced and unbalanced distribution systems with and without considering the RESs. Finally, conclusions are made in Section VII.

## II. DISTRIBUTION LOAD FLOW WITH TRANSFORMER MODELING

Generally, the distribution systems are unbalanced. Hence, a three-phase representation of distribution system components is necessary. The transformer is one of the most important components in the distribution network, and the impact of its winding connection is significant. A three-phase transformer is represented by two blocks as depicted in Fig. 1 [17-18]. The series block shows the winding connection and leakage impedance and the shunt block on the secondary side represents the active power and reactive power losses in the core of the transformer, as a function of voltage. Since the series block affects the core losses, the main focus is on the series block and the shunt block is treated as the load at the secondary of the transformer.

Several approaches have been developed to model various winding connections of the three-phase transformer. Fictitious current source injections along with a series branch are used to decoupled primary and secondary sides. The models involving primary and secondary voltages are dependent on the current injections and series branch, are different for different types of connections. However, this technique slows down the convergence of the forward/backward load flow method. By using the nodal admittance matrix ( $Y_T$ ), the voltage and current relationship of the transformer is represented as,

$$\begin{bmatrix} I_p \\ I_s \end{bmatrix} = \begin{bmatrix} Y_{pp} & Y_{ps} \\ Y_{sp} & Y_{ss} \end{bmatrix} \begin{bmatrix} V_p \\ V_s \end{bmatrix} = \begin{bmatrix} Y_{pp}V_p + Y_{ps}V_s \\ Y_{sp}V_p + Y_{ss}V_s \end{bmatrix} \quad (1)$$

Where the matrix  $Y_T$  is divided into the four ( $3 \times 3$ ) sub-matrices ( $Y_{pp}$ ,  $Y_{ps}$ ,  $Y_{sp}$  and  $Y_{ss}$ ) as shown in equation (1) [17]. Table I presents the sub-matrices of  $Y_T$ , for the common step-up and step-down transformer configurations.

In table I,

$$Y_I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} y_t, Y_{II} = \frac{1}{3} \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix} y_t, Y_{III} = \frac{1}{\sqrt{3}} \begin{bmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{bmatrix} y_t$$

### A. $Y_g - \Delta$ Step-Down Transformer

The augmented  $\pi$ -model for the  $Y_g - \Delta$  step-down transformer is described next:

By substituting  $Y_{pp}$ ,  $Y_{ps}$ ,  $Y_{sp}$  and  $Y_{ss}$  values from Table I, then the equation (1) becomes [18],

$$I_p = Y_I V_p + Y_{III} V_s \quad (2)$$

$$I_s = Y_{III}^T V_p + Y_{II} V_s \quad (3)$$

For developing a 3-phase transformer model, equations (2) and (3) is modified by voltage-dependent injections, and they are expressed as,

$$I_p = Y_I V_p + Y_{III} V_s + X V_s - X V_s \quad (4)$$

$$I_s = Y_{III}^T V_p + Y_{II} V_s + X^T V_p - X^T V_p \quad (5)$$

By selecting  $X = -Y_{III} - Y_I, X^T = -Y_{III}^T - Y_I^T$ , the above equations become,

$$\begin{bmatrix} I'_p \\ I'_s \end{bmatrix} = \begin{bmatrix} I_p + X V_s \\ I_s + X^T V_p \end{bmatrix} = \begin{bmatrix} Y_I & -Y_I \\ -Y_I^T & Y_{II} \end{bmatrix} \begin{bmatrix} V_p \\ V_s \end{bmatrix} \quad (6)$$

Here  $Y_I = Y_I^T$  and inverse of  $Y_I$  exists. In the equations (4) and (5), the left-hand side term corresponds to the fictitious current injections. The right-hand side term in equations (4) and (5) represents the  $\pi$ -model, and it is presented in Fig. 2.

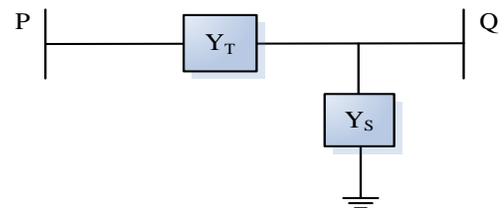


Fig. 1. Three-Phase Transformer Model.

TABLE I. SUBMATRICES FOR THE COMMON STEP-DOWN AND STEP-UP TRANSFORMER CONFIGURATIONS

Primary	Secondary	Step-down transformer connections				Step-up transformer connections			
		$Y_{pp}$	$Y_{ss}$	$Y_{ps}$	$Y_{sp}$	$Y_{pp}$	$Y_{ss}$	$Y_{ps}$	$Y_{sp}$
$Y_g$	$Y_g$	$Y_I$	$Y_I$	$-Y_I$	$-Y_I$	$Y_I$	$Y_I$	$-Y_I$	$-Y_I$
$Y_g$	$Y$	$Y_{II}$	$Y_{II}$	$-Y_{II}$	$-Y_{II}$	$Y_{II}$	$Y_{II}$	$-Y_{II}$	$-Y_{II}$
$Y_g$	$\Delta$	$Y_I$	$Y_{II}$	$Y_{III}$	$Y_{III}^T$	$Y_I$	$Y_{II}$	$Y_{III}^T$	$Y_{III}$
$Y$	$Y_g$	$Y_{II}$	$Y_{II}$	$-Y_{II}$	$-Y_{II}$	$Y_{II}$	$Y_{II}$	$-Y_{II}$	$-Y_{II}$
$Y$	$Y$	$Y_{II}$	$Y_{II}$	$-Y_{II}$	$-Y_{II}$	$Y_{II}$	$Y_{II}$	$-Y_{II}$	$-Y_{II}$
$Y$	$\Delta$	$Y_{II}$	$Y_{II}$	$Y_{III}$	$Y_{III}^T$	$Y_{II}$	$Y_{II}$	$Y_{III}^T$	$Y_{III}$
$\Delta$	$Y_g$	$Y_{II}$	$Y_I$	$Y_{III}$	$Y_{III}^T$	$Y_{II}$	$Y_I$	$Y_{III}^T$	$Y_{III}$
$\Delta$	$Y$	$Y_{II}$	$Y_{II}$	$Y_{III}$	$Y_{III}^T$	$Y_{II}$	$Y_{II}$	$Y_{III}^T$	$Y_{III}$
$\Delta$	$\Delta$	$Y_{II}$	$Y_{II}$	$-Y_{II}$	$-Y_{II}$	$Y_{II}$	$Y_{II}$	$-Y_{II}$	$-Y_{II}$

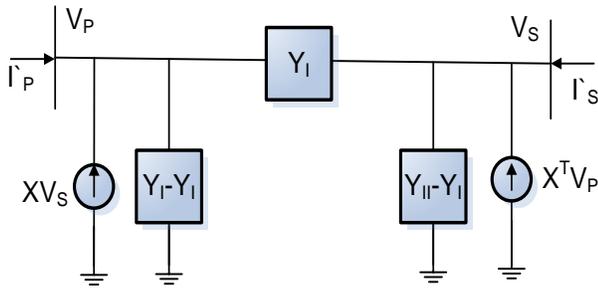


Fig. 2.  $\pi$ -Model of Yg- $\Delta$  Step-Down Transformer with Fictitious Currents.

### B. Step-by-Step Approach for the Load Flow with Transformers

Step 1: Read test system data, and initialize the voltages at all buses in the distribution network.

Step 2: Select X based on the transformer configuration.

Step 3: Determine the fictitious voltage-dependent current injections for the transformer.

Step 4: Form the BIBC and BCBV matrices.

Step 5: Run the load flow.

Step 6: Check for the convergence criteria. If satisfied, then STOP. Otherwise, go to Step 3.

### III. MODELING OF WIND AND SOLAR PV POWER GENERATION

The uncertain nature of wind speed ( $v$ ) and solar irradiance ( $G$ ) can be modeled by using the probability analysis/probability distribution function (PDF).

#### A. Modeling of Wind Power Generation

The amount of power output from WEG will depend on the location and the wind speed, and it can be expressed as [19],

$$P_W = \begin{cases} 0 & \text{for } v < v_{cin} \text{ and } v > v_{cout} \\ \left( \frac{P_W^r}{v_r^3 - v_{cin}^3} \right) v^3 + \left( \frac{v_{cin}^3}{v_r^3 - v_{cin}^3} \right) P_W^r & \text{for } v_{cin} \leq v \leq v_r \\ P_W^r & \text{for } v_r \leq v \leq v_{cout} \end{cases} \quad (7)$$

Here, the Weibull PDF is used to model the wind power output and it can be represented by [20],

$$f_p(P_W) = \frac{k(v_r - v_{cin})}{c^k P_W^r} \left[ v_{cin} + \frac{P_W}{P_W^r} (v_r - v_{cin}) \right] \exp \left[ - \left[ \frac{v_{cin} + \frac{P_W}{P_W^r} (v_r - v_{cin})}{c} \right]^k \right] \quad (8)$$

#### B. Modeling of Solar PV Power Generation

Power output from solar PV unit depends on solar insolation and ambient temperature at a particular location and it can be expressed as [20],

$$P_{PV} = (N_{PV} \times V \times I \times FF) \quad (9)$$

The voltage-current (V-I) characteristics of the solar PV module concerning solar insolation ( $G$ ) and ambient temperature ( $T_A$ ) are expressed as,

$$V = V_{oc} - (K_V \times T_c) \quad (10)$$

$$I = G[I_{sc} + K_I(T_c - 25)] \quad (11)$$

$$T_c = T_A + G \left( \frac{N_{OT} - 20}{0.8} \right) \quad (12)$$

$$FF = \frac{V_{MPP} I_{MPP}}{V_{oc} I_{sc}} \quad (13)$$

In this paper, the bimodal distribution function is used to model the solar PV power output. Here, the Weibull PDF is used to model the power output. This can be expressed as [20, 21],

$$f(G) = \omega \left( \frac{k_1}{c_1} \right) \left( \frac{G}{c_1} \right)^{k_1 - 1} e^{-\left( \frac{G}{c_1} \right)^{k_1}} + (1 - \omega) \left( \frac{k_2}{c_2} \right) \left( \frac{G}{c_2} \right)^{k_2 - 1} e^{-\left( \frac{G}{c_2} \right)^{k_2}} \quad (14)$$

$k_1$ ,  $k_2$  are shape factors, and  $c_1$ ,  $c_2$  are scale factors, respectively.

### IV. OPTIMAL FEEDER RECONFIGURATION (FRC): PROBLEM FORMULATION

FRC is an important tool to be used in the operation of the distribution network at an optimum operating cost and to enhance the system's security/reliability. FRC refers to varying the topology of feeders by opening and/or closing the tie and sectionalizing switches. It is used to minimize the power losses and to relieve overload in the feeders. The major objective of the proposed smart distribution network FRC is to find an optimal set of switches that need to be opened and closed by minimizing the total operating cost (TOC) of the system. This objective can be expressed as [22-24]:

Minimize,

$$TOC = \sum_{i=1}^{N_F} (C_i P_i) + \sum_{j=1}^{N_W} (C_{Wj} P_{Wj}) + \sum_{k=1}^{N_S} (C_{PVk} P_{PVk}) \quad (15)$$

The above equation is solved subjected to the following constraints.

#### A. Constraints

The proposed FRC optimization problem must satisfy the following constraints, and they are presented next:

1) *Equality constraints*: These constraints refer to the power balancing in the distribution system, and it can be expressed as [25]:

$$\sum_{i=1}^{N_F} (P_i) + \sum_{j=1}^{N_W} (P_{Wj}) + \sum_{k=1}^{N_S} (P_{PVk}) = P_D \quad (16)$$

2) *Inequality constraints*: The power constraint on feeders can be expressed as [26]:

$$P_i \leq P_i^{max} \quad i = 1, 2, \dots, N_F \quad (17)$$

Power output from WEG can be limited by [27],

$$P_{Wj} \leq P_{Wj}^{max} \quad j = 1, 2, \dots, N_W \quad (18)$$

Power output from solar PV unit can be limited by,

$$P_{PVk} \leq P_{PVk}^{max} \quad k = 1, 2, \dots, N_{PV} \quad (19)$$

Voltage at each bus can be limited by,

$$V_b^{min} \leq V_b \leq V_b^{max} \quad b = 1, 2, \dots, N_B \quad (20)$$

Current in each feeder is limited by [28],

$$|I_l| \leq I_l^{max} \quad l = 1, 2, \dots, N_l \quad (21)$$

### V. FRC USING ANT LION OPTIMIZATION (ALO) ALGORITHM

Generally, the DSs are unbalanced, and hence, three-phase representation of DS components is necessary. There are several works on load flows and FRC of balanced DSs. However, in actual practice the DSs are unbalanced. Therefore, in this section an unbalanced FRC approach for the total operating cost minimization objective is optimized by using the ALO algorithm. Here, it is important to consider the effect of three-phase transformer model as the configuration affects the system performance. As the FRC is a complex non-linear optimization problem and it can be solved by using various meta-heuristic algorithms. In the past several deterministic approaches have been used for solving this FRC problem. However, in recent years, various evolutionary-based optimization algorithms are found to be performing well for solving these problems.

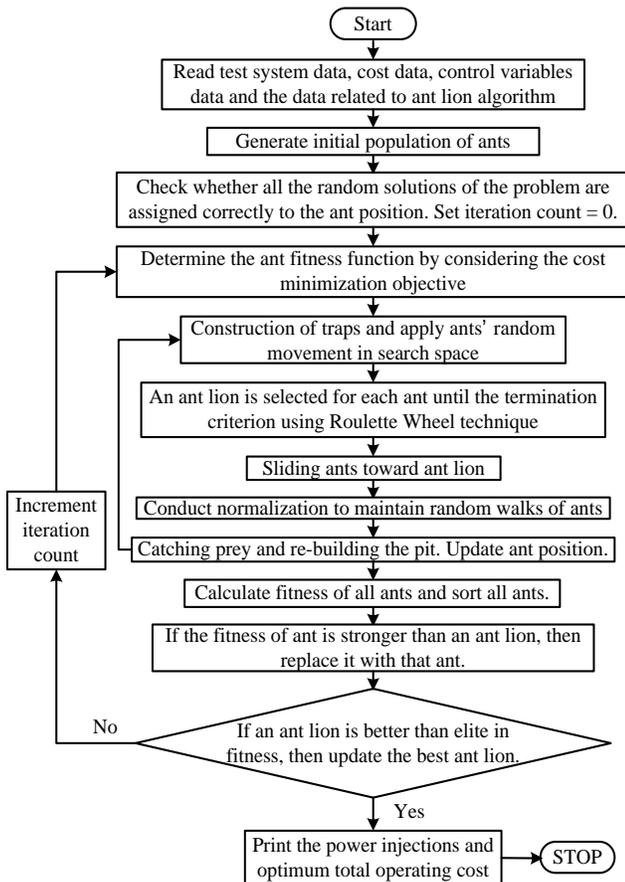


Fig. 3. Flowchart for FRC in RDS for Total Operating Cost Minimization using ALO Algorithm.

ALO is a meta-heuristic-based technique and it considers the interaction between the ants and ant lions in our nature [29]. In this ALO technique, two important stages are involved, and they are the larvae stage (i.e., hunting prey) and adult stage (i.e., reproduction) [30]. The flow chart of ALO for solving the proposed smart distribution network FRC has been depicted in Fig. 3. Initially, the data related to the test system and ant lion algorithm is read for solving the proposed FRC problem. The proposed ant lion algorithm includes various stages such as determination of fitness, construction of traps, catching prey, re-building the pit, and they are depicted in Fig. 3.

### VI. SIMULATION RESULTS AND DISCUSSION

The proposed feeder reconfiguration (FRC) approach has been applied for 17 bus balanced and unbalanced distribution systems (DSs) [17]. This DS has 17 buses, 3 feeders, 19 branches, 3 tie-switches, and the base MVA is 100 [18]. Transformer (115 kV/13.2 kV) with  $\Delta - Y_g$  is connected between buses 1 and 2, 1 and 3, and 1 and 4. The leakage impedance of these transformers is (0.01+j0.05) p.u. Power limits in the feeders of phases R, Y, and B are 14.1 MW, 18.1 MW, and 1.3 MW, respectively. The single line diagram (SLD) of this 17 bus test system has been depicted in Fig. 4. In this system, a wind farm is placed at bus number 14, and a solar PV unit is placed at bus number 9. As mentioned earlier, Ant Lion Optimization (ALO) technique is used to solve the proposed FRC problem with and without RESs. Three feeders are coming from a single substation and they are connected through the 3-three phase transformers.

Rated capacities of WEG and solar PV units considered in this work are 2 MW. For the WEG, it is considered that the rated wind speed is 12 m/s, cut-in speed is 3 m/s, and cut-out speed is 25 m/s. For the solar PV unit, the maximum power point current ( $I_{MPP}$ ) is 7.76 A, maximum power point voltage ( $V_{MPP}$ ) is 28.36V, the nominal operating temperature of the cell ( $N_{OT}$ ) is 43°C, short circuit current ( $I_{SC}$ ) is 8.38 A, open-circuit voltage ( $V_{OC}$ ) is 36.96 V, temperature coefficient of voltage ( $K_V$ ) is 0.1278 V/°C, and the temperature coefficient of current ( $K_I$ ) is 0.00545 A/°C.

In this paper, two different case studies are simulated on 17 bus distribution system, and they are:

- Case Study 1: Feeder reconfiguration (FRC) in a balanced distribution system with and without renewable energy sources (RESs).
- Case Study 2: FRC in unbalanced distribution system with and without RESs.

#### A. Simulation Results for Case Study 1

As mentioned earlier, in this case, a balanced distribution system is considered. The active and reactive power demands in the balanced system are 86.10 MW and 51.90 MVar, respectively. Here, the total operating cost (TOC) minimization objective is optimized with and without considering the RESs in the 17 bus balanced system. Table II presents the scheduled powers from the feeders and RESs for the 3-phase balanced system with and without RESs. Without considering the RESs, the optimum TOC obtained by using

the ALO algorithm is 1895 MU/MWh. In this case, the obtained active and reactive power losses are 3.02 MW and 4.12 MVar, respectively.

In this case, the obtained opened lines for the FRC are between buses 5-8 (line number 7), 5-9 (line number 9), and 6-11 (line number 12). Fig. 6 depicts the final topology/after the FRC. The obtained voltage profile for Case Study 1 without RESs has been depicted in Fig. 6. The minimum voltages obtained in phases R, Y, and B are 0.9352 p.u., 0.9352 p.u., and 0.9352 p.u., respectively.

Table II also presents the FRC results considering the wind and solar PV units at buses 14 and 9, respectively. The TOC obtained, in this case, is 1870.358 MU/MWh, which is less compared to without considering the RESs. The FRC/opened lines, in this case, are the same as the case without RESs (this topology is shown in Fig. 5). The voltage profile obtained in this case by considering the RESs has been depicted in Fig. 7. The minimum voltages obtained in R, Y, and B phases are 0.9506 p.u., 0.9506 p.u., and 0.9506 p.u., respectively.

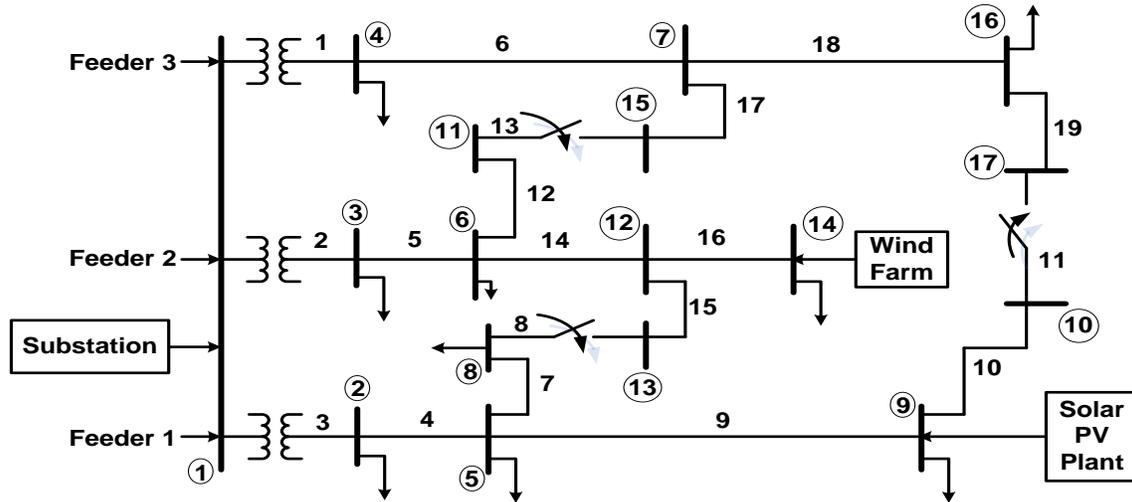


Fig. 4. Single Line Diagram (SLD) of 17 Bus Distribution System.

TABLE II. SCHEDULED POWERS FROM FEEDERS AND RESs FOR 3 PHASE BALANCED DISTRIBUTION SYSTEM (CASE STUDY 1)

Balanced distribution system	Without renewable power generation		With renewable power generation	
	Active Power (MW)	Reactive Power (MVar)	Active Power (MW)	Reactive Power (MVar)
Feeder 1	6.04	4.82	4.77	2.02
Feeder 2	53.56	30.91	51.42	29.54
Feeder 3	29.52	20.29	26.24	19.85
Total generation	89.12	56.02	88.75	55.21
Active power from WEG	-----		1.81	
Active power from solar PV	-----		1.72	
Active power demand	86.10 MW		86.10 MW	
Reactive power demand	51.90 MVar		51.90 MVar	
Active power loss	3.02 MW		2.79	
Reactive power loss	4.12 MVar		3.80	
<b>Total operating cost (MU/MWh)</b>	<b>1895.486</b>		<b>1870.358</b>	
<b>Opened lines between the buses</b>	<b>5-8, 5-9, 6-11</b>		<b>5-8, 5-9, 6-11</b>	
Minimum voltage in phase R (in p.u.)	0.9352 at bus 15		0.9506 at bus 15	
Minimum voltage in phase Y (in p.u.)	0.9352 at bus 15		0.9506 at bus 15	
Minimum voltage in phase B (in p.u.)	0.9352 at bus 15		0.9506 at bus 15	

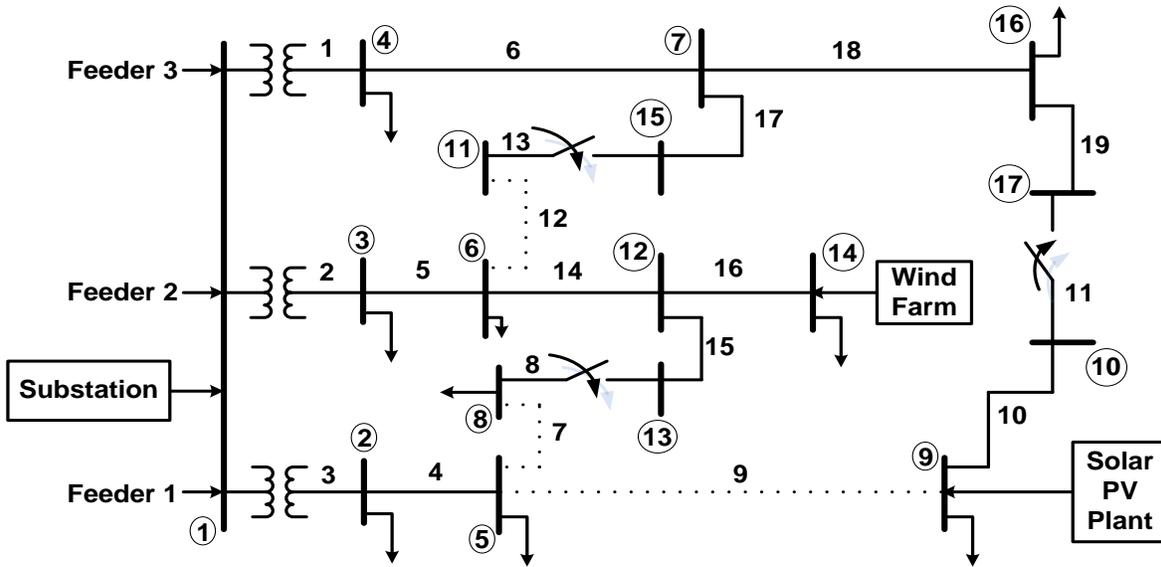


Fig. 5. SLD of 17 Bus System after the FRC for Case Study 1.

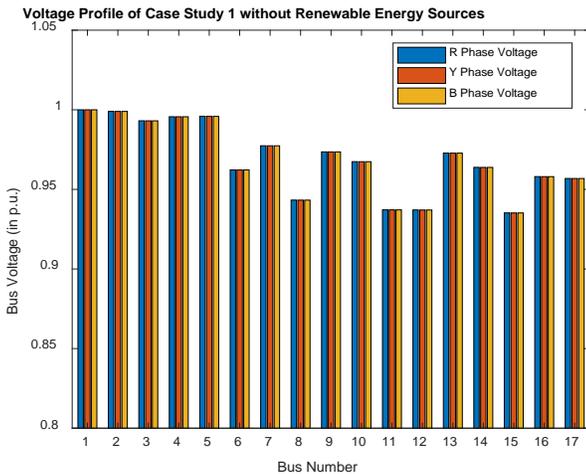


Fig. 6. Voltage Profile of Case Study 1 without Renewable Power Generation.

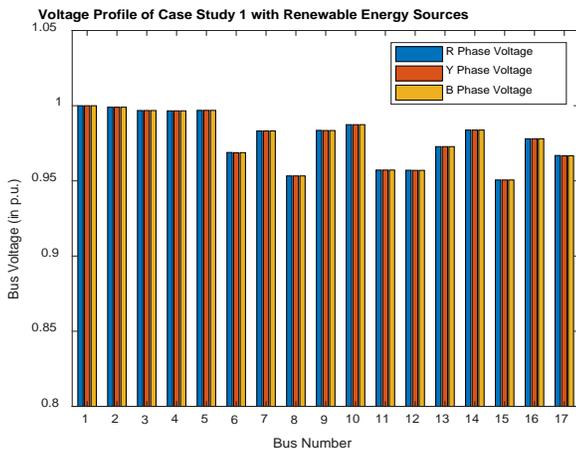


Fig. 7. Voltage Profile of Case Study 1 with Renewable Power Generation.

### B. Simulation Results for Case Study 2

In this case study, an unbalanced distribution system with and without RESs is considered. The active and reactive power demands, in this case, are 86.961 MW and 52.419 MVar, respectively. Here, the TOC minimization objective is optimized with and without considering the RESs in the 17 bus balanced system. Table III presents the scheduled powers from the feeders and RESs for Case Study 2. Without considering the RESs, the optimum TOC obtained by using the ALO algorithm is 1958.351 MU/MWh. In this case, the obtained active and reactive power losses are 3.464 MW and 0.892 MVar, respectively.

In this case, the obtained opened lines for the FRC are between buses 5-9 (line number 9), 6-11 (line number 12), and 8-13 (line number 8). Fig. 8 depicts the final topology/after the FRC. The obtained voltage profile for Case Study 2 without RESs has been depicted in Fig. 9. The minimum voltages obtained in phases R, Y, and B are 0.9495 p.u., 0.9488 p.u., and 0.9474 p.u., respectively.

Table III also presents the FRC results considering the wind and solar PV units at buses 14 and 9, respectively. The TOC obtained, in this case, is 1926.247 MU/MWh, which is less compared to without considering the RESs. The FRC/opened lines, in this case, are the same as the case without RESs (this topology is shown in Fig. 8). The voltage profile obtained in this case by considering the RESs has been depicted in Fig. 10. The minimum voltages obtained in R, Y, and B phases are 0.9657 p.u., 0.9641 p.u., and 0.9628 p.u., respectively.

From the above simulation results, it can be observed that the FRC topology obtained for the unbalanced DS is different from the balanced DS. However, the topology is the same for the cases with and without RESs. And also, the TOC obtained with RESs is less than the TOC obtained without the RESs. The nomenclature used in this work is presented in Table IV.

TABLE III. SCHEDULED POWERS FROM FEEDERS AND RESs FOR 3 PHASE UNBALANCED DISTRIBUTION SYSTEM

Unbalanced distribution system	Without renewable power generation		With renewable power generation	
	Active Power (MW)	Reactive Power (MVar)	Active Power (MW)	Reactive Power (MVar)
Feeder 1	15.112	9.513	12.24	9.563
Feeder 2	45.001	24.053	43.287	42.157
Feeder 3	30.312	19.745	27.86	19.548
Total generation	90.425	53.311	90.012	52.968
Active power from WEG	-----		1.85	
Active power from solar PV	-----		1.76	
Active power demand	86.961 MW		86.961 MW	
Reactive power demand	52.419 MVar		52.419 MVar	
Active power loss	3.464 MW		3.015	
Reactive power loss	0.892 MVar		0.826	
<b>Total operating cost (MU/MWh)</b>	<b>1958.351</b>		<b>1926.247</b>	
<b>Opened lines between the buses</b>	<b>5-9, 6-11, 8-13</b>		<b>5-9, 6-11, 8-13</b>	
Minimum voltage in phase R (in p.u.)	0.9495 at bus 14		0.9657 at bus 13	
Minimum voltage in phase Y (in p.u.)	0.9488 at bus 14		0.9641 at bus 13	
Minimum voltage in phase B (in p.u.)	0.9474 at bus 14		0.9628 at bus 13	

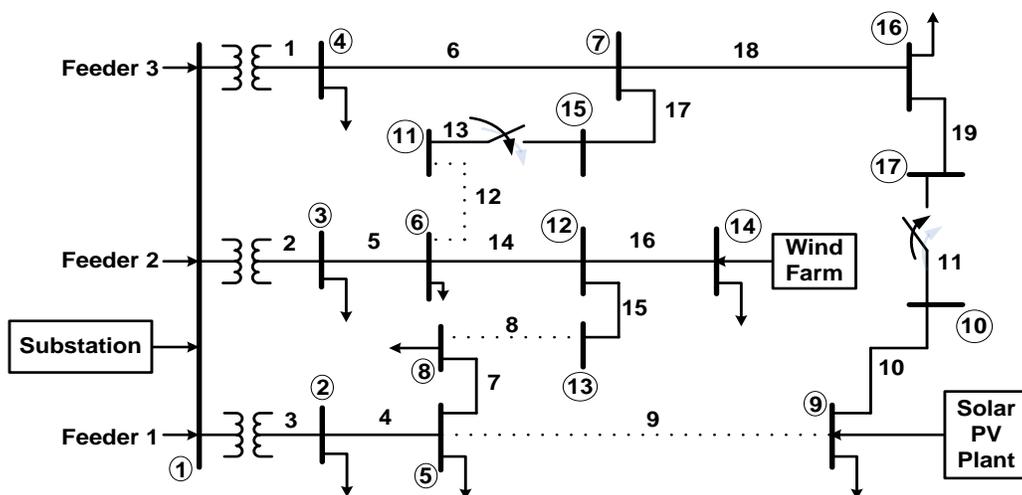


Fig. 8. SLD of 17 Bus System after the FRC for Case Study 2.

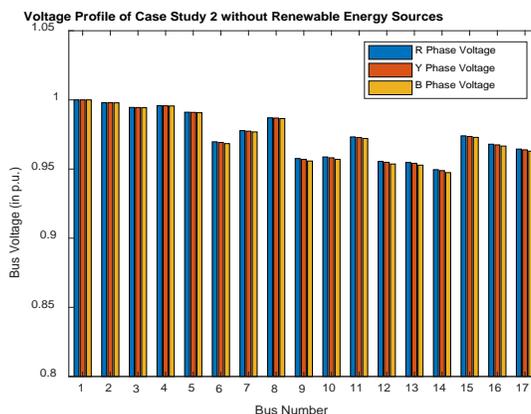


Fig. 9. Voltage Profile of Case Study 2 without Renewable Power Generation.

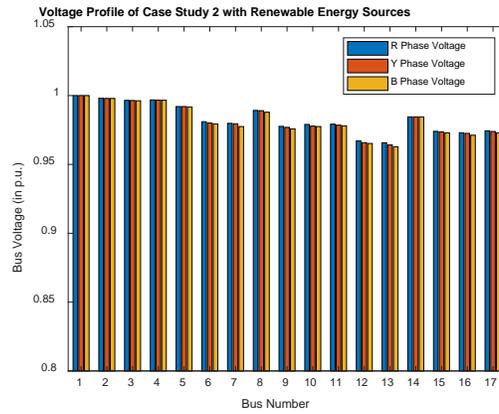


Fig. 10. Voltage Profile of Case Study 2 with Renewable Power Generation.

TABLE IV. NOMENCLATURE

Symbol	Description
$V_p, V_s$	3-phase bus voltages at the primary side and secondary side of the 3-transformer
$T_A$	Ambient temperature ( $^{\circ}\text{C}$ )
$v_{cin}$	Cut-in wind speed
$y_t$	Per unit transformer leakage admittance
$P_W^r$	Rated power of wind energy generator (WEG)
$N_{OT}$	The nominal operating temperature of the cell ( $^{\circ}\text{C}$ )
$v$	Wind speed at a particular time and location
$v_{cout}$	Cut-out wind speed
$G$	Solar irradiance ( $\text{W}/\text{m}^2$ )
$\omega$	Weight factor ( $0 < \omega < \infty$ )
$T_c$	Solar PV cell temperature ( $^{\circ}\text{C}$ )
$v_r$	Rated wind speed
$K_I$	Temperature coefficient of current ( $\text{V}/^{\circ}\text{C}$ )
$V_{MPP}$	Maximum power point voltage (V)
$I_{MPP}$	Maximum power point current (A)
$I_p, I_s$	3-phase bus injection currents at the primary side and secondary side of the 3-transformer
$FF$	Fill factor
$N_F$	Number of feeders
$V_{OC}$	Open circuit voltage (V)
$C_i$	Cost coefficient of $i^{\text{th}}$ feeder
$P_i$	Active power injection from the $i^{\text{th}}$ feeder
$P_{Wj}$	Active power output from $j^{\text{th}}$ wind generator
$P_{PVk}$	Active power output from $k^{\text{th}}$ solar PV unit
$N_B$	Number of buses
$p_i^{\text{max}}$	Maximum power injected at $i^{\text{th}}$ feeder
$I_{SC}$	Short circuit current (A)
$V_b$	The magnitude of voltage at $b^{\text{th}}$ bus
$V_b^{\text{min}}, V_b^{\text{max}}$	Minimum and maximum bus voltages at $b^{\text{th}}$ bus
$I_l$	Current in $l^{\text{th}}$ line
$N_l$	Number of lines
$I_l^{\text{max}}$	Maximum allowable branch current
$N_{PV}$	Number of solar PV modules in a solar array
$Y_T$	Nodal admittance matrix
$K_V$	Temperature coefficient of voltage ( $\text{A}/^{\circ}\text{C}$ )

## VII. CONCLUSIONS

This paper proposes the FRC approach for the balanced and unbalanced distribution system for the total operating cost (TOC) minimization. Generally, the distribution systems are unbalanced, and hence the 3-phase representation is required. The importance and the effect of the 3-phase transformer model and its effect on system performance have been highlighted in this paper. In this work, wind and solar photovoltaic (PV) units are selected as distributed energy resources (DERs) and they are considered in the proposed FRC approach. The amount of power generation from wind and solar PV units is determined by using probability analysis. The proposed approach has been solved by using the ant lion optimization (ALO) algorithm. The optimal topology for an unbalanced system is different from that of a balanced system. However, the topology is the same for the cases with and without RESs. And also, the TOC obtained with RESs is less than the TOC obtained without the RESs. Solving the proposed FRC problem including the battery energy storage units and electric vehicle charging loads is the scope for future research work.

## ACKNOWLEDGMENT

This research work was funded by “Woosong University’s Academic Research Funding – 2021”.

## REFERENCES

- [1] K.S. Kumar, S. Naveen, “Power system reconfiguration and loss minimization for a distribution systems using Catfish PSO algorithm”, *Frontiers in Energy*, vol. 8, pp. 434-442, 2014.
- [2] A.V.S. Reddy, M.D. Reddy, M.S.K. Reddy, “Network Reconfiguration of Primary Distribution System Using GWO Algorithm”, *International journal of electrical and computer engineering*, vol. 7, no. 6, pp. 3226-3234, Dec. 2017.
- [3] Z. Ye, C. Chen, B. Chen, K. Wu, “Resilient Service Restoration for Unbalanced Distribution Systems With Distributed Energy Resources by Leveraging Mobile Generators”, *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1386-1396, Feb. 2021.
- [4] F. Ding, K.A. Loparo, “Feeder Reconfiguration for Unbalanced Distribution Systems with Distributed Generation: A Hierarchical Decentralized Approach”, *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1633-1642, Mar. 2016.
- [5] Y. Du, X. Lu, H. Tu, J. Wang, S. Lukic, “Dynamic Microgrids With Self-Organized Grid-Forming Inverters in Unbalanced Distribution Feeders”, *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 8, no. 2, pp. 1097-1107, June 2020.
- [6] M. Khederzadeh, S. Zandi, “Enhancement of Distribution System Restoration Capability in Single/Multiple Faults by Using Microgrids as a Resiliency Resource”, *IEEE Systems Journal*, vol. 13, no. 2, pp. 1796-1803, June 2019.
- [7] T.T. The, D.V. Ngoc, N.T. Anh, “Distribution Network Reconfiguration for Power Loss Reduction and Voltage Profile Improvement Using Chaotic Stochastic Fractal Search Algorithm”, *Complexity*, vol. 2020, pp. 1-15, 2020.
- [8] J.B.V. Subrahmanyam, C. Radhakrishna, “A Simple Method for Feeder Reconfiguration of Balanced and Unbalanced Distribution Systems for Loss Minimization”, *Electric Power Components and Systems*, vol. 38, no. 1, pp. 72-84, 2009.
- [9] H. Lotfi, R. Ghazi, M.B. Naghibi-Sistani, “Multi-objective dynamic distribution feeder reconfiguration along with capacitor allocation using a new hybrid evolutionary algorithm”, *Energy Systems*, no. 3, 2020.
- [10] M.A. Abdelkader, Z.H. Osman, M.A. Elshahed, “New analytical approach for simultaneous feeder reconfiguration and DG hosting allocation in radial distribution networks”, *Ain Shams Engineering Journal*, 2020.
- [11] Md.R. Islam, H. Lu, M.J. Hossain, L. Li, “Mitigating unbalance using distributed network reconfiguration techniques in distributed power generation grids with services for electric vehicles: A review,” *Journal of Cleaner Production*, vol. 239, 2019.
- [12] H.F. Zhai, M. Yang, B. Chen, N. Kang, “Dynamic reconfiguration of three-phase unbalanced distribution networks,” *International Journal of Electrical Power & Energy Systems*, vol. 99, pp. 1-10, 2018.
- [13] S.A. Taher, M.H. Karimi, “Optimal reconfiguration and DG allocation in balanced and unbalanced distribution systems,” *Ain Shams Engineering Journal*, vol. 5, no. 3, pp. 735-749, 2014.
- [14] S.S. Fazlhashemi, M. Sedighzadeh, M.E. Khodayar, “Day-ahead energy management and feeder reconfiguration for microgrids with CCHP and energy storage systems”, *Journal of Energy Storage*, vol. 29, 2020.
- [15] M. Sedighzadeh, R.V. Doyran, A. Rezaazadeh, “Optimal simultaneous allocation of passive filters and distributed generations as well as feeder reconfiguration to improve power quality and reliability in microgrids,” *Journal of Cleaner Production*, vol. 265, 2020.
- [16] A. Azizivahed, H. Narimani, M. Fathi, E. Naderi, H.R. Safarpour, M.R. Narimani, “Multi-objective dynamic distribution feeder reconfiguration in automated distribution systems,” *Energy*, vol. 147, pp. 896-914, 2018.
- [17] G.K.V. Raju, P.R. Bijwe, “Efficient reconfiguration of balanced and unbalanced distribution systems for loss minimization,” *IET Generation, Transmission and Distribution*, vol. 2, no. 1, pp. 7-12, 2008.
- [18] G.K.V. Raju, P.R. Bijwe, “An Efficient Algorithm for Minimum Loss Reconfiguration of Distribution System Based on Sensitivity and Heuristics,” *IEEE Transactions Power Systems*, vol.23, no.3, pp. Aug. 2008.
- [19] S.S. Reddy, P.R. Bijwe, A.R. Abhyankar, “Optimum day-ahead clearing of energy and reserve markets with wind power generation using anticipated real-time adjustment costs,” *International Journal of Electrical Power & Energy Systems*, vol. 71, pp. 242-253, 2015.
- [20] S.S. Reddy, “Optimal scheduling of thermal-wind-solar power system with storage,” *Renewable Energy*, vol. 101, pp. 1357-1368, 2017.
- [21] S.S. Reddy, J.A. Momoh, “Realistic and Transparent Optimum Scheduling Strategy for Hybrid Power System,” *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3114-3125, Nov. 2015.
- [22] M. Kaur, S. Ghosh, “Network reconfiguration of unbalanced distribution networks using fuzzy-firefly algorithm,” *Applied Soft Computing*, vol. 49, pp. 868-886, 2016.
- [23] S. Ghasemi, “Balanced and unbalanced distribution networks reconfiguration considering reliability indices,” *Ain Shams Engineering Journal*, vol. 9, no. 4, pp. 1567-1579, 2018.
- [24] I.G. Guimarães, D.P. Bernardon, V.J. Garcia, M. Schmitz, L.L. Pfitscher, “A decomposition heuristic algorithm for dynamic reconfiguration after contingency situations in distribution systems considering island operations,” *Electric Power Systems Research*, vol. 192, 2021.
- [25] Sang-Bong Rhee, Yu-Jeong Lee, Seok-Ku You, Kyu-Ho Kim, “Network Reconfiguration Using Chaos Search Method in Unbalanced Distribution Systems,” *IFAC Proceedings Volumes*, vol. 36, no. 20, pp. 803-807, 2003.
- [26] A. Swarnkar, N. Gupta, K.R. Niazi, “Adapted ant colony optimization for efficient reconfiguration of balanced and unbalanced distribution systems for loss minimization,” *Swarm and Evolutionary Computation*, vol. 1, no. 3, pp. 129-137, 2011.
- [27] C.H.N.R. Barbosa, M.H.S. Mendes, J.A. Vasconcelos, “Robust feeder reconfiguration in radial distribution networks,” *International Journal of Electrical Power & Energy Systems*, vol. 54, pp. 619-630, 2014.
- [28] G. Mahendran, C. Govindaraju, “Flower pollination algorithm for distribution system phase balancing considering variable demand,” *Microprocessors and Microsystems*, vol. 74, 2020.
- [29] M. Wang, A.A. Heidari, M. Chen, H. Chen, X. Zhao, X. Cai, “Exploratory differential ant lion-based optimization”, *Expert Systems with Applications*, vol. 159, 2020.
- [30] J. Wang, P. Dua, H. Lub, W. Yanga, T. Niu, “An improved grey model optimized by multi-objective ant lion optimization algorithm for annual electricity consumption forecasting”, *Applied Soft Computing*, vol. 72, pp. 321-337, 2018.

# Determinants of e-Commerce Use at Different Educational Levels: Empirical Evidence from Turkey

## e-Commerce Use at Different Educational Levels

Şeyda Ünver<sup>1</sup>

Research Assistant, Department of Econometrics  
Ataturk University, Erzurum, Turkey

Ömer Alkan<sup>2</sup>

Associate Professor, Department of Econometrics  
Ataturk University, Erzurum, Turkey

**Abstract**—Rapid spread of internet has made e-commerce an essential and effective tool for commercial transactions. The purpose of this study is to investigate e-commerce use differences between individuals in Turkey according to their educational levels and to specify the relationship between demographic characteristics of individuals and e-commerce use. In this study, the cross-sectional data obtained by Household Information Technologies Usage Survey were used. Binary logistic regression analysis was utilized to determine the factors associated with the e-commerce use of individuals. This study has concluded that the variables of income level, age, gender, occupation, region, social media use, use of internet banking, use of e-government, number of information equipment in a household and the number of people in a household have relationships with e-commerce use. In addition, it has been found out that the variables in e-commerce use showed differences according to educational levels of individuals. It has been determined as a result of this study that as the education level of the individuals increased, their tendency towards online shopping increased. Higher education level refers to higher income level at both state and private institutions and more perception towards innovations. This has naturally a positive effect on online shopping behaviors of individuals.

**Keywords**—Electronic commerce; online shopping; educational level; e-commerce; Turkey; binary logistic regression

### I. INTRODUCTION

Significant developments are observed in commercial issues due to the significant increase in the impact of information technologies on our lives. There are new electronic commerce opportunities for purchasers (customers or enterprises). Electronic commerce refers to internet-based sales [1]. It is usually abbreviated as e-commerce or e-Commerce [2]. e-Commerce first started in 1994, and has aroused the interest of many retailers and traders due to the advantages it offers for both companies and consumers [3]. The rapid spread of internet has made e-commerce an essential and effective tool for commercial transactions [4].

e-Commerce may be defined as the use of electronic networked computer-based technologies to place new products, services and ideas on the market, to support and develop business operations [1]. e-Commerce benefits from the technologies, such as mobile commerce, electronic fund transfer, supply chain management, internet marketing, online transaction processing, electronic data interchange, inventory management systems and automated data collection systems.

Modern electronic commerce generally uses World Wide Web during at least one part of a transaction's life cycle in addition to other technologies, such as e-mail [5]. Today, e-commerce is used as a quick tool to transform the world into an information society [6].

In online shopping, consumers can do shopping 24 hours a day and are not required to visit any physical store of sellers, located in another city or country [7]. In addition, online shopping provides consumers with more control and bargaining power when compared with traditional shopping as it is possible to obtain more information about products and services available on the internet [2].

Turkey is a country with a significant growth potential in e-commerce, having increasing number of e-sellers and a large, young population. e-Commerce started to be carried out significantly in Turkey as of 1990s, and has been in a rapid increase as of early 2000s [8]. Turkish Informatics Industry Association stated that e-commerce increased by 42% in Turkey in 2018 [9].

It is seen that individuals use e-commerce in several different manners and for various purposes [10, 11]. As e-commerce use improves opportunities in many areas, it is of importance to evaluate the scopes of differences and underlying causes [12]. It is known that the demographic characteristics of individuals affect their actions before they display any behavior [13]. Therefore, the differences in e-commerce use in various respects between demographic groups is an interesting research topic [14]. In the literature, there are studies showing that demographic factors affect individuals' attitudes towards online purchasing behavior [15-18]. Distribution of different demographic groups is of importance to analyze e-commerce use according to educational levels of individuals. In this study, a systematic analysis was carried out to investigate the effect of selected demographic factors on e-commerce use among individuals according to their education levels.

In Turkey, there is not sufficient information on educational level differences of individuals regarding e-commerce use. As far as we know, this is the first study conducted to determine the e-commerce related factors according to educational levels of individuals across Turkey. In this study, the following research questions were developed regarding the e-commerce use of individuals in Turkey according to their educational

levels: "Does e-commerce use differs according to the education levels of individuals?", "Is there a relationship between individuals' demographic characteristics and e-commerce use?" and "Are the factors related to the use of e-commerce by individuals with different education levels the same?".

## II. LITERATURE REVIEW

In the early studies on e-commerce, it was investigated how e-commerce influenced price levels and price range [19]. In these studies, it was concluded that online markets did not offer lower prices than traditional markets [20]. However, the conclusions achieved in the following studies urged that online markets referred to a tendency of lower price ranges than traditional markets [19].

In e-commerce platforms, extensive investigations were conducted by academics to learn about e-commerce adoption behaviors. It was tried to provide information on e-commerce adoption behaviors from various perspectives, such as individual consumers and enterprises or organizations [21]. Of these studies, those subjecting individual consumers examined the commercial features of Internet and how it would affect consumer adoption of B2C (manufacturer-to-consumer) e-commerce [22-24]. In addition, some studies implemented the elaboration likelihood model (ELM) and the technology acceptance model (TAM) to discover the factors leading consumers to purchase food through e-commerce platforms [25-27]. Another study investigated the basic factors of e-commerce adoption wish from the perspectives of farmers [28].

The studies on adoption behaviors of e-commerce from the perspectives of enterprises and organizations were also examined. It was seen that a study compared the theory of planned behavior (TPB) and theory of reasoned action (TRA) by using a structural equation model, which was developed to predict whether small-sized enterprises or medium-sized enterprises (SMEs) were more willing in the adoption of e-commerce [29]. In another study, the factors affecting e-commerce adoption by Malaysian SMEs in terms of relative advantage and competitive pressure were examined [30]. In addition, while a recent study has investigated the obstacles before the adoption of mobile commerce (m-commerce) by SMEs in the United Kingdom [31], another study has examined the basic factors in the adoption of m-commerce by SMEs in Vietnam [32]. Another study conducted in China investigated the main factors affecting consumers' willingness and behaviors to adopt e-commerce as well as willingness-behavior consistency [21].

In e-commerce literature, there are also studies used logit and probit models. For example, a study on the comparison of e-commerce strategies between males and females used logit and probit models [33]. Moreover, probit models were also used in the studies on the adoption of e-commerce [34, 35]. In a study conducted in Iran's Kermanshah province, nonlinear logit and probit models were used to analyze the important factors affecting the tendency of small and medium enterprises (SMEs) to use electronic commerce [36].

In the studies conducted in recent years in Turkey, the factors effective on individuals' online purchasing behaviors

have been identified [2, 3, 37-39]. In addition, these studies have subjected the issues such as e-satisfaction, e-loyalty and e-service quality regarding e-commerce [8, 40, 41]. In a study discussing the relationship between e-commerce and business logistics, e-commerce use in Turkey and Croatia was analyzed and the importance of business logistics was underlined for the development of e-commerce [1].

## III. MATERIALS AND METHODS

### A. Data

In this study, Household Information Technologies (IT) Usage Survey performed by the Turkish Statistical Institute in 2019 was used as micro data set. Household Information Technologies Usage Survey, which is carried out since 2004, aims to collect information about information and communication technologies owned by households and individuals and their uses.

In the Household Information Technologies Usage Survey, all residential areas across Turkey were included for sample selection. This study covers all households in all residential areas within the borders of Turkey. This study does not include those living in schools, dormitories, hotels, kindergartens, old age asylums, hospitals and prisons, which are defined as institutional population, and those staying in barracks and army houses. In addition, residential areas that were not considered to reach a sufficient number of sample households (small villages, large nomad tents, hamlet, etc.) with a population not exceeding 1% of the total population were excluded. The study covers the individuals between the age range of 16-74.

Two-stage stratified cluster sampling method was used for sampling. In the first stage, clusters (blocks) with an average of 100 households were selected as sample by proportional probability (PPS). In the second stage, sample addresses from the clusters selected for the sample were determined using the systematic selection method. Statistical Territorial Units Classification was used as the 1<sup>st</sup> Level stratification criterion [42].

In this study, 18031 of the individuals participated in Household Information Technologies Usage Survey in 2019 have an elementary and lower degree graduation, 5552 of them are high school graduated and 5092 of them have a university degree.

### B. Measures and Variables

In The dependent variable of this study is the commerce use status of individuals in the recent year according to their educational levels (elementary and lower, high school and university). The individuals participating in the research received the code "1" if used e-commerce within the recent year as of the period of the survey, and "0" if they did not. In this study, a separate binary logit model was established for each educational level.

Categorical variables included in the model were measured by a nominal and ordinal scale. The independent variables were specified as follows: income level (₺2000 and below, ₺2001-₺4000, ₺4001-₺6000 and ₺6001 and above), age (15-24, 25-34, 35-44, 45-54, 55-64 and 65, and above), gender (male, female), occupation (unemployed individuals, managers,

professionals, technicians and associate professionals, clerical support workers, service/sales workers, skilled agricultural/forestry/fishery workers, craft/related trades workers, plant-machine operators/assemblers, elementary occupations), use of social media in the recent three months (yes, no), use of internet banking (yes, no), use of e-government in the last 12 months (yes, no), the number of information equipment in the household (1 and above, 2-3, 4 and above), the number of individuals in the household (3 and less, 4-5, 6 and above). Another independent variable is region. Turkey was classified into 12 regions in Level 1 under Nomenclature of Territorial Units for Statistics (NUTS). We classified these 12 regions as west, middle and east in this study. These regions and the provinces in these regions are shown in detail in Table I [43].

Ordinal and nominal variables were identified as dummy variables in order to observe the effects of the categories of all variables to be included in binary logistic regression [44].

### C. Analysis Technique/Method

SPSS 20 and Stata 15 programs were used to analyze the data. First of all, e-commerce use status of individuals participating in the study and frequency and percentages of independent variables were obtained. In this study, binary logistic regression method was utilized to investigate the differences between e-commerce use according to education levels. Binary logistic regression is a statistical analysis method used for the examination of a relationship between dependent variables and independent variable(s) in the event that dependent variable has two categories [45].

TABLE I. NOMENCLATURE OF TERRITORIAL UNITS FOR STATISTICS - LEVEL 1

Region	Code	Level 1	Provinces
Western Region	TR1	İstanbul	İstanbul
	TR2	West Marmara	Tekirdağ, Edirne, Kırklareli, Balıkesir, Çanakkale
	TR3	Aegean	İzmir, Aydın, Denizli, Muğla, Manisa, Afyonkarahisar, Kütahya, Uşak
	TR4	East Marmara	Bursa, Eskişehir, Bilecik, Kocaeli, Sakarya, Düzce, Bolu, Yalova
Central Region	TR5	West Anatolia	Ankara, Konya, Karaman
	TR6	Mediterranean	Antalya, Isparta, Burdur, Adana, Mersin, Hatay, Kahramanmaraş, Osmaniye
	TR7	Central Anatolia	Kırıkkale, Aksaray, Niğde, Nevşehir, Kırşehir, Kayseri, Sivas, Yozgat
	TR8	West Black Sea	Zonguldak, Karabük, Bartın, Kastamonu, Çankırı, Sinop, Samsun, Tokat, Çorum, Amasya
Eastern Region	TR9	East Black Sea	Trabzon, Ordu, Giresun, Rize, Artvin, Gümüşhane
	TRA	Northeast Anatolia	Erzurum, Erzincan, Bayburt, Ağrı, Kars, Iğdır, Ardahan
	TRB	Centraleast Anatolia	Malatya, Elâzığ, Bingöl, Tunceli, Van, Muş, Bitlis, Hakkâri
	TRC	Southeast Anatolia	Gaziantep, Adıyaman, Kilis, Şanlıurfa, Diyarbakır, Mardin, Batman, Şırnak, Siirt

## IV. RESULTS

### A. Descriptive Statistics

As of the date when this questionnaire was administered, it was identified that 12.45% of the individuals with an elementary and lower graduation, 45.57% of the individuals graduated from high school and 71.11% of the individuals with a university degree did a shopping on internet in the recent year.

The results of the factors that are associated with e-commerce use according to educational levels of individuals in Turkey are shown in Table II.

### B. Model Estimation

The results of estimated binary logistic regression model are provided in Table III. In this study, it was tested whether there was any multicollinearity among the independent variables to be included in the binary logistic regression model. It is considered that those with variance inflation factor (VIF) values of 5 and above cause moderate, and those with 10 and above variance inflation factor (VIF) values cause a high degree multicollinearity [46]. In this study, there was not any variable causing any multicollinearity problem among the variables.

In Table III, the binary logistic regression models estimated for individuals with an elementary and lower graduation, graduated from high school and with a university degree are shown.

The marginal effects of the factors associated with e-commerce use of individuals according to their education levels are given in Table IV.

For individuals with an elementary and lower graduation, the likelihood of an individual with an income of ₺6001 and above to use e-commerce is 57.9% more than an individual with an income of ₺2000 and lower (reference group). The likelihood of a 25-34 years old individual with an elementary and lower graduation to use e-commerce is 32.2% less than a 15-24 years old individual. The likelihood of a 45-54 years old individual with an elementary and lower graduation to use e-commerce is 119.3% less than a 15-24 years old individual. The likelihood of a female with an elementary and lower graduation to use e-commerce is 38.2% less than a male having the same education level. The likelihood of an individual with an elementary and lower graduation in the middle region to use e-commerce is 39.9% more than an individual in the east region. An individual with an elementary and lower graduation as well as a member of a professional occupation is 148.7% more likely to use e-commerce than a unemployed individual.

The likelihood of an individual with an elementary and lower graduation as well as a skilled agricultural/forestry/fishery workers to use e-commerce is 71.6% less than a unemployed individual. The likelihood of an individual with an elementary education and lower graduation in households with 1 or less information equipment is 75.2% less than an individual in a household with 4 or more information equipment. An individual with an elementary and lower graduation in a household with 6 and above individuals is 40.9% less likely to use e-commerce than an individual in a household with 3 and

lower individuals. The likelihood of an individual with an elementary and lower graduation as well as a using social media to use e-commerce is 123.4% higher than an individual not using social media. An individual with an elementary and lower graduation as well as a using internet banking is 106.5% more likely to use e-commerce than an individual not using internet banking. The likelihood of an individual with an elementary and lower graduation as well as a using e-government to use e-commerce is 79% higher than an individual not using this application.

TABLE II. FINDINGS OF THE FACTORS AFFECTING E-COMMERCE USE OF INDIVIDUALS ACCORDING TO THEIR EDUCATIONAL LEVELS

Variables		Elementary and lower graduation (n=18031)		High school graduation (n=5552)		University graduation (n=5092)	
		n	%	n	%	n	%
Income level	£2000 and below	8101	44.9	1163	20.9	381	7.5
	£2001-£4000	7305	40.5	2563	46.2	1486	29.2
	£4001-£6000	2002	11.1	1247	22.5	1424	28
	£6001 and above	623	3.5	579	10.4	1801	35.4
Age	15-24	2531	14.0	1498	27.0	481	9.4
	25-34	2414	13.4	1234	22.2	1914	37.6
	35-44	3468	19.2	1353	24.4	1447	28.4
	45-54	3827	21.2	766	13.8	681	13.4
	55-64	3464	19.2	512	9.2	379	7.4
	65 and above	2327	12.9	189	3.4	190	3.7
Gender	Male	10097	56.0	2494	44.9	2355	46.2
	Female	7934	44.0	3058	55.1	2737	53.8
Region	West	6267	34.8	2308	41.6	2246	44.1
	Middle	5977	33.1	2030	36.6	1845	36.2
	East	5787	32.1	1214	21.9	1001	19.7
Occupation	Managers	58	0.3	95	1.7	242	4.8
	Professionals	7	0.0	76	1.4	1754	34.4
	Technicians and associate professionals	12	0.1	53	1.0	197	3.9
	Clerical support workers	178	1.0	410	7.4	584	11.5
	Service/sales workers	1165	6.5	733	13.2	392	7.7
	Skilled agricultural/ forestry/ fishery workers	933	5.2	97	1.7	31	0.6
	Craft/related trades workers	527	2.9	180	3.2	62	1.2
	Plant-machine operators/ assemblers	318	1.8	168	3.0	56	1.1
	Elementary occupations	2771	15.4	782	14.1	239	4.7
	Unemployed individuals	12062	66.9	2958	53.3	1535	30.1
Number of information equipment in the household	1 and below	8775	48.7	1199	21.6	476	9.3
	2-3	7699	42.7	3111	56.0	2789	54.8
	4 and above	1557	8.6	1242	22.4	1827	35.9
Number of individuals in the household	3 and below	7894	43.8	2417	43.5	3033	59.6
	4-5	6522	36.2	2538	45.7	1837	36.1
	6 and above	3615	20.0	597	10.8	222	4.4
Social media	Yes	7651	42.4	4386	79.0	4205	82.6
	No	10380	57.6	1166	21.0	887	17.4
Internet banking	Yes	2394	13.3	2801	50.5	3947	77.5
	No	15637	86.7	2751	49.5	1145	22.5
E-government use	Yes	5073	28.1	4009	72.2	4567	89.7
	No	12958	71.9	1543	27.8	525	10.3

TABLE III. ESTIMATED MODEL RESULTS FOR THE FACTORS ASSOCIATED WITH E-COMMERCE USE OF INDIVIDUALS BY EDUCATION LEVELS

Variables	Elementary and lower graduation		High school graduation		University graduation	
	$\beta$	SE	$\beta$	SE	$\beta$	SE
<b>Constant</b>	-2.377 <sup>a</sup>	0.172	-1.148 <sup>a</sup>	0.193	-1.397 <sup>a</sup>	0.275
<b>Income level (reference category: £2000 and below)</b>						
£2001-£4000	0.281 <sup>a</sup>	0.08	0.11	0.101	0.451 <sup>a</sup>	0.159
£4001-£6000	0.280 <sup>a</sup>	0.108	0.26 <sup>b</sup>	0.118	0.611 <sup>a</sup>	0.168
£6001 and above	0.668 <sup>a</sup>	0.149	0.523 <sup>a</sup>	0.148	0.826 <sup>a</sup>	0.173
<b>Age (reference category: 15-24)</b>						
25-34	-0.399 <sup>a</sup>	0.093	-0.421 <sup>a</sup>	0.106	-0.007	0.152
35-44	-1.059 <sup>a</sup>	0.097	-0.832 <sup>a</sup>	0.107	-0.424 <sup>a</sup>	0.159
45-54	-1.719 <sup>a</sup>	0.111	-1.604 <sup>a</sup>	0.127	-1.188 <sup>a</sup>	0.173
55-64	-2.718 <sup>a</sup>	0.177	-2.222 <sup>a</sup>	0.176	-1.754 <sup>a</sup>	0.205
65 and above	-2.399 <sup>a</sup>	0.239	-2.673 <sup>a</sup>	0.324	-2.342 <sup>a</sup>	0.306
<b>Gender (reference category: male)</b>						
Female	-0.437 <sup>a</sup>	0.08	-0.281 <sup>a</sup>	0.085	-0.179 <sup>b</sup>	0.091
<b>Region (reference category: east)</b>						
West	0.416 <sup>a</sup>	0.098	0.278 <sup>b</sup>	0.112	0.33 <sup>a</sup>	0.118
Middle	0.451 <sup>a</sup>	0.098	0.146	0.11	0.33 <sup>a</sup>	0.117
<b>Occupation (reference category: unemployed individuals)</b>						
Managers	0.637	0.397	0.517 <sup>c</sup>	0.29	0.591 <sup>b</sup>	0.234
Professionals	1.934 <sup>a</sup>	0.6	-0.094	0.273	0.164	0.12
Technicians and associate professionals	0.475	0.674	0.721 <sup>c</sup>	0.393	0.113	0.236
Clerical support workers	0.382 <sup>c</sup>	0.227	0.207	0.157	0.084	0.152
Service/sales workers	-0.019	0.12	0.067	0.12	-0.095	0.169
Skilled agricultural/ forestry/ fishery workers	-0.801 <sup>a</sup>	0.287	-0.863 <sup>b</sup>	0.364	-0.56	0.386
Craft/related trades workers	-0.471 <sup>a</sup>	0.163	-0.142	0.213	-0.157	0.389
Plant-machine operators/ assemblers	-0.480 <sup>b</sup>	0.2	-0.382 <sup>c</sup>	0.208	-0.915 <sup>b</sup>	0.362
Elementary occupations	-0.451 <sup>a</sup>	0.104	-0.245 <sup>b</sup>	0.123	-0.635 <sup>a</sup>	0.196
<b>Number of information equipment in the household (reference category: 4 and above)</b>						
1 and below	-0.858 <sup>a</sup>	0.111	-0.896 <sup>a</sup>	0.125	-0.989 <sup>a</sup>	0.158
2-3	-0.303 <sup>a</sup>	0.092	-0.34 <sup>a</sup>	0.091	-0.506 <sup>a</sup>	0.092
<b>Number of individuals in the household (reference category: 3 and below)</b>						
4-5	-0.173 <sup>b</sup>	0.074	-0.326 <sup>a</sup>	0.08	-0.18 <sup>b</sup>	0.089
6 and above	-0.465 <sup>a</sup>	0.107	-0.5 <sup>a</sup>	0.136	-0.489 <sup>b</sup>	0.202
<b>Social media (reference category: no)</b>						
Yes	1.366 <sup>a</sup>	0.106	0.653 <sup>a</sup>	0.103	0.525 <sup>a</sup>	0.106
<b>Internet banking (reference category: no)</b>						
Yes	1.246 <sup>a</sup>	0.085	1.342 <sup>a</sup>	0.86	1.465 <sup>a</sup>	0.103
<b>E-government use (reference category: no)</b>						
Yes	-2.377 <sup>a</sup>	0.172	0.93 <sup>a</sup>	0.105	1.017 <sup>a</sup>	0.141

<sup>a</sup>p<.01; <sup>b</sup>p<.05; <sup>c</sup>p<.10

TABLE IV. MARGINAL EFFECTS OF FACTORS ASSOCIATED WITH INDIVIDUALS' USE OF E-COMMERCE BY EDUCATION LEVEL

Variables	Elementary and lower graduation		High school graduation		University graduation	
	ME	S.E	ME	S.E	ME	S.E
<b>Income level (reference category: ₹2000 and below)</b>						
₹2001-₹4000	0.248 <sup>a</sup>	0.705	0.062	0.057	0.156 <sup>a</sup>	0.059
₹4001-₹6000	0.247 <sup>b</sup>	0.952	0.143 <sup>b</sup>	0.066	0.203 <sup>a</sup>	0.061
₹6001 and above	0.579 <sup>a</sup>	0.126	0.277 <sup>a</sup>	0.077	0.26 <sup>a</sup>	0.061
<b>Age (reference category: 15-24)</b>						
25-34	-0.322 <sup>a</sup>	0.075	-0.193 <sup>a</sup>	0.049	-0.002	0.034
35-44	-0.891 <sup>a</sup>	0.081	-0.415 <sup>a</sup>	0.054	-0.108 <sup>a</sup>	0.038
45-54	-1.493 <sup>a</sup>	0.098	-0.914 <sup>a</sup>	0.08	-0.377 <sup>a</sup>	0.053
55-64	-2.448 <sup>a</sup>	0.167	-1.386 <sup>a</sup>	0.133	-0.647 <sup>a</sup>	0.085
65 and above	-2.139 <sup>a</sup>	0.226	-1.763 <sup>a</sup>	0.275	-0.997 <sup>a</sup>	0.18
<b>Gender (reference category: male)</b>						
Female	-0.382 <sup>a</sup>	0.069	-0.152 <sup>a</sup>	0.046	-0.051 <sup>b</sup>	0.026
<b>Region (reference category: east)</b>						
West	0.369 <sup>a</sup>	0.088	0.154 <sup>b</sup>	0.063	0.101 <sup>a</sup>	0.038
Middle	0.399 <sup>a</sup>	0.087	0.082	0.063	0.102 <sup>a</sup>	0.037
<b>Occupation (reference category: unemployed individuals)</b>						
Managers	0.533 <sup>c</sup>	0.321	0.256 <sup>c</sup>	0.132	0.148 <sup>a</sup>	0.053
Professionals	1.487 <sup>a</sup>	0.435	-0.052	0.152	0.046	0.034
Technicians and associate professionals	0.401	0.555	0.344 <sup>b</sup>	0.164	0.032	0.066
Clerical support workers	0.324 <sup>c</sup>	0.189	0.108	0.08	0.024	0.043
Service/sales workers	-0.016	0.104	0.036	0.064	-0.029	0.051
Skilled agricultural/ forestry/ fishery workers	-0.716 <sup>a</sup>	0.264	-0.531 <sup>b</sup>	0.25	-0.189	0.147
Craft/related trades workers	-0.416 <sup>a</sup>	0.146	-0.079	0.12	-0.048	0.123
Plant-machine operators/ assemblers	-0.424 <sup>b</sup>	0.179	-0.219 <sup>c</sup>	0.125	-0.337 <sup>b</sup>	0.16
Elementary occupations	-0.398 <sup>a</sup>	0.093	-0.137 <sup>c</sup>	0.07	-0.218 <sup>a</sup>	0.075
<b>Number of information equipment in the household (reference category: 4 and above)</b>						
1 and below	-0.752 <sup>a</sup>	0.096	-0.502 <sup>a</sup>	0.072	-0.305 <sup>a</sup>	0.057
2-3	-0.258 <sup>a</sup>	0.078	-0.174 <sup>a</sup>	0.045	-0.137 <sup>a</sup>	0.024
<b>Number of individuals in the household (reference category: 3 and below)</b>						
4-5	-0.15 <sup>b</sup>	0.064	-0.174 <sup>a</sup>	0.042	-0.052 <sup>b</sup>	0.026
6 and above	-0.409 <sup>a</sup>	0.095	-0.274 <sup>a</sup>	0.078	-0.152 <sup>b</sup>	0.069
<b>Social media (reference category: no)</b>						
Yes	1.234 <sup>a</sup>	0.099	0.384 <sup>a</sup>	0.06	0.166 <sup>a</sup>	0.037
<b>Internet banking (reference category: no)</b>						
Yes	1.065 <sup>a</sup>	0.071	0.76 <sup>a</sup>	0.051	0.53 <sup>a</sup>	0.046
<b>E-government use (reference category: no)</b>						
Yes	0.790 <sup>a</sup>	0.071	0.557 <sup>a</sup>	0.069	0.366 <sup>a</sup>	0.062

<sup>a</sup>p<.01; <sup>b</sup>p<.05; <sup>c</sup>p<.10

For individuals with high school graduation, the likelihood of an individual with an income of £6001 and above to use e-commerce is 27.7% more than an individual with an income of £2000 and lower (reference group). A 25-34 years old individual with a high school graduation is 19.3% less likely to use e-commerce than a 15-24 years old individual. The likelihood of an individual with high school graduation and in 65 and above age range to use e-commerce is 176.3% less than a 15-24 years old individual. A female with a high school graduation is 15.2% less likely to use e-commerce than a male with same degree graduation. The likelihood of an individual with a high school graduation in the west region to use e-commerce is 15.4% less than an individual in the east region. The likelihood of an individual with a high school graduation as well as a technicians and associate professional to use e-commerce is 34.4% more than a unemployed individual. The likelihood of an individual with a high school graduation as well as a skilled agricultural/forestry/fishery workers to use e-commerce is 53.1% less than a unemployed individual. The likelihood of an individual with a high school graduation in households with 1 or less information equipment is 50.2% less than an individual in a household with 4 or more information equipment. An individual with a high school graduation in a household with 6 and above individuals is 27.4% less likely to use e-commerce than an individual in a household with 3 and lower individuals. The likelihood of an individual with a high school graduation as well as using social media to use e-commerce is 38.4% higher than an individual not using social media. An individual with a high school graduation as well as a using internet banking is 76% more likely to use e-commerce than an individual not using internet banking. The likelihood of an individual with a high school graduation as well as a using e-government to use e-commerce is 55.7% higher than an individual not using this application.

For individuals with a university degree graduation, the likelihood of an individual with an income of £6001 and above to use e-commerce is 26% more than an individual with an income of £2000 and lower (reference group). A 35-44 years old individual with a university degree graduation is 41.5% less likely to use e-commerce than a 15-24 years old individual. The likelihood of an individual with a university degree graduation and in 65 and above age range to use e-commerce is 99.7 % less than a 15-24 years old individual. A female with a university degree graduation is 5.1% less likely to use e-commerce than a male with the same degree graduation. The likelihood of an individual with a university degree graduation in the west region to use e-commerce is 10.1% less than an individual in the east region. The likelihood of an individual with a university degree graduation as well as a manager to use e-commerce is 14.8% more than a unemployed individual. The likelihood of an individual with a university degree graduation as well as a Plant-machine operators/assembler to use e-commerce is 33.7% less than a unemployed individual. The likelihood of an individual with a university degree graduation in households with 1 or less information equipment is 30.5% less than an individual in a household with 4 or more information equipment. An individual with a university degree graduation in a household with 6 and above individuals is 15.2% less likely to use e-commerce than an individual in a household with 3 and lower

individuals. The likelihood of an individual with a university degree graduation as well as using social media to use e-commerce is 16.6% less than an individual not using social media. An individual with a university degree graduation as well as a using internet banking is 53% more likely to use e-commerce than an individual not using internet banking. The likelihood of an individual with a university degree as well as a using e-government to use e-commerce is 36.6% higher than an individual not using this application.

## V. DISCUSSION

The rapid growth of online shopping activities in recent years has required a careful description of the main factors affecting consumers' behavior and attitudes towards online shopping. Individuals use e-commerce in several different types and for various reasons. As it is known that demographic characteristics affect the actions of individuals before displaying a certain behavior, the differences regarding internet use among demographic groups in various aspects have become an interesting area of research. It is of importance that the factors related to online shopping should be understood both by e-commerce suppliers and online shoppers. Education is a significant factor affecting the decision-making process of a customer in online shopping, and the effect of education level on online consumption is getting more important.

In this study, the data regarding 28675 individuals participated in the Household Information Technologies Usage Survey performed by the Turkish Statistical Institute in 2019. In addition, the factors affecting e-commerce use of individuals in Turkey have been determined according to their education levels by utilizing binary logistic regression.

In this study, the variables of income level, age, gender, occupation, region, social media use, internet banking use, e-government use, number of information equipment in a household and the number of people in a household have been found to be related to e-commerce use.

As the income levels of individuals increase, their likelihood to use e-commerce increases. Other studies have also reached similar conclusions [47, 48]. It was reported in a study carried out in New Zealand that the higher an individual's income, the more s/he trusts sales on internet [49].

It has been concluded in the study that as the age of the individuals increase, their possibility of using e-commerce decrease. Parallel results have been found in different studies [3, 50]. Age is one of the factors affecting the attitudes of individuals to use e-commerce, thus, different age groups may have different tendencies regarding e-commerce [51]. On the other hand, prior studies show that as the age of individuals increase, their likelihood to use e-commerce increases [52]. It has been found out in a study conducted in New Zealand that the time used by elders for e-commerce on internet is not less than the time spent by other age groups [49].

It has been achieved that the likelihood of males to use e-commerce is higher than females. Other studies have also arrived at similar conclusions [53, 54]. It has been reported in a study that males have significantly more internet knowledge, computer understanding and experience compared to females [10]. It has been stated in another study that females are more

anxious and less self-confident than males about computer, internet use and e-commerce [55].

It has been also identified that the likelihood of the individuals living in the western region to use e-commerce has been more than the individuals living in middle and eastern regions. The digital divide between regions with different levels of development affects how telecommunications and other advanced technologies are used [56]. Socioeconomic factors influence the use of information and communication technologies, and cause regional differences [57]. Different regions have different infrastructures, economies and populations, and this leads an environmental diversification of the location [58]. Therefore, this affects the difference between the shopping made by individuals on internet according to regions [59].

It has been found out that the e-commerce use of the individuals using social media is more than the individuals not using social media. The individuals managing a social media account may involve in more purchasing transactions through online channels. Parallel results have been found in different studies [60-62].

e-Commerce use of the individuals using internet banking is more than other individuals. Other studies have also arrived at similar conclusions [60, 63]. It has been reported in a study that increase in internet access and growth in internet banking have resulted in a significant increase in e-commerce use [60].

In the study, it has been concluded that the e-commerce use of the individuals using e-government services is more than other individuals. Parallel results have been found in different studies [37, 64].

The study also urges that as the number of information equipment increases, the possibility of using e-commerce increases. Other studies have also arrived at similar conclusion [39, 47, 65]. It has been found out in a study that the increase in telephone numbers in families has increased the likelihood of online shopping [65].

It has been concluded in the study that as the household size increases, the likelihood to use e-commerce decreases. Parallel results have been found in different studies [39]. The effect of number of children on e-commerce use has been identified to be negative, little but insignificant in a study [66]. On the other hand, there are also studies that the effect of the number of children is the positive way on e-commerce use [67].

It has been found out that the significance and effects of variables in e-commerce use show differences according to educational levels of individuals. It has been concluded that as the education level of individuals' increase, the possibility of using e-commerce increase. The customers with different educational levels have different expectations and perceived service quality value. Our results show that the higher the education level of individuals, the higher their tendency towards online shopping. Higher education level refers to higher income level at both state and private institutions and more perception towards innovations. This has naturally a positive effect on online shopping behaviors of individuals.

## ACKNOWLEDGMENT

The authors would like to thank the Turkish Statistical Institute for the data. The views and opinions expressed in this manuscript are those of the authors only and do not necessarily represent the views, official policy, or position of the Turkish Statistical Institute.

## REFERENCES

- [1] Erceg, A. and Z. Kilic. Interconnection of e-commerce and logistics: examples from Croatia and Turkey. in *Business Logistics in Modern Management*. 2018. Osijek, Croatia: Boris Crnković, Dean of Faculty of Economics in Osijek.
- [2] Huseynov, F. and S.Ö. Yıldırım, Internet users' attitudes toward business-to-consumer online shopping: A survey. *Information Development*, 2016. 32(3): p. 452-465.
- [3] Akman, I. and M. Rehan, Online purchase behaviour among professionals: a socio-demographic perspective for Turkey. *Economic Research-Ekonomiska Istrazivanja*, 2014. 27(1): p. 689-699.
- [4] Çelik, H.E. and V. Yılmaz, Extending the technology acceptance model for adoption of e-shopping by consumers in Turkey. *Journal of Electronic Commerce Research*, 2011. 12(2): p. 152-164.
- [5] Gümüş, R. and A. Kısa. Analysis of usability of web sites in hospitals in Diyarbakır, Turkey. in *3rd International Conference on Education, Social Sciences and Humanities*. 2016. İstanbul: Socioint 2016.
- [6] Kawa, A. and W. Zdrenka, Conception of integrator in cross-border e-commerce. *LogForum*, 2016. 12(1): p. 63-73.
- [7] Gökmen, A., Virtual business operations, e-commerce & its significance and the case of Turkey: current situation and its potential. *Electronic Commerce Research*, 2012. 12(1): p. 31-51.
- [8] Kaya, B., et al., The moderating role of website familiarity in the relationships between e-service quality, e-satisfaction and e-loyalty. *Journal of Internet Commerce*, 2019. 18(4): p. 369-394.
- [9] TÜBİSAD. E-Commerce in Turkey 2018 Market Size. 2018; Available from: [https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/TUB%C4%B0SAD\\_2019\\_Ecommerce\\_ENG.pdf](https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/TUB%C4%B0SAD_2019_Ecommerce_ENG.pdf).
- [10] Potosky, D., The Internet knowledge (iKnow) measure. *Computers in Human Behavior*, 2007. 23(6): p. 2760-2777.
- [11] AlGhamdi, R., A. Nguyen, and V. Jones, A study of influential factors in the adoption and diffusion of B2C e-commerce. *International Journal of Advanced Computer Science and Applications*, 2013. 4(1): p. 89-94.
- [12] Ono, H. and M. Zavodny, Digital inequality: A five country comparison using microdata. *Social Science Research*, 2007. 36(3): p. 1135-1155.
- [13] Zhang, Y., Age, gender, and Internet attitudes among employees in the business world. *Computers in Human Behavior*, 2005. 21(1): p. 1-10.
- [14] Yang, S.C. and C.-J. Tung, Comparison of Internet addicts and non-addicts in Taiwanese high school. *Computers in Human Behavior*, 2007. 23(1): p. 79-96.
- [15] Cheung, C.M., G.W. Chan, and M. Limayem, A critical review of online consumer behavior: Empirical research. *Journal of Electronic Commerce in Organizations* 2005. 3(4): p. 1-19.
- [16] Lightner, N.J., What users want in e-commerce design: effects of age, education and income. *Ergonomics*, 2003. 46(1-3): p. 153-168.
- [17] Sim, L.L. and S.M. Koi, Singapore's Internet shoppers and their impact on traditional shopping patterns. *Journal of Retailing and Consumer Services*, 2002. 9(2): p. 115-124.
- [18] Teo, T.S. and V.K. Lim, Gender differences in internet usage and task preferences. *Behaviour & Information Technology*, 2000. 19(4): p. 283-295.
- [19] Duch-Brown, N., et al., The impact of online sales on consumers and firms. Evidence from consumer electronics. *International Journal of Industrial Organization*, 2017. 52: p. 30-62.
- [20] Pan, X., B.T. Ratchford, and V. Shankar, The evolution of price dispersion in internet retail markets, in *Organizing the New Industrial Economy (Advances in Applied Microeconomics)*, M.R. Baye, Editor. 2003, Emerald Group Publishing Limited: Bingley. p. 85-105.

- [21] Li, B., et al., Key influencing factors of consumers' vegetable e-commerce adoption willingness, behavior, and willingness-behavior consistency in Beijing, China. *British Food Journal*, 2020.
- [22] Crespo, A.H. and I.R. Del Bosque, The influence of the commercial features of the Internet on the adoption of e-commerce by consumers. *Electronic Commerce Research and Applications*, 2010. 9(6): p. 562-575.
- [23] Castro-Lopez, A., J. Puente, and R. Vazquez-Casielles, Fuzzy inference suitability to determine the utilitarian quality of B2C websites. *Applied Soft Computing*, 2017. 57: p. 132-143.
- [24] He, P., S. Zhang, and C. He, Impacts of logistics resource sharing on B2C E-commerce companies and customers. *Electronic Commerce Research and Applications*, 2019. 34: p. 100820.
- [25] Kang, J.-W. and Y. Namkung, The information quality and source credibility matter in customers' evaluation toward food O2O commerce. *International Journal of Hospitality Management*, 2019. 78: p. 189-198.
- [26] Shen, C.-w., M. Chen, and C.-c. Wang, Analyzing the trend of O2O commerce by bilingual text mining on social media. *Computers in Human Behavior*, 2019. 101: p. 474-483.
- [27] Zhang, J., H. Chen, and X. Wu, Operation models in O2O supply chain when existing competitive service level. *International Journal of u-and e-Service, Science and Technology*, 2015. 8(9): p. 279-290.
- [28] Jamaluddin, N., Adoption of e-commerce practices among the indian farmers, a survey of Trichy District in the State of Tamilnadu, India. *Procedia Economics and Finance*, 2013. 7: p. 140-149.
- [29] Grandón, E.E., S.A. Nasco, and P.P. Mykytyn Jr, Comparing theories to explain e-commerce adoption. *Journal of Business Research*, 2011. 64(3): p. 292-298.
- [30] Sin, K.Y., et al., Relative advantage and competitive pressure towards implementation of e-commerce: Overview of small and medium enterprises (SMEs). *Procedia Economics and Finance*, 2016. 35: p. 434-443.
- [31] Rana, N.P., et al., Exploring barriers of m-commerce adoption in SMEs in the UK: Developing a framework using ISM. *International Journal of Information Management*, 2019. 44: p. 141-153.
- [32] Chau, N.T. and H. Deng, Critical determinants for mobile commerce adoption in Vietnamese SMEs: A conceptual framework. *Procedia Computer Science*, 2018. 138: p. 433-440.
- [33] Yang, B. and D. Lester, Gender differences in e-commerce. *Applied Economics*, 2005. 37(18): p. 2077-2089.
- [34] Baer, A.G. and C. Brown, Adoption of e-marketing by direct-market farms in the Northeastern United States. *Journal of Food Distribution Research*, 2007. 38(2): p. 1-11.
- [35] Sismeiro, C. and R.E. Bucklin, Modeling purchase behavior at an e-commerce web site: A task-completion approach. *Journal of Marketing Research*, 2004. 41(3): p. 306-323.
- [36] Solaymani, S., K. Sohaili, and E.A. Yazdinejad, Adoption and use of e-commerce in SMEs. *Electronic Commerce Research*, 2012. 12(3): p. 249-263.
- [37] Akman, I. and A. Mishra, Gender, age and income differences in internet usage among employees in organizations. *Computers in Human Behavior*, 2010. 26(3): p. 482-490.
- [38] Alkan, Ö., H. Küçükoğlu, and G. Tutar, Modeling of the factors affecting e-commerce use in Turkey by categorical data analysis. *International Journal of Advanced Computer Science and Applications*, 2021. 12 (1): p. 95-105.
- [39] Abar, H. and Ö. Alkan, What Factors Influence the Use of Electronic Commerce?: A Case in Turkey, in *Handbook of Research on IT Applications for Strategic Competitive Advantage and Decision Making*, E.C. Idemudia, Editor. 2020, IGI Global. p. 101-117.
- [40] Durmuş, B., Y. Uluşu, and Ş. Erdem, Which dimensions affect private shopping e-customer loyalty? *Procedia-Social and Behavioral Sciences*, 2013. 99: p. 420-427.
- [41] Zehir, C. and E. Narçıkara, E-service quality and e-recovery service quality: Effects on value perceptions and loyalty intentions. *Procedia-Social and Behavioral Sciences*, 2016. 229: p. 427 – 443.
- [42] TÜİK. Hanehalkı Bilişim Teknolojileri Kullanım Araştırması. 2019 24.11.2020; Available from: [https://www.tuik.gov.tr/Kurumsal/Mikro\\_Veri#](https://www.tuik.gov.tr/Kurumsal/Mikro_Veri#).
- [43] Alkan, Ö., H. Abar, and A. Karaaslan, Evaluation of determinants on number of various information equipment at households in Turkey. *International Journal of Business, Humanities and Technology*, 2015. 5(5): p. 24-32.
- [44] Alkan, Ö. and H. Abar, Determination of factors influencing tobacco consumption in Turkey using categorical data analyses. *Archives of Environmental & Occupational Health*, 2020. 75(1): p. 27-35.
- [45] Alkan, Ö. and Ş. Ünver, Determinants of domestic physical violence against women in Turkey. *Humanities & Social Sciences Reviews*, 2020. 8(6): p. 55-67.
- [46] Alkan, Ö. and Ş. Ünver, Tobacco smoke exposure among women in Turkey and determinants. *Journal of Substance Use*, 2021.
- [47] Cristóbal-Fransi, E., E. Martín-Fuentes, and N. Daries-Ramon, Behavioural analysis of subjects interacting with information technology: categorising the behaviour of e-consumers. *International Journal of Services Technology and Management*, 2015. 21(1-3): p. 163-182.
- [48] Vicente, M., Determinants of C2C e-commerce: an empirical analysis of the use of online auction websites among Europeans. *Applied Economics Letters*, 2015. 22(12): p. 978-981.
- [49] Smith, P., et al., The Internet: social and demographic impacts in Aotearoa New Zealand. *Observatorio (OBS\*) Journal*, 2008. 6: p. 307-330.
- [50] Alqahtani, A.S., R.D. Goodwin, and D.B. de Vries, Cultural factors influencing e-commerce usability in Saudi Arabia. *International Journal of Advanced and Applied Sciences*, 2018. 5(6): p. 1-10.
- [51] Hwang, W., H.-S. Jung, and G. Salvendy, Internationalisation of e-commerce: a comparison of online shopping preferences among Korean, Turkish and US populations. *Behaviour & Information Technology*, 2006. 25(1): p. 3-18.
- [52] Koyuncu, C. and D. Lien, E-commerce and consumer's purchasing behaviour. *Applied Economics*, 2003. 35(6): p. 721-726.
- [53] Hashim, A., E.K. Ghani, and J. Said, Does consumers' demographic profile influence online shopping?: An examination using Fishbein's theory. *Canadian Social Science*, 2009. 5(6): p. 19-31.
- [54] Escobar-Rodríguez, T., M.A. Grávalos-Gastaminza, and C. Pérez-Calañas, Facebook and the intention of purchasing tourism products: moderating effects of gender, age and marital status. *Scandinavian Journal of Hospitality and Tourism*, 2017. 17(2): p. 129-144.
- [55] DeYoung, C.G. and I. Spence, Profiling information technology users: En route to dynamic personalization. *Computers in Human Behavior*, 2004. 20(1): p. 55-65.
- [56] Donnermeyer, J.F. and C.A. Hollifield, Digital divide evidence in four rural towns. *IT & Society*, 2003. 1(4): p. 107-117.
- [57] Cullen, R., The digital divide: a global and national call to action. *The Electronic Library*, 2003. 21(3): p. 247-257.
- [58] Mills, B.F. and B.E. Whitacre, Understanding the Non - Metropolitan—Metropolitan Digital Divide. *Growth and Change*, 2003. 34(2): p. 219-243.
- [59] Wilson, K.R., J.S. Wallin, and C. Reiser, Social stratification and the digital divide. *Social Science Computer Review*, 2003. 21(2): p. 133-143.
- [60] Çera, G., et al., Financial capability and technology implications for online shopping. *E&M Economics and Management*, 2020. 23(2): p. 156-172.
- [61] Hubert, M., et al., Acceptance of smartphone - based mobile shopping: Mobile benefits, customer characteristics, perceived risks, and the impact of application context. *Psychology & Marketing*, 2017. 34(2): p. 175-194.
- [62] Pucci, T., et al., Does social media usage affect online purchasing intention for wine? The moderating role of subjective and objective knowledge. *British Food Journal*, 2019. 11(2): p. 275-288.
- [63] Duroy, D., P. Gorse, and M. Lejoyeux, Characteristics of online compulsive buying in Parisian students. *Addictive Behaviors*, 2014. 39(12): p. 1827-1830.
- [64] Akman, I., et al., E-Gov: A global perspective and an empirical assessment of citizens' attributes. *Government Information Quarterly*, 2005. 22(2): p. 239-257.

- [65] Hossein, K.M., et al., Factors Associated to Online Shopping at the BoP Community in Rural Bangladesh. *International Journal of Advanced Computer Science and Applications*, 2017. 8(10): p. 46-51.
- [66] Stranahan, H. and D. Kosiel, E - tail spending patterns and the importance of online store familiarity. *Internet Research*, 2007. 17(4): p. 421-434.
- [67] Leong, L.-Y., N.I. Jaafar, and S. Ainin, Understanding Facebook Commerce (F-Commerce) Actual Purchase from an Artificial Neural Network Perspective. *Journal of Electronic Commerce Research*, 2018. 19(1): p. 75-103.

# Fuzzy based Techniques for Handling Missing Values

Malak El-Bakry<sup>1</sup>, Ayman El-Kilany<sup>3</sup>, Sherif Mazen<sup>4</sup>

Information Systems Department  
Faculty of Computers and Information  
Cairo University, Cairo, Egypt

Farid Ali<sup>2</sup>

Information Technology Department  
Faculty of Computers and Information  
Beni-suef University, Egypt, Cairo, Egypt

**Abstract**—Usually, time series data suffers from high percentage of missing values which is related to its nature and its collection process. This paper proposes a data imputation technique for imputing the missing values in time series data. The Fuzzy Gaussian membership function and the Fuzzy Triangular membership function are proposed in a data imputation algorithm in order to identify the best imputation for the missing values where the membership functions were used to calculate weights for the data values of the nearest neighbor's before using them during imputation process. The evaluation results show that the proposed technique outperforms traditional data imputation techniques where the triangular fuzzy membership function has shown higher accuracy than the gaussian membership function during evaluation.

**Keywords**—Time series data; fuzzy logic; membership functions; machine learning; missing values

## I. INTRODUCTION

In computer science field, the data quality problem began to rise in the 1990s with arise of the data warehouse systems where the failure of a database project was returned to its poor data quality. [1] There is a lot of definitions for the word “data quality” but as mentioned in [2] there is a well-known definition used by a lot of researchers which is “fitness for use”. Data quality can be mainly summarized in how the system fits into the reality, or how users really utilize the data in the system. [2].

Data quality can be assessed in terms of data quality dimensions. These data quality dimensions consist of timelines to ensure that the value is new, consistency to ensure that representation of the data is unchanging in all cases, completeness to ensure that the data is completed with no missing values, and accuracy to ensure that the recorded value is identical with the actual value. [1].

Incompleteness of data is a natural phenomenon as the data is usually generated, entered, or collected with missing values. Missing data can be defined as the values that are not stored for a variable in the observation of interest. There are three types of missingness of the data. First, the missing completely at random (MCAR): the variable is missing completely at random where the probability of missingness is the same for all missing variables. Second, the Missing at random (MAR): Variable is missing at random where the probability of missingness is depending only on an available information. This type can also be named as missing conditionally which means missing with a condition; for an example if gender is male, they will leave questions related to women in the survey empty. Third, the Not Missing at

Random (NMAR) data where the missingness probability is not random and it depends on the variable itself and can't be predicted from another variable in the dataset. [3].

Missing data occurs in many types of the data sets but in specific it occurs with a very high percentage in the time series data. Time series data is a type of data that usually have incompleteness given to its nature. Time series data exist in nearly every scientific field, where data are measured, recorded, and monitored over time. Consequently, it is understandable that missing values may occur. Also, most of the time series data are collected by sensors and machines which is another reason for the occurrence of the missing values. [4].

This paper aims to ensure the data quality of time series data. More specifically, it aims to ensure the completeness dimensions of the time series data that suffers from missing value. Towards this aim, two novel techniques for imputing the missing values in time series data are proposed and compared with traditional techniques. The two proposed techniques impute the missing value by calculating the k-nearest neighbour between the missing value and the other values. Then it calculates a weight for each value in the nearest neighbours using fuzzy membership functions. Two fuzzy membership functions are used which are: the gaussian membership function and the triangular membership function. After calculating the weights, the data values and their weights are used in the weighted mean function to calculate the imputed value. The accuracy of the proposed techniques is evaluated by using three traditional classifiers: Neural Network, Naïve Bayes, and Decision Tree. Evaluation Results shows that the two proposed techniques have higher accuracy than the traditional data imputing techniques. In addition, it also shows that the triangular membership function yields higher accuracy rather than the gaussian membership function.

The rest of this paper is organized as follows: Section 2 presents the related work and some techniques used in imputing the missing values. Section 3 and 4 includes the summarization of the proposed techniques and the results. Finally, the paper is concluded in section 5.

## II. RELATED WORK

A lot of methods with different techniques have been proposed in the literature to solve the missing data problem. The management of missing data can be divided into three categories; deletion and ignoring methods; imputations methods and model-based methods. These categories will be discussed below with more details.

### A. Deletion and Ignoring Methods

Deletion/Ignorance of missing values is recognized as the simplest way in handle missing values. Authors in [5] proposed the traditional techniques for dealing with missing data. The listwise deletion algorithm was proposed where an entire record is excluded from the data set if any value is missing. The pairwise deletion method was also proposed where the method computes the correlation between missing and complete data to pair the correlated values and it only delete the un-correlated values. Listwise deletion would result in removing more data than the pairwise method. The drawback of this method is that it may be very risky in case of the missingness is a large portion of the data as it may interrupt the results of the analysis.

### B. Imputation Methods

The imputation methods work by substituting each of the missing values by an estimate value. The hot and cold deck imputation is one of the best methods used in missing data imputation. In [6], they used the cold deck imputation for variables where it uses external sources such as a value from a previous survey. It imputes missing values called as recipients using similar reported values from previous survey. Cold deck imputation was performed through probabilistic record linkage techniques in order to find the best matching records from different data sources containing the same set of entities.

Another imputation technique was proposed by authors in [7] to generate an estimate value for the missing values. In [7], the authors proposed a technique that considers multiple imputations for imputing missing values. This technique works by imputing missing values n-times to correspond to the uncertainty of all the possible values that can be imputed. Then the values are analyzed in order to get a combined single estimate. As an example, you can choose two different techniques and use them together so you can take advantages of both techniques and avoid the disadvantages of these techniques.

### C. Model-Based Methods

The model-based methods are the methods which imputes the missing values by using a predictive technique. These methods are mainly machine learning techniques that needs learning phase to be able to estimate missing values.

In [8], the authors work on the weather data for environmental factors and found out that this data set contains a lot of missing values. They calculated the percentage of missingness in the data to found out that 19% of the weather data for 2017 are missed. This percentage is big in these types of data and can cause misleading during the analysis that will be done on it. Four missing data imputation was applied on this data set. They divided the data sets into training and testing to measure the quality of the four imputation algorithms. The k-nearest neighbor (KNN) method results were the best results, and its results was so close to the original data with no missing values and the prediction model's performance is stable even when the missing data rate increases.

In [9], authors implemented a new approach that is based on vector autoregressive (VAR) model by combining prediction error minimization (PEM) method with expectation

and minimization (EM) algorithm. They called this algorithm a vector autoregressive imputation method (VAR-IM). Their proposed system is applied on a real-world data set involving electrocardiogram (ECG) data. They used linear regression substitution and list wise detection as a traditional method to be compared with their proposed method VAR-IM. They concluded that the proposed method VAR-IM produced a large improvement of the imputation tasks as compared to the traditional techniques. This technique has three limitations, the first one is it only deal with data that is missing completely at random. The second limitation is the validity of the approach requires that the time series should be stationary. The third limitation is the percentage of missing data has significant impact on most missing data analysis methods, the proposed technique does not have the priority to be used if the percentage of missing data is quite low (say less 10%). Despite these limitations, the proposed technique provides an important alternative to existing methods for handling missing data in multivariate time series.

In [10], the authors propose a genetic algorithm (GA) based technique to estimate the missing values in datasets. GA is introduced to generate optimal sets of missing values and information gain (IG) is used as the fitness function to measure the performance of an individual solution. Their goal is to impute missing values in a dataset for better classification results. This technique works even better when there is a higher rate of missing values or incomplete information along with a greater number of distinct values in attributes/features having missing values. They compared their proposed technique with single imputation techniques and multiple imputations (MI) statistically based approaches on various benchmark classification techniques on different performance measures. They show that the proposed methods outperform when compared with another state-of-the-art missing data imputation techniques.

In [11], the authors used the gene expression data that are recognized as a common data source which contains missing expression values. In this paper, they present a genetic algorithm optimized k- Nearest neighbour algorithm (Evolutionary KNN Imputation) for missing data imputation. They focused on local approach where the proposed Evolutionary k- Nearest Neighbour Imputation Algorithm falls in. The Evolutionary k- Nearest Neighbour Imputation Algorithm is an extension of the common k- nearest Neighbour Imputation Algorithm which the genetic algorithm is used to optimize some parameters of k- Nearest Neighbour Algorithm. The selection of similarity matrix and the selection of the parameter value k can be identified as the optimization problem. They compared the proposed Evolutionary k-Nearest Neighbour Imputation algorithm with k- Nearest Neighbour Imputation algorithm and mean imputation method. Results show that Evolutionary KNN Imputation outperforms KNN Imputation and mean imputation while showing the importance of using a supervised learning algorithm in missing data estimation. Even though mean imputation happened to show low mean error for a very few missing rates, supervised learning algorithms became effective when it comes to higher missing rates in datasets which is the most common situation among datasets.

### III. PROPOSED TECHNIQUE

In this paper, two techniques are proposed for imputing missing values in time series data. The two proposed techniques start by finding the K nearest neighbor data points for each data point containing a missing value for a certain feature. Then, the values of the missing feature in the nearest neighbor's data points are weighted using one of the two fuzzy membership functions: triangular fuzzy membership function and gaussian membership function. The missing feature value is then obtained using the weighted mean of the feature in nearest neighbors. Fig.1 Show the steps of the proposed technique.

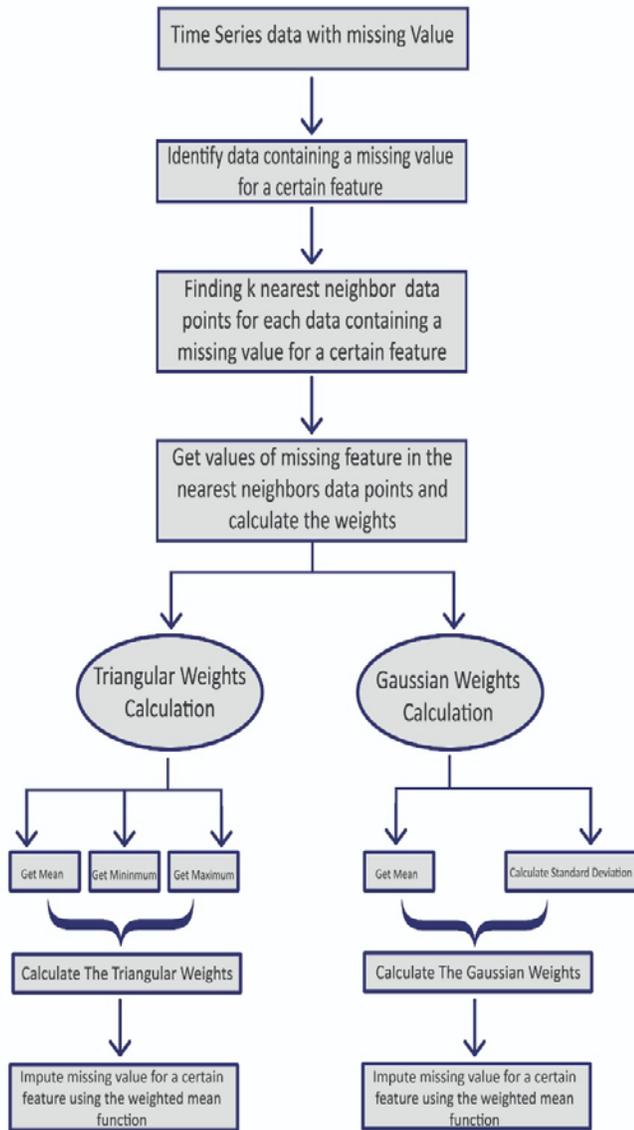


Fig. 1. Proposed Technique Block Diagram.

Two weighted functions are used to get the weight of each one of the nearest neighbors' data points for a certain missing feature before using them to impute the missing value. The triangular and the gaussian membership functions. The triangular membership weight function works by calculating the minimum, the maximum and the average of the nearest neighbors' values of the missing feature. Then, it calculates the weight for each value by using the triangular fuzzy membership function. Finally, the values and their weights are used in the weighted mean function to get the value of the missing data. Algorithm 1 show the exact details of Triangular fuzzy membership function.

#### Algorithm 1: Triangular fuzzy membership Function

1: Function Triangular fuzzy membership weights (Nearest Neighbors Values for the missing features)

Input: Nearest Neighbors Values for the missing features

Output: Missing feature value

2: Minimum= Minimum value of (Nearest Neighbors Values for the missing features)

3: Maximum= Maximum value of (Nearest Neighbors Values for the missing features)

4: Mean= Mean value of (Nearest Neighbors Values for the missing features)

5: Get weight for each Nearest Neighbors Values for the missing features using Triangular fuzzy membership function

Triangular function is defined by a minimum value a, a maximum value b, and a mean value m, where  $a < m < b$ .

$$\mu(x) = \begin{cases} 0 & x \leq a \\ \frac{x-a}{m-a} & a < x \leq m \\ \frac{b-x}{b-m} & m < x < b \\ 0 & x \geq b \end{cases}$$

6: Missing feature value = Calculate weighted mean using Nearest Neighbors Values for the missing features and weights for each one

$$\frac{\sum_{a \in A} \text{Nearest Neighbours Values}(a) \text{Triangular weight}(a)}{\sum_{a \in A} \text{Triangular weight}(a)}$$

7: End

The Gaussian membership weigh function works by calculating the mean, and the standard deviation of the nearest neighbors' values of the missing feature. Then, it calculates the weight for value by using the Gaussian fuzzy membership function. Finally, the values and their weights are used in the weighted mean function to get the value of the missing data. Algorithm 2 show the exact details of Gaussian fuzzy membership function.

TABLE I. DATA SETS

Data Set	Name	No of Samples	No of Attributes	No of class	Percentage of missingness
Data set 1	Ozone Level Detection [13]	2536	73	2	1.28%
Data set 2	Data for Software Engineering Teamwork Assessment in Education Setting [13]	74	102	2	15.9%
Data set 3	Hybrid Indoor Positioning Dataset from WiFi RSSI, Bluetooth and magnetometer Data Set [13]	1540	65	2	27.3%
Data set 4	India COVID-19 data [14]	4838	7	70	2%
Data set 5	Us COVID-19 data [14]	8500	6	31	1.60%
Data set 6	HPI master [14]	4236	8	3	37.1%

Algorithm 2: Gaussian fuzzy membership function

1: Function Gaussian fuzzy membership weights (Nearest Neighbors Values for the missing features)  
Input: Nearest Neighbors Values for the missing features  
Output: Missing feature value

2: Standard Deviation = Standard deviation of (Nearest Neighbors Values for the missing features)  
3: Mean= Mean value of (Nearest Neighbors Values for the missing features)  
4: Get weight for each data value using Gaussian fuzzy membership function

$$f(x) = e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

5: Missing feature value = Calculate weighted mean using data value and weights for each one

$$\frac{\sum_{a \in A} \text{Nearest Neighbours Values } (a) \text{Gaussian weight } (a)}{\sum_{a \in A} \text{Gaussian weight } (a)}$$

6: End

IV. PERFORMANCE EVALUATION AND DISCUSSION

The objective of performance evaluation is to prove the effectiveness of the proposed technique against standard imputation techniques. Towards this objective, the proposed techniques were evaluated on six datasets with different percentages of missing values. The proposed methods were evaluated against traditional imputation techniques. All algorithms were evaluated using accuracy measure after considering a classification scenario on the data after imputation to find out the quality of the imputed data where three different classifiers were used. [12].

Six different Time series data sets were used in this paper. The datasets are chosen with missing values due to machine malfunctions, and simple human errors. The data available to build time series models are often characterized by missing values, due to various causes such as sensor faults, problems of not reacting experiments, not recovering work situations, transferring data to digital systems. Table 1 shows the details of each dataset.

Each data set was divided into training and testing sets. The training set are 75% of the whole dataset while the remaining 25% is considered as the testing set. Accuracy is used as an evaluation metric where the accuracy is obtained after using three well-known classification methods on Different 6 data sets. The classifiers are the Decision tree, Naive Bayes and artificial neural network classifiers. The artificial neural networks architecture is; 3 hidden layers and 200 epochs. Four imputation methods are used, the two proposed methods (Gaussian weighted mean and Triangular weighted mean) and two traditional methods (Average and weighted mean) [15, 16]. The accuracy between the 4 methods is computed. Results of the proposed and traditional techniques over the 6 datasets are summarized in the figures respectively.

As shown in Fig [2] to Fig [7], the two proposed techniques using fuzzy algorithms [17][18] gives higher accuracy than the traditional techniques. Fuzzy logic performs better than the non-fuzzy since fuzzy logic has the advantage of being grey not black nor white. As fuzzy logic uses membership functions, it can answer the uncertainties generated from non-fuzzy logics where you must choose between two options. Membership functions gives each value a membership value in each class rather than a binary decision “belongs to or not belong to”. Fuzzy logic has multiple membership functions (Gaussian, triangular, Trapezium, ...etc). Membership functions are equally good in performance but usually Gaussian and triangular MFs are found to be closely performing well and better than other types of membership functions. The choice of which of the functions to use depends entirely on the size, problem type and data distribution.

The evaluation results show that the proposed triangular weighted mean technique performs better in terms of accuracy than that of the proposed gaussian weighted mean technique. Triangular MF has many advantages over the gaussian MF as; simple to implement, more convenient, response quickly, and fast computation [19]. Also, the datasets used in this paper were found not to be normally distributed where triangular MF usually works better with these types of data. The normality of the six datasets were tested using Kolmogorov-Smirnov test [20] and it is found that they are not following the normal distribution. The Kolmogorov-Smirnov test, which is also known as KS test returns a test decision for the null hypothesis that the data in vector x comes from a standard normal distribution, against the alternative that it does not come from such a distribution. In addition, it was found that the Triangular MF gives higher weights to the values near to

the mean value and gives less weights to the values far from the mean until it reaches zero weight at the farthest two values from the mean. This would result higher weights to more representative values and consequently better imputations for the missing values.

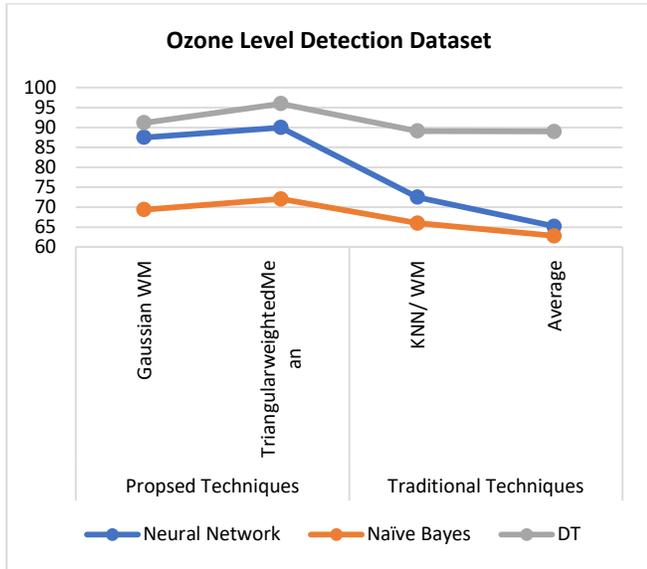


Fig. 2. Results for Ozone Detection Dataset.

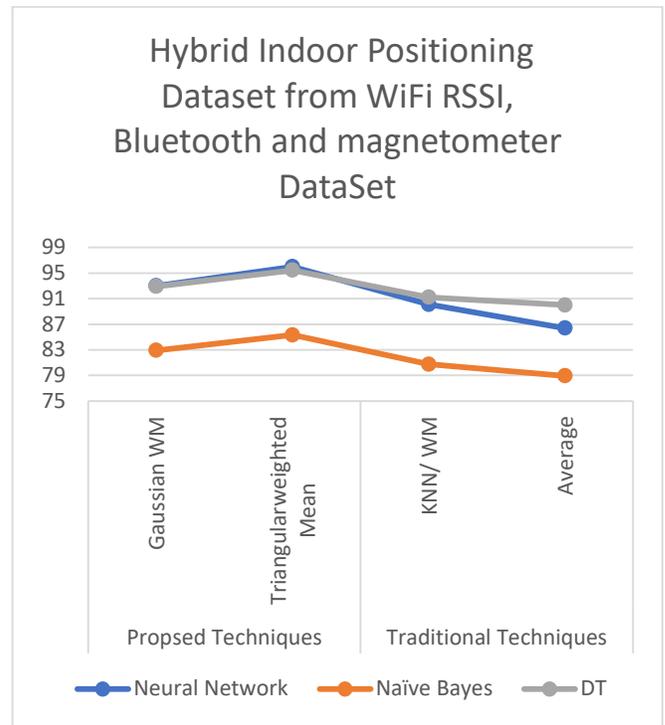


Fig. 4. Results for Hybrid Indoor Positioning Dataset from WiFi RSSI, Bluetooth and Magnetometer DataSet.

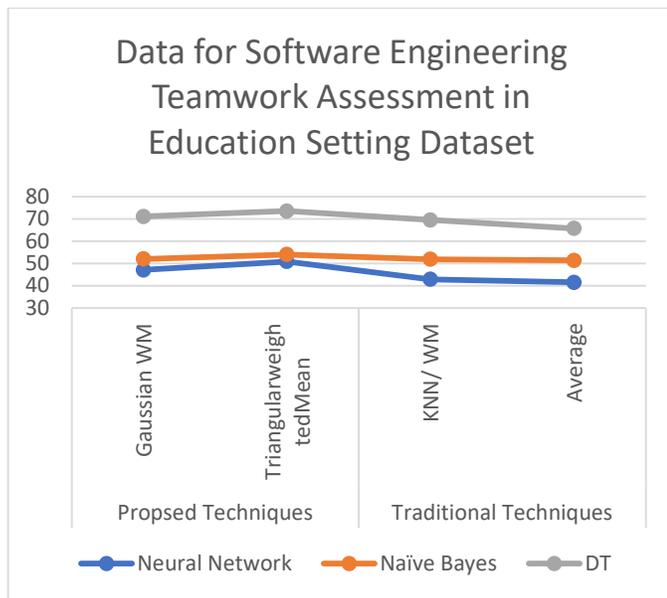


Fig. 3. Results for Data for Software Engineering Teamwork Assessment in Education Setting Dataset.

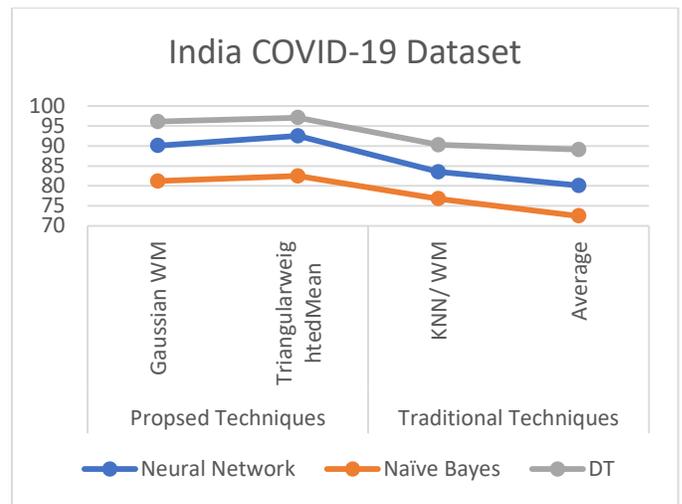


Fig. 5. Results for India COVID-19 Dataset.

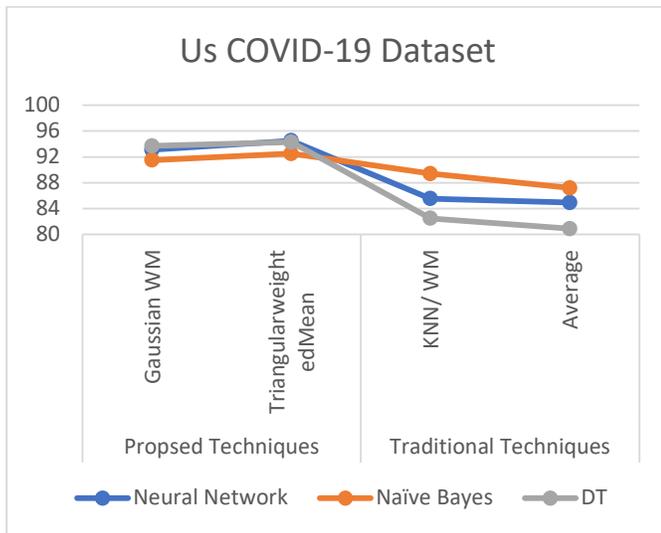


Fig. 6. Results for Us COVID-19 Dataset.

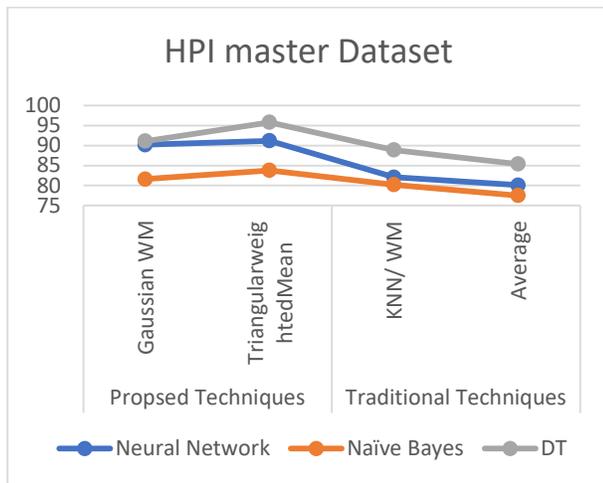


Fig. 7. Results for HPI Master Dataset.

## V. CONCLUSION

The paper introduced two proposed techniques based on the fuzzy logic while imputing missing values in time series data. The first proposed technique is the Gaussian weighted mean technique. This technique uses the KNN first to find the nearest neighbours then it gives to each neighbour a weight using the gaussian membership function, these weights is sent to the weighted mean function to calculate the imputed value. The second proposed technique is the Triangular weighted mean technique. This technique uses the KNN first to find the nearest neighbours then it gives to each neighbour a weight using the triangular membership function, these weights is sent to the weighted mean function to calculate the imputed value. The results of the two proposed techniques were compared with other two traditional techniques. The results output is that the two proposed techniques have higher accuracy than the traditional imputation techniques. Based on the experiments conducted in this paper it can be concluded that fuzzy membership functions can have better accuracy, and this is due to its behaviour in dealing with the data as it

gives a membership value for each point. Also, the results of the two proposed techniques were compared to find out that the triangular fuzzy membership function has higher accuracy than the gaussian membership function. Many different tests, and experiments have been left for the future due to lack of time. Future work concerns deeper analysis for the data, new proposals to try different methods. We also can start forecasting the new data in the future as we now have a complete data set.

## REFERENCES

- [1] Kumar, p.v., p. Scholar, and m.v. gopalachari, a review on prediction of missing data in multivariable time series.
- [2] Pratama, I., et al. A review of missing values handling methods on time-series data. in 2016 International Conference on Information Technology Systems and Innovation (ICITSI). 2016. IEEE.
- [3] Tong, G., F. Li, and A.S. Allen, Missing data. Principles and practice of clinical trials, 2020: p. 1-21.
- [4] Rantou, K., Missing Data in Time Series and Imputation Methods. University of the Aegean, Samos, 2017.
- [5] Williams, R., Missing data part 1: Overview, traditional methods. University of Notre Dame, 2015: p. 1-11.
- [6] Jayamanne, I.T., Cold Deck Imputation for Survey Non-response Through Record Linkage, in International Statistical Conference 2017 IASSL. 2017.
- [7] Rubin, D.B., Multiple imputation after 18+ years. Journal of the American statistical Association, 1996. 91(434): p. 473-489.
- [8] Kim, T., W. Ko, and J. Kim, Analysis and impact evaluation of missing data imputation in day-ahead PV generation forecasting. Applied Sciences, 2019. 9(1): p. 204.
- [9] Bashir, F. and H.-L. Wei, Handling missing data in multivariate time series using a vector autoregressive model-imputation (VAR-IM) algorithm. Neurocomputing, 2018. 276: p. 23-30.
- [10] Shahzad, W., Q. Rehman, and E. Ahmed, Missing data imputation using genetic algorithm for supervised learning. International Journal of Advanced Computer Science and Applications, 2017. 8(3): p. 438-445.
- [11] De Silva, H.M. and A.S. Perera, Evolutionary k-nearest neighbor imputation algorithm for gene expression data. ICTer, 2017. 10(1).
- [12] Flach, P. Performance evaluation in machine learning: The good, the bad, the ugly, and the way forward. in Proceedings of the AAAI Conference on Artificial Intelligence. 2019.
- [13] <https://archive.ics.uci.edu/ml/datasets.php>.
- [14] <https://www.kaggle.com/>.
- [15] Meng, Z., Ground Ozone Level Prediction Using Machine Learning. Journal of Software Engineering and Applications, 2019. 12(10): p. 423-431.
- [16] Petkovic, D., et al. Using the random forest classifier to assess and predict student learning of software engineering teamwork. in 2016 IEEE Frontiers in Education Conference (FIE). 2016. IEEE.
- [17] Kreinovich, Vladik, Olga Kosheleva, and Shahnaz N. Shahbazova. "Why triangular and trapezoid membership functions: A simple explanation." Recent Developments in Fuzzy Logic and Fuzzy Sets. Springer, Cham, 2020. 25-31.
- [18] Radhakrishna, Vangipuram, et al. "Design and analysis of a novel temporal dissimilarity measure using Gaussian membership function." 2017 international conference on engineering & MIS (ICEMIS). IEEE, 2017.
- [19] Sadollah, A., Introductory chapter: which membership function is appropriate in fuzzy system?, in Fuzzy logic based in optimization methods and control systems and its applications. 2018, IntechOpen.
- [20] Godina, R. and J.C. Matias. Improvement of the statistical process control through an enhanced test of normality. in 2018 7th International Conference on Industrial Technology and Management (ICITM). 2018. IEEE.

# Change Detection Method with Multi-temporal Satellite Images based on Wavelet Decomposition and Tiling

Kohei Arai

Saga University  
Faculty of Science and Engineering  
Saga City, Japan

**Abstract**—Change detection method with multi-temporal satellite images based on Wavelet decomposition with Daubechies wavelet function (Multi Resolution Analysis), and tiling is proposed. The method allows detection of changes in time series analysis and is not sensitive to geometric distortions included in the satellite images. In this paper, the author proposed a method based on MRA as a method for extracting change points from satellite images acquired over many periods. Change detection method with multi-temporal satellite images based on Wavelet decomposition and tiling is proposed. The method allows to detect changes and is not sensitive to geometric distortions included in the satellite images. The experimental results with simulation image and a Landsat Thematic Mapper (TM) image show that more appropriate changes can be detected with the proposed method in comparison with the existing method of subtraction. When applied to simulations and real satellite images, it was confirmed that they were robust to minute nonlinear geometric distortion.

**Keywords**—Daubechies wavelet; multi-resolution analysis; MRA; change detection; multi-temporal satellite image; geometric distortion; Landsat Thematic Mapper (TM) image

## I. INTRODUCTION

Change detection is important for time series analysis obviously. Trend analysis of the global warming issues is needed for identifying the locations and the timing for severely damaged areas and timing for instance. From the time series of satellite-based imagery data, it is possible to check the location and the timing of which warming phenomena is getting severe due to the estimated carbon dioxide and methane as well as nitric acid concentrations based on change detections.

As an example of applying wavelet analysis (development, transformation, etc.) to processing and analysis of earth observation satellite images, a method of superimposing multiple visible images after wavelet transformation [1], superimposing multiple Synthetic Aperture Radar: SAR images with different off-nadir angles After the wavelet transform [2], the method of applying the wavelet transform to the pattern of the annual fluctuation of the sea surface temperature estimated from the satellite data to extract its features [3], and the wavelet transform to the extraction of the surface roughness of sea ice [4], and [5] a method of extracting spatial features from images from which soil moisture has been extracted.

Extraction of water mass features from satellite images using polar coordinate representation Wavelet is discussed [6].

In this paper, the author examines a method of extracting change points of satellite images acquired over many periods using multi-resolution analysis (MRA). Extraction of change points from satellite image data acquired at each time as a method of performing the above, a method of taking a difference between images can be considered. However, the satellite image includes geometric distortion, and pixels resulting from the distortion are also extracted as change points in the difference image.

Among them, the linear distortion can be removed relatively easily, but the removal of the nonlinear distortion is not easy. Therefore, the author applied a multi-resolution analysis to the satellite image and devised a method of extracting a change point robust to nonlinear distortion by reducing the number of nodes, and confirmed the effect using a simulation image and a satellite image. The author reports here because good results were obtained.

In the following section, related research works and research background including motivation of the research are described. Then, the proposed context classification method is described followed by experimental method together with experimental results. After that, concluding remarks and some discussions are described.

## II. RELATED RESEARCH WORKS

Improved method of change detection method for remotely sensed images is proposed [7]. On the other hand, CO<sub>2</sub> concentration changes detection in time and space domains by means of wavelet analysis of MRA: Multi Resolution Analysis is proposed [8]. Method for support length determination of base function of Wavelet for edge and line detection as well as moving object and change detections is proposed [9].

Wavelet based change detection for four-dimensional assimilation data in space and time domains is also proposed [10]. Meanwhile, method for psychological status monitoring with line-of-sight vector changes (Human eyes movements) detected with wearing glass is proposed [11].

Method for real time text extraction of digital manga comic is proposed [12]. On the other hand, extraction of line features from multifidus muscle of Computer Tomography: CT scanned

images with morphological filter together with wavelet multi resolution analysis is proposed [13]. Method for extraction product information from TV commercial is also proposed [14].

Text extraction from TV commercial using blob extraction method is proposed [15]. Eye-based human-computer interaction allowing phoning, reading e-book/e-comic/e-learning, Internet browsing, and TV information extraction is also proposed [16]. Meanwhile, comparative study of feature extraction components for several wavelet transformations for ornamental plants is conducted [17].

Human gait gender classification using 3D discrete wavelet transformation feature extraction is proposed [18]. Comparison contour extraction based on layered structure and Fourier descriptor on image retrieval is conducted [19]. On the other hand, phytoplankton discrimination method with wavelet descriptor-based shape feature extraction from microscopic images is proposed [20].

### III. RESEARCH BACKGROUND

#### A. Wavelet Transformation

The Wavelet transformation of the function  $f(x)$  by the mother wavelet  $\psi(x)$  is given by the following equation.

$$(W_{\psi}f)(b, a) = \frac{1}{\sqrt{|a|}} \int_{-\infty}^{\infty} \psi\left(\frac{x-b}{a}\right) f(x) dx \quad (1)$$

Note that  $\psi(\bullet)$  is the complex conjugate of  $\psi(\bullet)$ . In this paper, Haar mother wavelet is used.

#### B. Haar Wavelet Function

Haar wavelet is one of the Wavelets. In 1909, Alfréd Haar announced it under the name of the Haar train. It is also one of the Daubechies wavelets. Haar Wavelets are the simplest wavelets. The disadvantage is that they are not continuous and therefore not differentiable.

The definition of the Wavelet transformation is as follows:

$$\psi(t) = \begin{cases} 1 & \text{for } 0 \leq t < 1/2, \\ -1 & \text{for } 1/2 \leq t < 1, \\ 0 & \text{for otherwise.} \end{cases} \quad (2)$$

The corresponding scaling functions are:

$$\phi(t) = \begin{cases} 1 & \text{for } 0 \leq t < 1, \\ 0 & \text{otherwise.} \end{cases} \quad (3)$$

Haar Wavelet function is shown in Fig. 1.

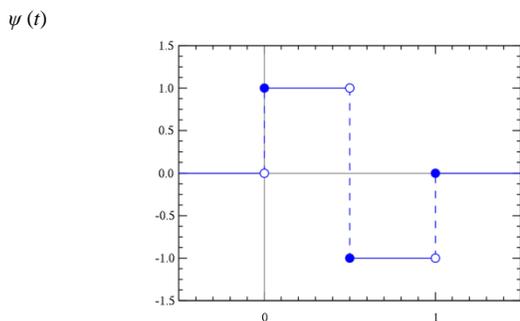


Fig. 1. Haar Wavelet Function.

#### C. Daubechies Wavelet Function

Fig. 2 shows Daubechies 4 tap Wavelet functions (red line indicates Wavelet function while blue line shows scaling function).

#### D. 2D(Two Dimensional) Discrete Wavelet Transformation

For 2D image signals, this process is performed horizontally and vertically one level at a time. Fig. 3 shows the band components when two-dimensional DWT is performed twice.

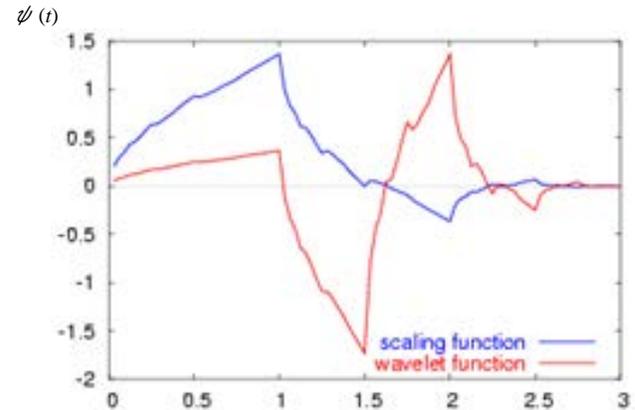


Fig. 2. Daubechies 4 tap Wavelet.

LLLL	LLHL	HL
LLLH	LLHH	
LH		HH

Fig. 3. Band Components after the 2D DWT.



(a) Original Image of "Lena" Included in SIDBA Database

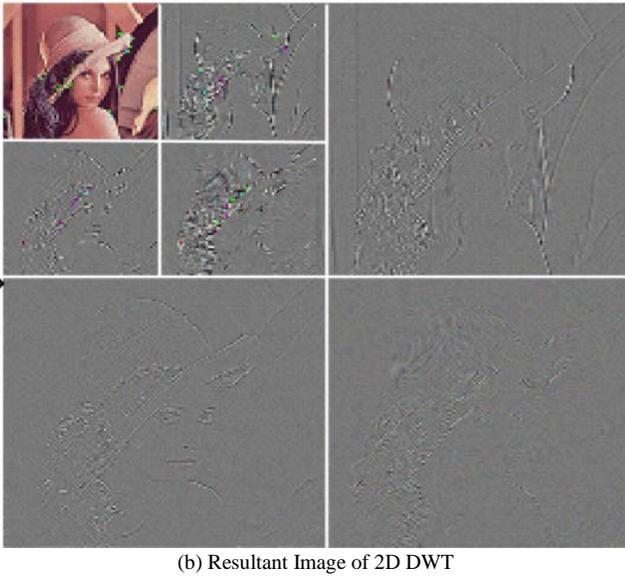


Fig. 4. Example of 2D DWT of the Image of "Lena" in the Image Database of SIDBA.

In the figure, L indicates a low frequency component, and H indicates a high frequency component. The image is decomposed into four bands (LL, LH, HL, HH) by the first two-dimensional DWT, and the lowest band component (LL) is further divided into four bands (LLLL, LLLH, LLHL, LLHH). Fig. 4 shows the results of two-dimensional DWT performed twice on an actual image.

#### E. Tiling

Tiling divides an image into several blocks (tiles), and then treats the tiles as one independent image. The size of the tile is arbitrarily selectable, and its minimum unit is  $1 \times 1$ .

### IV. PROPOSED METHOD

Change detection by Multi-Resolution Analysis: MRA is proposed. When MRA is applied to multi-temporal satellite images, it is divided into four components: LL, LH, HL, and HH. Since the image of the LL component does not reflect minute non-linear geometric distortion, it can be expected to be robust against such distortion.

The LL component represents a global feature of the image before the wavelet transform is performed, and the difference between the LL components of the images acquired at many times is considered to represent a change point. At this time, the setting of the number of levels of the MRA uses a difference between the number of points considered as the change points before conversion and the number of points considered as the change points after conversion.

### V. EXPERIMENT

#### A. Simulation Study

Simulation images were generated, and the validity of the proposed method was evaluated. With respect to the original image (the left figure in Fig. 5), a case of a changing image (the left figure of Fig. 6) and a case of a distorted image (the right figure of Fig. 6) were examined.

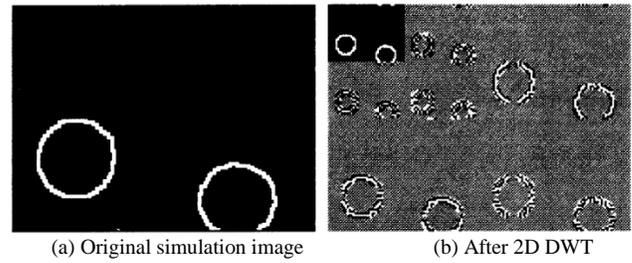


Fig. 5. Original Simulation Image and the Resultant Image after the 2D DWT.

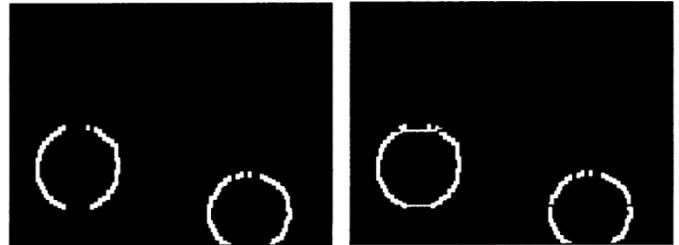


Fig. 6. Non-Distorted [Left] and Distorted [Right] Images.

The right diagram in Fig. 5 is an image obtained by performing the Daubechies wavelet transform on the left diagram in Fig. 5. The left diagram in Fig. 7 shows the difference between the left diagram in Fig. 5 and the left diagram in Fig. 6 by the wavelet transform. This is the result of direct extraction without performing. The right diagram of Fig. 7 is a result of directly extracting the difference between the right diagram of Fig. 5 and the right diagram of Fig. 6 without performing the wavelet transform. The right diagram in Fig. 8 is an image obtained by performing a Daubechies wavelet transform on the right diagram in Fig. 8. The left diagram in Fig. 9 is an image showing the difference between the right diagram in Fig. 5 and the left diagram in Fig. 6. The right diagram in Fig. 9 is an image showing the difference between the right diagram in Fig. 5 and the right diagram in Fig. 6. The white areas in Fig.7 and Fig. 9 represent the change points.

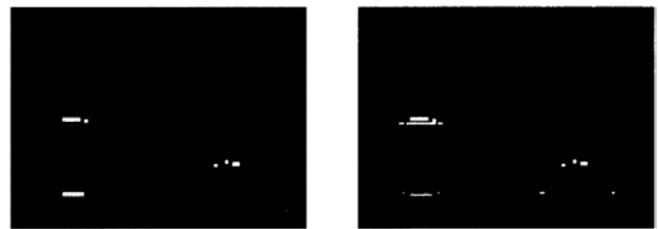


Fig. 7. Difference Images between the Original and the Changed [left] and the Distorted [Right] Images.

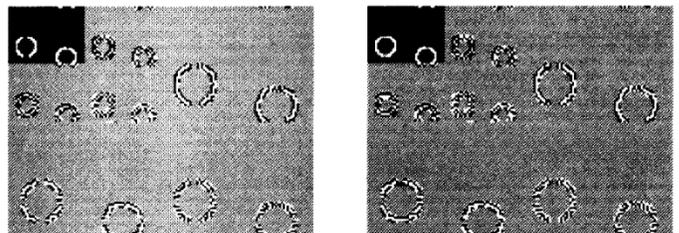


Fig. 8. The Resultant Images of MRA with 2D Daubechies Wavelet Transformation for the Changed [left] and the Distorted [Right] Images.



Fig. 9. Difference Images between the Original and the Changed [left] and the Distorted [right] Images after the MRA.

### B. Experiment with Actual Satellite Image

In addition, experiments using satellite images were also conducted. The data used this time is Landsat TM (Thematic Mapper) images acquired at many times in Tokyo Bay's waterfront subcenter. TM images are used for creating land cover maps. Fig. 10 and 11 show the acquired TM images. By performing the change extraction, it is possible to easily grasp the progress of the development of the seaside subcenter.

Fig. 12 shows the result of directly extracting the difference between Fig. 10 and Fig. 11 without performing the wavelet transform. Fig. 13 is an image obtained by performing the Daubechies wavelet transform on the image of Fig. 10 and Fig. 14 is an image obtained by performing the Daubechies wavelet transform on the image of Fig. 12. Fig. 15 is an image showing the difference between Fig. 13 and Fig. 14. The white areas in Fig. 12 and 15 represent the changing points.

When the difference is directly extracted without performing the wavelet transform, even a minute nonlinear geometric distortion is extracted as a change point. On the other hand, when the differences are extracted using the wavelet transform, it is understood that they are not extracted as the change points. Therefore, it can be said that the change point extraction method using the wavelet transform is robust to minute nonlinear geometric distortion as a method for extracting change points from satellite data acquired at many times.



Fig. 10. Landsat TM Image before Change.



Fig. 11. Landsat TM Image after Change.



Fig. 12. A Difference Image between before and after Change.

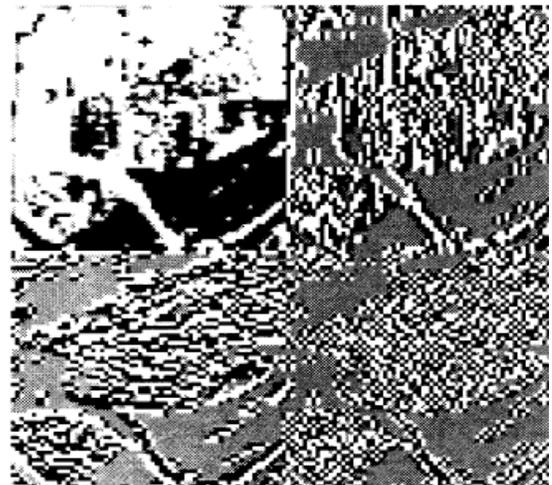


Fig. 13. The Resultant Image of MRA with 2D Daubechies Wavelet Transformation [Before Change Image].

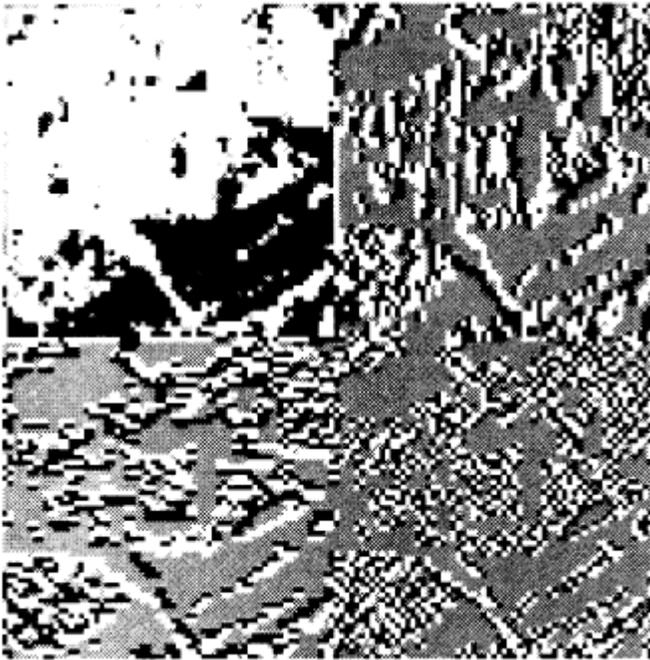


Fig. 14. The Resultant Image of MRA with 2D Daubechies Wavelet Transformation [After Change Image].



Fig. 15. A Difference Image between Before and After Change through MRA.

## VI. CONCLUSION

In this paper, the author proposed a method based on MRA as a method for extracting change points from satellite images acquired over many periods. Change detection method with multi-temporal satellite images based on Wavelet decomposition and tiling is proposed. The method allows detecting changes and is not sensitive to geometric distortions included in the satellite images. The experimental results with simulation image and a Landsat Thematic Mapper (TM) image

show that more appropriate changes can be detected with the proposed method in comparison with the existing method of subtraction.

When applied to simulations and real satellite images, it was confirmed that they were robust to minute nonlinear geometric distortion.

## VII. FUTURE RESEARCH WORKS

The proposed method is adopted in the real earth observation satellite imagery data, and it is a future subject to realize a more usable change detection method. In the future, the author will compare with conventional methods such as relaxation method. The author also considers the definition of Wavelet transform on polar coordinates and its application to water mass extraction.

## ACKNOWLEDGMENT

The author would like to thank Dr. Kaname Seto of former student of Saga University and Dr. Leland M. Jameson of Naval Research Laboratory for their contribution of this study. The author, also, would like to thank Professor Dr. Hiroshi Okumura and Professor Dr. Osamu Fukuda for their valuable discussions.

## REFERENCES

- [1] Jean-Pierre Djamdji, Albert Bijaoui, Roger Maniere: "Geometrical Registration of Images: The Multiresolution Approach," *Photogrammetric Engineering & Remote Sensing*, Vol.59, No. 5, pp.645-653, (1993).
- [2] Wooil M. Moon, J.S.Won, Vern Singhroy, and Paul D. Lowman Jr.: "ERS-1 and CCRS C-SAR data integration for lookdirection bias correction using wavelet transform," *Canadian Journal of Remote Sensing*, Vol.20, No.3, pp.280-285, (1994).
- [3] Nankin Mak: "Orthogonal Wavelet analysis: Interannual Variability in Sea Surface Temperature," *Bulletin of the American Meteorological Society*, Vol.76, No.11, pp.2179-2186, (1995).
- [4] Ronald W. Lindsay, Donald B. Percival, and D. Andrew Rothrock: "The Discrete Wavelet Transform and the Scale Analysis of the Surface Properties of Sea Ice," *IEEE Transactions on Geoscience and Remote Sensing*, Vol. 34, No.3, pp.771-787, (1996).
- [5] Zhenglin Hu, Yizong Chen, and Shafiqul Islam: "Multiscaling properties of soil moisture images and decomposition of large and small-scale features using wavelet transforms," *International Journal of Remote Sensing*, Vol.19, No.13, pp.2451-2467, (1998).
- [6] Kohei Arai, Kaname Seto, Leland M. Jameson: "Extraction of water mass features from satellite images using polar coordinate representation Wavelet", *Journal of Japan Society for Visualization Information*, Vol.19, Suppl.1, No.1, pp.99-102, Kogakuin University, (1999).
- [7] H. Okumura and Kohei Arai, Improvement of change detection method for remotely sensed images, *Proceedings of SPIE European Remote Sensing*, Invited Paper, ERS-10-RS07-61, 2010.
- [8] Kohei Arai, CO2 concentration change detection in time and space domains by means of wavelet analysis of MRA: Multi Resolution Analysis, *International Journal of Advanced Computer Science and Applications*, 2, 8, 82-86, 2011.
- [9] Kohei Arai, Method for support length determination of base function of wavelet for edge and line detection as well as moving object and change detections, *International Journal of Research and Reviews on Computer Science*, 2, 4, 1133-1139, 2011.
- [10] Kohei Arai, Wavelet based change detection for four dimensional assimilation data in space and time domains, *International Journal of Advanced Computer Science and Applications*, 3, 11, 71-75, 2012.
- [11] Kohei Arai, Kiyoshi Hasegawa, Method for psychological status monitoring with line of sight vector changes (Human eyes movements)

- detected with wearing glass, International Journal of Advanced Research in Artificial Intelligence, 2, 6, 65-70, 2013.
- [12] Kohei Arai, Tolle Herman, Method for real time text extraction of digital manga comic, International Journal of Image Processing, 4, 6, 669-676, 2011
- [13] Kohei Arai, Yuichiro Eguchi and Yoichiro Kitajima, Extraction of line features from multifidus muscle of CT scanned images with morphological filter together with wavelet multi resolution analysis, International Journal of Advanced Computer Science and Applications, 2, 8, 60-66, 2011.
- [14] Kohei Arai and Tolle Herman, Method for extraction product information from TV commercial, International Journal of Advanced Computer Science and Applications, 2, 8, 125-131, 2011.
- [15] Kohei Arai and Tolle Herman, Text extraction from TV commercial using blob extraction method. International Journal of Research and Review of Computer Science, 2, 3, 895-899, 2011.
- [16] Kohei Arai, Ronny Mardiyanto, Eye-based human-computer interaction allowing phoning, reading e-book/e-comic/e-learning, Internet browsing and TV information extraction, International Journal of Advanced Computer Science and Applications, 2, 12, 26-32, 2011.
- [17] Kohei Arai, Indra Nugraha Abdullar, H.Okumura, Comparative study of feature extraction components for several wavelet transformations for ornamental plants, International Journal of Advanced Research in Artificial Intelligence, 3, 2, 5-11, 2014.
- [18] Kohei Arai, Rosa Andrie Asmara, Human gait gender classification using 3D discrete wavelet transformation feature extraction, International Journal of Advanced Research in Artificial Intelligence, 3, 2, 12-17, 2014.
- [19] Cahya Rahmad, Kohei Arai, Comparison contour extraction based on layered structure and Fourier descriptor on image retrieval, International Journal of Advanced Computer Science and Applications, 6, 12, 71-74, 2015.
- [20] Kohei Arai, Phytoplankton discrimination method with wavelet descriptor based shape feature extraction from microscopic images, Journal of RIMS Signal and time frequency analysis, Kokyuroku edited by Ryuichi Ashino, Kyoto University, 50-86, 2010.

#### AUTHOR'S PROFILE

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

# Comprehensive Analysis of Resource Allocation and Service Placement in Fog and Cloud Computing

A.S. Gowri<sup>1</sup>, P.Shanthi Bala<sup>2</sup>, Immanuel Zion Ramdinthara<sup>3</sup>  
Department of Computer Science, School of Engineering and Technology  
Pondicherry University, India

**Abstract**—The voluminous data produced and consumed by digitalization, need resources that offer compute, storage, and communication facility. To withstand such demands, Cloud and Fog computing architectures are the viable solutions, due to their utility kind and accessibility nature. The success of any computing architecture depends on how efficiently its resources are allocated to the service requests. Among the existing survey articles on Cloud and Fog, issues like scalability and time-critical requirements of the Internet of Things (IoT) are rarely focused on. The proliferation of IoT leads to energy crises too. The proposed survey is aimed to build a Resource Allocation and Service Placement (RASP) strategy that addresses these issues. The survey recommends techniques like Reinforcement Learning (RL) and Energy Efficient Computing (EEC) in Fog and Cloud to escalate the efficacy of RASP. While RL meets the time-critical requirements of IoT with high scalability, EEC empowers RASP by saving cost and energy. As most of the early works are carried out using reactive policy, it paves the way to build RASP solutions using alternate policies. The findings of the survey help the researchers, to focus their attention on the research gaps and devise a robust RASP strategy in Fog and Cloud environment.

**Keywords**—Cloud; fog; reinforcement learning; energy-efficient computing; resource allocation; service placement

## I. INTRODUCTION

Digitalization has revolutionized anything as a service (XaaS) on pay per usage basis [1]. With the increase in smart handheld devices, online business, transportation, health care, education, and food court which were once a commodity, are delivered as a service at the doorstep of the individual. These digital services produce and consume a variety of voluminous data, at a rapid speed that needs to be stored for big data analytics [2]. Consequently, enterprises depend on cloud Data Centers (DC) to store, process, and manage their data [3], [4].

A large number of commercial Cloud Service Providers (CSP) deliver compute, storage, and communication resources in the form of Infrastructure as a Service (IaaS) [5]. Estimating the required amount of IaaS resources and assigning the service (tasks) for execution is termed as Resource Allocation and Service Placement (RASP) [6][7]. Service is defined as the actual software instance that executes a task. The terms service and tasks are often used interchangeably [8].

A RASP framework abides by the Service Level Agreement (SLA) made between consumer and service provider [9][10]. SLA is the mutual agreement cum negotiation made between the service consumer and the CSP. Providing guaranteed resources to the consumers/applications on time

aggravates many challenges. Inaccurate estimation of available resources, wrong forecast of workload, incorrect prediction of required resources, deadline violation, uncontrolled energy consumption, unexpected failures of hardware/software, SLA Violation (SLAV) are some of the other problems encountered by a RASP framework. Hence, a robust RASP that benefits the consumer and the service provider in terms of their requirements and revenue is needed.

Resources are allocated to the requesting services by either of the three policies viz., Reactive, Predictive, or Hybrid. In reactive policy, the initial allocation of resources is subject to change, only after the system enters an undesirable state. The reactive policy follows a predefined set of rules for scaling the resources. On the other hand, the predictive (also known as a proactive) policy, anticipates the forthcoming disruptions in advance, and updates the resources, well before the system enters the undesirable state [11]. It forecasts the workload and scales the resources in advance to meet future needs. The hybrid approach is an amalgamation of both the reactive and proactive policy [5].

Each policy bears its own cost in satisfying the SLA. The choice of policy purely depends upon the application and the RASP strategy adopted. Out of the works considered from the period 2011 to 2020, Table I shows that most of the works were carried out in the reactive policy, which opens the research gap in other policies to model RASP.

### A. Significance of RASP in Cloud Computing

Cloud computing is an Information Technology service model that provides on-demand computing resources over the Internet independent of device and location [12]. The need for online services has made the enterprises move their data and applications to the DC, from where they are provisioned as services to the end-user. With the proliferation of IoT, communications, among smart devices are made possible through the cloud-assisted IoT, called a Cloud of Things (CoT) [13]. Consequently, RA in the cloud has become inevitable to serve IoT requests.

### B. Significance of RASP in Fog Computing

Despite its huge processing capacity, the cloud suffers latency problems when it comes to delay-sensitive IoT applications. By the time the data are sent to the cloud for processing, the necessity to act on it might be gone, which costs lives. Hence, a computing model like Fog, which delivers services of the Cloud near the edge network is a better choice for time-sensitive applications.

TABLE I. POLICY DISTRIBUTION OF RASP WORKS

	Reactive	Proactive	Hybrid	Total
Cloud Computing	7	5		12
Reinforcement Learning	2	5	1	8
Energy-Efficient Computing	6	4	-	10
Fog Computing	17	1	-	18
Total	32	15	1	48
Percentage	67%	31%	2%	

Fog Computing (FC) is a computing paradigm where a huge number of ubiquitous, decentralized, heterogeneous, geo-distributed devices provide computation, storage, and communication facility at the edge of the local network from where the devices/objects generate and consume data [13]. It accelerates awareness cum response to events by eliminating RTT (Round Trip Time) to the cloud and avoids failures during peak period. As such, not all requests are serviced in Fog. Some of the delay-tolerant applications that involve huge computation are processed in the cloud [14] [15]. In fact, Fog complements Cloud to realize its potential with IoT applications.

### C. Relevance of Reinforcement Learning (RL) in RASP

The design and implementation of RASP for the growing scale of IoT, require intelligence that is far beyond the capacity of the case-driven programming style [16]. Such programs depend on predefined rules which is hard to change instantaneously for the stochastic needs of IoT [17]. A robust RASP requires an approach like Reinforcement Learning which learns the environment (requirement and availability of resources) and maps the appropriate action on the fly.

RL is an Artificial Intelligence-based technique that automatically learns to make decisions under a dynamic environment without prior domain knowledge[18]. When service providers suffer to handle the complexity of stochastic requests in real-time, RL-assisted RASP, delivers better service in both Cloud and Fog.

### D. Energy-Efficient Computing (EEC) in RASP for Green Environment

The rapid growth of DC has become the highest consumer of power that leads to the dissipation of Green House Gas (GHG) [5]. Compute and non-compute resources incur abundant energy waste [17],[19]. Measures taken to control the speed of processors, frequency/voltage, and switch-off/sleep modes, are not sufficient to reduce the effect of GHG emission [20]. Hence, an EEC-based RASP that enables sustainability of the Green Environment with minimal operational expenses is required.

An illustration of the coordinating computing models is shown in Fig. 1. It portrays the association of the Edge-Fog-Cloud computing paradigm in association with the application requests. The Fog Controller embeds the Reinforcement Learning and Energy-Efficient Computing components to achieve an efficient RASP system.

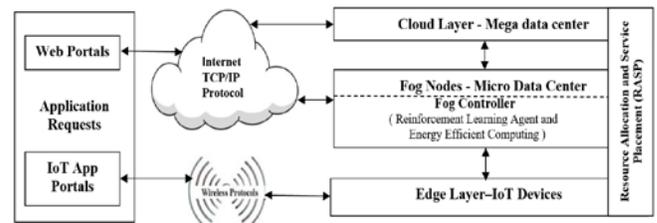


Fig. 1. Fog-Cloud Framework.

The rest of the paper is organized as follows. Section 2 reviews the existing literature works in RASP. Section 3 analyzes the RASP works in cloud datacenters. Section 4 discusses the approaches made in RASP using RL techniques while Section 5 presents EEC-based RASP. Section 6 discusses the efficacy of FC in addressing IoT applications and elaborates on the existing Fog based RASP works. Then the proposed survey concludes with a discussion on identified research gaps that could be useful to the research and development community in the future.

## II. OVERVIEW OF EXISTING SURVEYS

This section analyzes the existing survey papers of RA, in Cloud Computing, RL, EEC, IoT, and Fog Computing. Resource provisioning and application management often exclude issues like unpredictable workload, poor utilization of resources, and unexpected Hardware (HW)-Software (SW) failures. The brownout paradigm that addresses such issues by enabling/disabling the optional parts of the application was presented in [21].

In [22] the author reviewed energy efficiency in four dimensions: (i) Virtual Machine (VM) placement, (ii) VM migration, (iii) Server consolidation, and (iv) Dynamic Voltage Frequency Scaling (DVFS). In [23] the author explored energy management techniques at the HW level, Resource Management (RM) level, and application level. While Static Power Management (SPM) technique was used at the HW level, Dynamic Power Management (DPM) was tackled at the RM level. Green Computing with renewable energy was recommended at the application level.

Maximization of resource utilization and minimizing the cost were the main goal of Resource Allocation (RA) in the IoT environment [24]. Scarce processing-storage capacity, low battery level, less bandwidth, and, poor implementation of resource management protocol were shortlisted as limitations of IoT. Lightweight container-based virtualization was suggested to process and store IoT applications. Though Cloud supports IoT, Fog computing resolves the time-sensitive-issues of IoT more diligently.

Application placement, resource scheduling, task offloading, and load balancing, were explored in [25]. distinguished Fog, from Multi-Access Edge Computing (MEC) and cloud, in terms of operation mode and application addressed [4]. In [15], the author identified the challenges faced by Fog computing to process context-aware applications of IoT. In [3], RA and task scheduling were considered as one of the key challenges in IoT. The survey suggested CloudSim, MATLAB, and iFogSim to implement RA in Cloud and Fog.

The author recommended container-enabled micro-services to resolve the resource limitation problem.

### III. ANALYSIS OF RASP IN CLOUD COMPUTING

Cloud is a ubiquitous technology that offers infrastructure, software, and platform as service on-demand with the least interaction and management effort of the service provider [26],[27]. Despite its control over the IaaS management, CSP lacks knowledge about the application hosted in their machines. VMs of different applications overlap on physical servers leading to catastrophic failure which is not recognized by the CSP instantly.

Deployment of multi-tier applications is yet another complexity, as the configuration of VMs in one tier differs from the other causing interoperability problems [28] [29]. This section analyzes the existing RASP works in Cloud. While certain works adapt their own architecture, others follow the specific algorithm for the existing RASP. Table II shows the distribution of existing RASP articles under various criteria.

#### A. Uncertainty in Resource Availability

Unexpected HW failures, SW faults like overflow conditions, malware, DoS (Denial of Service) attacks, and changes in the number of objectives during execution are some of the uncertain behavior projected in [30]. Power consumption cost and overestimation of resources hinder the profit of the CSP due to which certain objectives like deadline and make-span are ignored/altered while deliberating RASP. As HW/SW failure is unavoidable, the Neural Network based Dynamic Non-dominated Sorting Genetic Algorithm (NN-DNSGA-II) converges before the occurrence of the next failure. Change in the number of objectives at runtime is tackled by a generalized periodic change in the objective size.

#### B. Impact of SLA/QoS in RASP

The applications that are hosted in DCs expect the utmost performance in terms of low latency and high throughput within budget and specified deadline. These performance measures form the QoS requirements. The mutual negotiation between the consumer and the CSP for a guaranteed QoS results in SLA. With the growing number of IaaS providers, not only does it require expertise but is time-consuming for the clients to select an efficient CSP.

TABLE II. CLASSIFICATION OF EXISTING RASP PAPERS IN CLOUD COMPUTING

Paper ID	Reference	Author	Architecture based	Algorithm-based	RA Policy			Problem Addressed				
					Reactive	Proactive	Hybrid	Uncertainty	SLA/QoS	Slashdot	Elasticity	ASP viewpoint
C1	[30]	Ismayilov & Topcuoglu, 2020		✓		✓		✓				
C2	[9]	Soltani et al., 2018	✓		✓				✓			
C3	[10]	Singh & Viniotis, 2017		✓		✓			✓			
C4	[12]	Djebbar & Belalem, 2016		✓	✓				✓			
C5	[32]	Ashraf, 2016		✓		✓				✓		
C6	[29]	RahimiZadeh et al., 2015	✓		✓					✓		
C7	[28]	Kaur & Chana, 2014	✓			✓					✓	
C8	[33]	Agarwal & Jain, 2014		✓	✓					✓		
C9	[34]	Espadas et al., 2013	✓		✓							✓
C10	[35]	Casalichio & Silvestri, 2013	✓		✓							✓
C11	[36]	Xu & Li, 2013	✓		✓							✓
C12	[31]	Islam et al., 2012	✓			✓						✓

The RA framework in [9] follows the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) in which the available IaaS resources are ranked by their similarity index concerning the application requirements. Then, the top IaaS resource was allocated to the corresponding application.

Lack of CSP's knowledge about the message arrival rate and length of the Enforcement Period (EP) were the problems encountered in satisfying SLA. To overcome the loss caused by SLAV, a RA mechanism that allows an additional EP to execute the unpredictable IoT traffic is recommended by [10]. Execution speed and deadline were considered as primary QoS constraints in [12].

### C. Slashdot Prediction in RASP

Slashdot refers to the unpredictable flash crowd workload on the Internet at any instant of time [31]. A sudden traffic surge makes the RASP framework unstable. The Slashdot effect if not addressed properly, leads to a cascade of problems like unacceptable delay, long downtime, application unavailability, revenue reduction, and losing the customer in the worst case.

Conventional predictive policies turn failure as they forecast the expected workload traffic, only a few steps ahead during which the Slashdot effect remains invisible. The Long Short Term Memory Recurrent Neural Network (LSTM-RNN) technique that predicts the workload traffic/pattern a thousand steps ahead was implemented in [32]. Based on the prediction provided by LSTM-RNN, resource scaling was performed without compromising SLA.

The performance of Virtualized Multi-Tier Application (VMTA) for the unstable workload was analyzed using the queuing network in [29]. Apache, Tomcat, and MySQL servers were used for the front end, application, and database tiers, respectively [33]. A Generalized Priority Algorithm (GPA) for scheduling tasks in the cloud, consumed the least execution time when compared to the First Come First Serve method.

### D. Need for Elasticity in RASP

Resource elasticity refers to the automatic acquisition and release of resources at runtime to fulfill the QoS requirements in response to the changing workload. Though the workload traffic is predicted in advance, RA without an elasticity component is a failure, as neither the resources are efficiently scaled nor is the QoS met [34]. The QoS aware resource elasticity framework for multi-tier application was modeled in [28]. The framework employed MT-PerfMod (Multitier Performance Module) to compute the overall response time and resource utilization, based on which, the MT-ResElas (Multi-Tier Resource Elasticity) module computed the SLAV rate. Whenever the response time and the resource utilization rate were violated, VMs were increased; otherwise, the number of VMs was reduced by half.

### E. RASP on ASP (Application Service Provider) Point of View

The majority of RA is performed from the CSP point of view, which reduces the preference for ASP. The ASP is charged for the resources that were wasted due to underutilization. Hence, an ASP (tenant) centric RA for scaling the application was modeled in [31][34]. The knapsack problem approach was implemented to predict the minimum number of VMs required.

Though the maximum number of VMs required was estimated in advance, it keeps changing depending upon the number of active users who access the application. The problem arises when the ASP (consumer) is charged for the idle resources. An SLA-based RP mechanism in the ASP point of view was presented in [35]. A framework where clients and operators suggest their preference for RA policies was presented in [36]. The technique described the allocation of jobs to a machine, based on the stable matching algorithm. Tables IIIA and IIIB tabulate the observations of the RASP works in Cloud Computing.

TABLE III. A. ANALYSIS OF RASP WORKS IN CLOUD COMPUTING

Paper ID	Ref.	Problem addressed	Objective	Algorithm/Approach	Performance metrics addressed
C1	[30]	Unexpected Hardware-Software failure and change in the number of objectives at runtime	Formulate a scheduling strategy to minimize cost, energy and maximize resource utility for periodical workflow	Neural network-based dynamic non-dominating sorting genetic algorithm (NN-DNSGA-II)	Cost, energy, and resource utility through Non-dominated solutions (NS), Schott's spacing (SS), and Hyper Volume (HV)
C2	[9]	Time and cost difficulties in cloud service selection	To build an automatic cloud service selection framework that overcomes time and cost problem	Architecture based- Hybridization of case-based reasoning with Multi-criteria decision making (MCDM) and TOPSIS (Technique for order of preferences by Similarity to Ideal Solutions)	Recommended CSP, CSP's service type, memory storage, region, Price/Hr., OS
C3	[10]	Enforcement of IoT SLA in the cloud environment	Conformance of SLA within enforcement period	Server over-provisioning approach, policing, Weighted Round Robin (WRR) scheduling algorithm, rate-limiting mechanism to enforce SLA	Number of messages arrived/processed, SLA confirmation rate, number of servers, additional enforcement period used
C4	[12]	High data management in scientific application	Minimize response time	Space and Time-shared policy based on deadline, length of the task, the execution speed of VM, and VM tree method.	Total response time
C5	[32]	Inaccuracy in the prediction of workload violates SLA and increases the cost	Prediction of resource demand and auto-scale them instantaneously that minimizes cost irrespective of application traffic	Long short-term memory RNN with peephole connections with Mean Absolute Deviation (MAD) to set threshold	Response time, No. of VMs, No. of completed request with the deadline.
C6	[29]	Stochastic burst and non-burst workload	Propose an analytical model-based queuing network to estimate aggregated QoS metrics	Analytical model-based queuing network (M/G/1)	Response time, disk utilization, CPU utilization.
C7	[28]	The contradiction between QoS and elasticity of resources	Mapping of the QoS attribute with minimum SLA violations thus maximizing the overall profit	Architecture-based - QoS aware resource Elasticity framework for the multi-tier web application. Control Theoretic based scaling algorithm	Response time < 5 secs, Resource utilization > 80%
C8	[33]	Task scheduling	Minimize execution time	Generalized Priority algorithm (GPA) based on highest length cloudlet to highest MIPS VMs	Execution time
C9	[34]	To solve under-utilization and over utilization of resources in cloud applications	tenant-based isolation, tenant-based load balancing, tenant-based VM allocation	Architecture based	CPU Utilization, memory utilization, Throughput
C10	[35]	SLA based resource provisioning in cloud	Achieve SLA oriented resource provision irrespective of workload type	Queuing model M/G/1 and M/M/m with autonomic QoS aware resource provisioning	CPU utilization, response time, number of VMs required
C11	[36]	Tasks to occupy a minimum number of VMs to achieve server consolidation	Develop a unified framework for resource management in the cloud, where policies are decoupled.	Conventional Job-Machine stable matching problem	Execution time, no of VMs
C12	[31]	Resource Prediction and Provisioning	Build an adaptive RM for applications hosted in the cloud.	Neural Network and Linear Regression to satisfy upcoming demands	CPU Utilization for each technique

B. ANALYSIS OF RASP WORKS IN CLOUD COMPUTING

Paper ID	Ref.	Experiment	Evaluation	Workload	Limitations
C1	[30]	Real-time experiment with Amazon EC2	Evaluated with DNSGA-RI, DMOPSO, DNSGA-II-HM, DNSGA II-A, and DNSGA-II-B	100 to 1000 tasks from Pegasus workflow management that covers astronomy, physics, biology, geology, and bio-informatics dataset.	The work is compared with non-predictive algorithms.
C2	[9]	Test bed	Validated with a sample application that is to be deployed on one of the US regions	Service template of a sample application	Criteria for CSP selection, resource provision, task scheduling are problem-specific
C3	[10]	Discrete event simulator in C	Evaluated for a different rate of traffic request, change in capacity, enforcement period	Two million messages per tenant per month	Homogenous message size limited to 512 bytes
C4	[12]	CloudSim	Compared with time/space shared policy.	Simulated with 10-50 cloudlets (tasks)	The reactive policy cannot scale and tolerate dynamism
C5	[32]	CloudSim using deeplearnig4j open source	Compared with automatic scaling and conventional threshold-based scaling techniques.	NASA Clark net workload	Explanation required for computations of response time, number of the completed request.
C6	[29]	Test bed constructed with 2 servers, 6-VM/server	Evaluate the performance of VMTA (virtualized multi-tier applications) through cache hit ratio, request arrival rate.	Rubis and Wikipedia tiers under burst & non-burst workloads.	The trade-off between assignments of cores to domains, cache contention can be investigated.
C7	[28]	Amazon cloud watch (EC2 monitoring tool)	JMeter load tests-to measure response time & utilization, Amazon cloud watch - % of utilization	3-tier web applications	QRE (QoS aware Resource Elasticity) framework is considered a homogenous type of VMs only. Resource availability, fault tolerance can be measured.
C8	[33]	Cloud Sim	Compared with first come first serve, round-robin	web service generated workload traces	Cannot handle instantaneous demand of resources, leads to over-provisioning or under-provisioning.
C9	[34]	Test bed: eucalyptus cloud, Tomcat-based SaaS platform deployed over it.	t-test statistical analysis	Apache JMeter to create web service workloads to the Tomcat cluster	HPC and Online transactions, bandwidth, storage, and transfer data, need to experiment
C10	[35]	Amazon cloud watch (EC2 monitoring tool) with Mat lab graph generation	Partial ASP and limited ASP (Application service provider)	Wikibench- to generate workload from Wikipedia, Mediawiki for backend database	The reactive approach cannot address stochastic heterogeneous workload type
C11	[36]	1) Test bed-prototype implementation with a cluster of 20 dual-core machines and 2) Trace-driven simulation.	Correctness convergence, job-optimality of multistage deferred acceptance are proved through theorems & lemma	RICC (RIKEN Integrated Cluster of Clusters), explored for 200 tasks with 1000 VMs	VM migration can be included
C12	[31]	Amazon EC2 instances	Evaluated with MAPE (Mean absolute Percentage), PRED (25) (Prediction accuracy within 25%), RMSE (Root Mean Square Error)	TPC-W - interactive E-commerce application	Integration of prediction strategies with auto-scaling can enhance the effectiveness of the adaptive resource allocation in terms of performance and cost.

#### IV. ANALYSIS OF REINFORCEMENT LEARNING ASSISTED RASP

The human-to-machine and machine-to-machine interaction-based IoT applications demand a technique that makes the optimal decision at high speed. The traditional rule-based programming approach does not withstand the stochastic requirements of IoT. Hence, a machine learning programming approach that observes and adapts to the environment is required. Such requirement leads to the choice of Reinforcement Learning (RL) which automatically learns to take decisions by trial and error method under a dynamic environment with prior domain knowledge. Fig. 2 depicts the basic structure of RL.

In RL based RASP, service request and the resource pool forms the environment. The values like the expected number of service requests and the amount of available resource observed at any instant of time form the state. At every time-step of interaction, the state values form the input to the agent from the environment. Action is the decision taken to place the service request in the appropriate resource. The agent chooses its action in such a way that the system achieves maximum

resource utilization with minimum cost. For every action taken, the agent receives a suitable positive or negative reward as an incentive. By trial and error, the agent tries to maximize its reward by taking optimal decisions (actions) in the long run.

The agent is trained to take optimal action through either of the RL algorithms like Q-learning, SARSA, E-SARSA, or Deep RL. The choice of the RL algorithm depends on the type of problem encountered and the feasibility of implementation. This section analyzes the RL-assisted RASP works for the categories given in Table I.

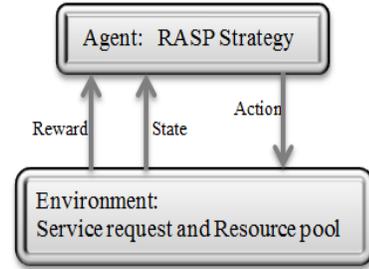


Fig. 2. RL Assisted RASP.

TABLE IV. CLASSIFICATION OF RL ASSISTED RASP WORKS

Paper ID	Reference	Author	Architecture based	Algorithm-based	RA Policy			Problem Addressed			
					Reactive	Proactive	Hybrid	Fog-RAN	Job rejection & client retention	QoE	Auto Reconfiguration
R1	[37]	Nassar & Yilmaz, 2019		✓	✓			✓			
R2	[40]	Gai & Qiu, 2018	✓			✓				✓	
R3	[6]	Cheng et al., 2018	✓			✓			✓		
R4	[38]	Bahrpeyma et al., 2015	✓			✓			✓		
R5	[41]	Xiangping Bu et al., 2013	✓			✓					✓
R6	[42]	Xu et al., 2012	✓				✓				✓
R7	[43]	Dutreilh et al., 2011		✓	✓						✓
R8	[26]	Rao et al., 2011		✓		✓					✓

TABLE V. ANALYSIS OF REINFORCEMENT LEARNING ASSISTED RASP WORKS

Paper ID	Ref.	Problem addressed	Objective	Algorithm/Approach	Performance metrics addressed	Experiment	Evaluation	Workload	Limitations
R1	[37]	Intolerable delay due to sequential allocation of Fog resources for IoT	To achieve ultra-reliable low latency communication using Fog-RAN	RL methods - QL, SARSA, E-SARSA, MC	Resource utility and idle time	Test bed	RL based methods compared with a fixed threshold algorithm	19 scenarios of IoT applications	Sequential request arrival pattern alone considered. Effective only for static IoT environment.
R2	[40]	The contradiction between performance and time in providing QoE for IoT requests	To derive an optimal resource allocation strategy to achieve QoE	RL based mapping table algorithm and dynamic programming based RL enabled RA algorithm	QoE in terms of latency and energy	Java programming based simulated experiment	Performance time compared for varying number of tasks and compute nodes	Four data blocks	The number of IoT tasks assumed to be less than available compute nodes.
R3	[6]	Frequent change of QoS request pattern by clients	To allocate resources with minimum run-time, energy cost, and job rejection rate	Semi Markov Decision Process (SMDP) and Deep RL to solve the problem	Energy cost, run-time, job rejection rate.	Simulation experiments	With Greedy, Round Robin & FERPTS (Fast energy-aware resource provision & task scheduling)	200,000 user requests in 5000 servers in 10-100 clusters with the real workload from Google traces for 29 days.	Evaluated for batch application requests only. Real-time applications need to be considered.
R4	[38]	Client retention problem	Derive optimal policy that prevents job rejection and minimize energy consumption	Q-learning to deal with the uncertainty of problems, Neural NW- to predict future demand of a resource, Genetic Algorithm for the action selection mechanism	Job rejection rate (0%), wastage in resource usage (9.55%)	MATLAB tool box with 23 neurons in the hidden layer and Gaussian kernel function.	NN prediction for VM demand evaluated through normalized MSE (mean square error)	90 days' workload trace.	Cost overhead on different techniques. Response time and energy are not explained well.
R5	[41]	To overcome performance degradation of IoT applications	enable coordinated configuration of VMs and their hosted application dynamically	Hybridization of simplex and reinforcement learning	Throughput, response time	Test bed with 16 physical servers each with 100 VMs	Validated with 720 iterations, compared with Nelder Mead, Hill climbing strategy, ARMA controller strategy	Xen based virtualized environment with TPC-W & TPC-C benchmarks consisting of about 5000 clients	The model-free approach takes time to optimize configuration. Suitable only for applications that could be stable for a long time.
R6	[42]	Real-time auto reconfiguration of VM and the applications that run on it	To achieve SLA optimization on VM and application-specific parameter	RL algorithm with multilayer feed-forward back propagation neural network and polynomial regression to predict application parameter for reconfiguration	Response Time, Throughput, and resource utilization	Test bed with Xen virtualization platform	Tested homogenous & heterogeneous applications indifferent physical server	TPC-C, TPC-W, SPEC web workloads	RL suffers from scalability in model-based approach when there are insufficient prior cases
R7	[43]	Dynamic adaptation of resources	To achieve, 1). Effective allocation policy from the start of RL 2) prompt convergence to the optimal policy	Reinforcement learning-based autonomous resource allocation	Decision on convergence speed up measured	Test bed in Amazon EC2	With and without convergence speed-up applied for every 5000 observations	Ohio - a standard test bed for web services	To be tested for large scale application
R8	[26]	Resource provisioning	Minimize response time and number of VMs utilized	Architecture based iBalloon framework with the RL algorithm	Throughput, response time, number of VMs	Tested on 2 clusters with 16 & 22 machines each with 8 to 12 cores	Compared with ARMA, Optimal strategy, Adaptive PI (Proportional Integral)	SPEC-Web (e-commerce), TPC-W (CPU intensive)	A discrete set of actions alone is considered. RL capacity management suffers poor initial

### A. RL based RASP for F-RAN (Fog-Radio Access Network)

Fifth-generation wireless communication is an emerging solution to the expectations of ultra-low latency, minimized energy consumption, and high throughput [37]. Cloud-based Radio Access Network (C-RAN) used base stations, remote radio heads as resources to process IoT applications. But, the unlimited IoT traffic imposes a heavy burden, turning the C-RAN less efficient for IoT applications. Employing RL assisted Fog nodes in the front-haul alleviated the cloud's burden, and elevated Fog-RAN (F-RAN) as a promising solution to tackle time-critical applications of IoT [39]. RL-enabled RASP in F-RAN has the advantage of local processing and distributed storage capability at the vicinity of the end-user resulting in high resource utilization [37].

### B. Job Rejection Rate and Customer Retention in RL based RASP

Enterprises look for CSPs to host their applications for online business. A CSP is chosen based on the service quality they provide. But, in the CSP viewpoint, a job is rejected under certain circumstances: (i) If the job cannot be completed within the deadline even after using a large number of resources, (ii) if the estimated resource capacity is greater than the available resource capacity (iii) frequent change of requirements from the client-side. The increase in DCs has driven competition among the CSPs to attract and retain customers. Though the CSPs advertise a low price, consumers do not prefer them due to the diminished QoS they offer. [38] Hence, to avoid customer loss, CSPs adopt an optimal resource provisioning policy like RL-DRP (Reinforcement Learning based Dynamic Resource Provision).

### C. Quality of Experience (QoE) in RL based RASP

In [40], the author addressed the issues of RA and achieved QoE through Smart Content-Centric Services for IoT applications (SCCS-IoT). The algorithm employs RL based Mapping Table (RLMT) to update/maintain the cost mapping table. Each IoT task is an n-tuple to represent m number of costs (energy, latency, bandwidth, execution time). The allocation path and the quality level represented the state of the environment. Each update that was carried out on the table represented the action. The sequence of costs formed the feedback. The updated cost mapping table forms the input to the second algorithm called, RL-based RA (RLRA) that generated a policy to obtain an optimal RA for the incoming tasks.

### D. Auto Reconfiguration of VMs in RL Assisted RASP

Large-scale application deployment demands adaptive techniques like RL-based RASP that dynamically configure/reconfigure the VMs and the application requirements, as needed. The RL-based framework called CoTuner synchronizes the configuration of VMs and the applications hosted in it [41]. VMs and applications in the cloud were auto-reconfigured at an optimal range to improve the resource utility and application performance in [42]. Dynamic resource configuration through RL was suggested in [43]. The delayed learning process of RL was overcome by a value-function that converged the optimal learning policy at a fast rate.

A self-adaptive learning agent called iBalloon handled the dynamic capacity management of each VM in [26]. iBalloon was based on RL in which utilization of the CPU, memory, and I/O are considered as the state of the environment. The action to be taken was of the form (no-operation, scale-up, scale-down) on the VM's resources. The Decision Maker (DM) module computed the required resource capacity. The Host Agent module monitored and reconfigured VM's resources. Any deviation from the SLA was reported back to the DM that updated the capacity management. The observations of the existing works on RL-assisted RASP are tabulated in Table V.

## V. ANALYSIS OF ENERGY EFFICIENT COMPUTING (EEC) ASSISTED RASP

With the proliferation of DCs, the CAGR (Cumulative Annual Growth Rate) of carbon emission is expected to cross 11% worldwide, which is a serious threat to be handled immediately [5]. Hence, an EEC-based RASP that minimizes energy consumption and carbon emission is required [44]. The EEC-assisted RASP is classified as thermal aware and power-aware energy management as shown in Fig. 3. In general, thermal aware energy depends on the number of resources involved rather than the temperature density of those resources. As power is directly proportionate to the temperature density of the resources, the proposed survey focuses on power-aware energy management [23].

Energy management through Load balancing tackles the overload and underload aspects of resources, only after the tasks are scheduled. Whereas, RA approach handles energy management by predicting the power consumption in advance and optimizes the resource utilization [22]. This section discusses the works related to EEC-assisted RASP under various criteria as shown in Table VI.

### A. Minimization of Energy Cost and Latency

Energy consumption and latency reduction in Fog computing were implemented in[16]. In the health care case study, the Medium Access Control (MAC) scheduler allocated the available time slots in Time Slotted Channel Hopping (TSCH) frame to the requesting sensors, by an equally spaced method. Cloudlet (an interface node between the mobile device and cloud server) assisted with Dynamic Energy Cost Minimization (DECM) technique was adopted to reduce the energy cost in [19]. Whenever applications are invoked through mobile, the DECM finds the cloudlets that reside near to the CSP. Then, the mobile request is forwarded to the recommended cloudlet.

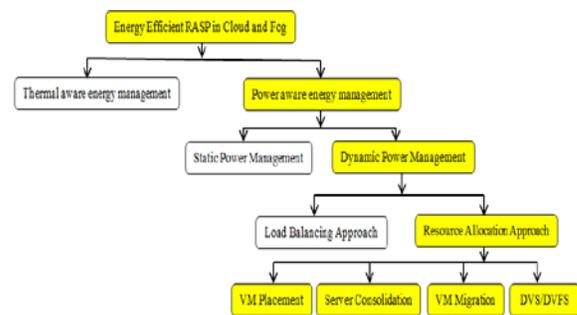


Fig. 3. Taxonomy of EEC.

TABLE VI. EEC ASSISTED RASP WORKS

Paper ID	Reference	Author	Architecture based	Algorithm-based	RA Policy			Problem Addressed			
					Reactive	Proactive	Hybrid	Energy cost and Latency Minimization	DCiE & PUE	VM Migration / Server Consolidation	DVS / DVFS
E1	[16]	La et al., 2019	✓		✓			✓			
E2	[18]	Thein et al., 2018	✓		✓				✓		
E3	[17]	Duan et al., 2017	✓			✓				✓	
E4	[45]	Shelar et al., 2017		✓	✓					✓	
E5	[19]	Gai et al., 2016		✓		✓		✓			
E6	[49]	Wu et al., 2014	✓		✓						✓
E7	[48]	Fargo et al., 2014	✓			✓					✓
E8	[20]	Basmadjian et al., 2012		✓	✓						✓
E9	[44]	Beloglazov et al., 2012		✓	✓					✓	
E10	[49]	Zhang et al., 2012	✓			✓					✓

### B. Energy Conservation through PUE and DCiE

Power Usage Effectiveness (PUE) and DC infrastructure Efficiency (DCiE) were referred to in the RA framework to compute the power consumption of a DC in [18]. PUE is the ratio of the power consumed by IT equipment to the power consumed by the total IT facility. But, DCiE is inversely proportional to PUE [23]. The framework senses the state (number of physical hosts) of the DC and takes actions (allocate or not allocate), respectively.

### C. Energy Conservation based on VM Placement, Migration, and Server Consolidation

VM migration is the process of transferring the process of the selected VMs from one host to another, to avoid overutilization or under-utilization issues [22]. VM migration enables server consolidation by utilizing only the optimal number of servers thereby shutting down the unused servers in [17]. To reduce energy consumption, the Modified Best Fit Decreasing (MBFD) algorithm[44], arranged VMs in decreasing order of CPU utilization and allocated them to the highest power-efficient host. The algorithm aiCloud optimized the total power consumption, by switching the idle and

underutilized physical machines to a power-saving state or offline state (hibernate/ sleep/standby) in [45].

### D. DVS/DVFS based Energy-Efficient Computing

The growth in the number of DCs has become a huge consumer of power. Scaling down the frequency/voltage, at the level of processor, memory, HDD, and NIC were the techniques employed to save power consumption in general. DVFS scaling that controls the frequency and voltage to maintain optimal performance was employed in [46]. The architecture specified the minimum and maximum frequency to run a job as one of the requirements, based on which the DVFS was programmed.

An Autonomic Workload and Resource Management framework (AWRM) that reduced power consumption by predicting the workload was employed in [47]. [20] [48] presented an energy-saving and carbon footprint reduction model where the processor frequency was reduced instantly, once it turned idle. The author proved that with the right combination of optimization policy and power prediction model, energy consumption was reduced by 20%. Table VII, tabulates the observations of the EEC-assisted RASP works.

TABLE VII. ANALYSIS OF ENERGY EFFICIENT COMPUTING ASSISTED RASP WORKS

Paper ID	Ref.	Problem addressed	Objective	Algorithm	Performance metrics addressed	Experiment	Evaluation	Workload	Limitations
E1	[16]	1. Time slot allocation to the sensor for transmission, 2. Device driven task offloading	To achieve energy efficiency and latency reduction in time-critical IoT applications	Mixed-integer programming based Semi-definite relaxation algorithm	Delay, power consumption, Radio duty cycle, Packet delivery ratio	Test bed-Open Mote CC2538 as fog node & border router with Raspberri-pi gateway	Compared with local processing, random assignment, all to cloud policy.	Data from ECG, Accelerometer, Temperature and humidity reading	2 case studies- applications are limited to a single user.
E2	[18]	Inefficient resource allocation consuming more energy	To achieve energy efficiency and to avoid SLAV	RL + Fuzzy logic approach	DCIE, PUE, CPU utilization, SLAV	CloudSim	experimented on the traces of the planet lab virtualized environment	Planet lab virtualized research data sets of 10	CPU alone considered for energy
E3	[17]	Non-adaptability of scheduling algorithm to peak demands instantaneously	Reduce energy consumption with high computation capacity	Fractal Mathematics (FM), Improved Ant Colony algorithm (IAC).	Energy consumption, CPU utilization, VM migration count	CloudSim (FM for prediction model, IAC to optimize energy consumption )	Compared with the first fit, round-robin, minimum migration, FM calculated by Pearson correlation coefficient.	Web services from Google cluster.	SLA violation to be addressed.
E4	[45]	Power conservation and reduction of VM placement failure rate.	Minimize frequency of VM migration, minimize active servers in DCs	aiCloud algorithm - switches idle PMs to power-saving state(sleep/standby)	Power consumption in DC, VM placement failure rate.	Test bed	Compared with FF, Best Fit (BF), and random selection.	Web service (memory and CPU intensive applications)	SLA/QoS not considered.
E5	[19]	Insufficient bandwidth and device capacity of mobile phones in accessing cloud	Minimize cost and make-span with efficient resource utilization	Dynamic programming approach	Energy and Latency	Dynamic energy cost minimization Simulator (DECM)	Mathematical comparison of DECM with traditional cloud applications	Simulated requests workload from mobile phones	Cloudlets are assumed static.
E6	[47]	Energy consumption, SLA violation	Minimize power consumption and execution time	Priority Job Scheduling algorithm.	Execution time(secs), power (watts)	CloudSim	Compared with the applicable machine and HPC machine (Max/Min scheduling MMs - DVFS)	Simulated with low workload (8000-44000 MIPS), high workload (250000-450000MIPS)	Only 3 VMs considered for power consumption
E7	[48]	Power management methodology without compromising SLA requirements.	To invoke exactly the required number of VMs and minimize power consumption	Rule-based data mining algorithm Jrip (Weka implementation of RIPPER algorithm)	Power consumption, Execution time.	Test bed configured with IBM blade server, Debian, Xen hypervisor.	Execution time & power consumption compared between static resource allocation and frequency schedule	Rubis benchmark (an auction model - emulating eBay transactions)	Correct VM configuration to be analyzed in the training phase.
E8	[20]	Energy conservation	Incentives for saving energy	Power consumption prediction model	Energy	Test bed	Lo (integrated Lights out), PCM(Power consumption model)	Steady task - constant resource, Spiky task-sudden increase of resource, Rippling task-mixed	Carbon emission to be considered
E9	[44]	Operational cost due to electricity consumption and huge carbon emission	Energy-efficient RA satisfying QoS and power usage.	Modified best fit decreasing and Minimization of migration algorithm	Power consumption, average SLA violation, No. of VM migration	CloudSim tool kit	Compared with policies, Non-power aware (NPA), DVFS, ST	Modeled web application of variable workload	Power consumption of non-compute devices missed.
E10	[49]	Virtualization challenges power consumption	To devise a power management model that reconfigures resources based on their utilization, workload, and power consumption.	Reinforcement learning algorithm	Power(watts), execution time.	Manual test bed consisting of 64 servers, Watstup Pro digital -power meter to collect power consumption.	Compared with ARMA (Auto Regression Moving Average) and CAPM (cloud adaptive power management). Validated with NPB, ioZone	NPB - CPU/memory-intensive application, ioZone - I/O intensive	SLA to be considered

## VI. ANALYSIS OF RASP IN FOG COMPUTING

The term Fog computing was proposed by Cisco systems in 2012. Cisco defines Fog as a computing architecture that extends the capabilities of the cloud closer to the things that produce and act on data. The IoT devices that produce and consume data are located in the edge network. Fog computing resides as a middle layer between the edge network and the cloud as shown in Fig. 1. The proximity of fog nodes near the edge network guarantees minimum bandwidth and latency for time-critical applications. A well-defined RASP strategy in Fog layer helps IoT realize its potential. The Fog computing-based RASP works considered for the survey are categorized in Table VIII.

### A. Profit-Cost Oriented QoS in RASP

The profit-centric service provider saved their cost by employing an optimized RA model that guaranteed less response time in [8]. An empirical approach that maximized Fog utilization and minimized cost was presented in [49]. A RA strategy that maximized the profit of both the resource provider and consumer was suggested in [50]. The contradiction between price and time in completing a task was resolved through Priced Timed Petri Nets (PTPN) in which the required resources were chosen from a group of pre-allocated resources.

Besides other requirements, the cost is a significant QoS metric for both the service provider and the user [51]. A Cost aware Fog RA for the medical cyber-physical system was presented in [51]. While the base transceiver station was employed as a fog node, the data transmission rate, delay, and service rate were the QoS metrics used to compute the total cost in allocating the resource.

### B. RASP based on Resource Utilization Oriented QoS

Resource utilization is the allocation of available resources among the competing tasks within the budget as specified in the QoS. The price of a resource depends upon whether it is over-demanded or under-demanded. A market equilibrium framework that balanced the interests of both the service (buyer) and the Fog resource (goods) was employed in [52].

A two-sided matching game problem that stabilized the association of Fog and IoT to maximize resource utilization was presented in [53]. The higher resource utilization rate indicated its optimal consumption which in turn reduces the carbon emission. A proximal algorithm that assured utility-oriented RA and reduced carbon disposal was suggested in [54].

### C. RASP based on Quality of Experience (QoE)

Quality of Experience (QoE) is the key factor to evaluate the service satisfaction of the end-user. QoE varies with the expectation of the end-user. While certain consumers are satisfied with minimal latency and bandwidth, others prefer

saving the cost. An efficient RASP strategy that enhanced the QoE of mobile users was described in [55]. A RA model that enhanced the QoE of IoT users in terms of cost reduction through the game theory approach was implemented in [56].

### D. RASP based on Bandwidth Oriented QoS

The geographical distance and insufficient bandwidth issues of the Cloud were overcome by the Fog enabled Cloud architecture called ROUTER (ResOURce management TEchnique for smaRt homes) [57]. ROUTER ensured minimum bandwidth and response time through the Particle Swarm Optimization algorithm. The algorithm found the best resource for a job (particle) through fitness value (sum of weighted values of required energy, bandwidth, latency, and response time).

Bandwidth aware Component Deployment Problem (CDP) was presented in [58]. The backtrack search algorithm picked a compatible Fog node to deploy a component (IoT request). The compatibility was verified in terms of the HW-SW requirement, communication link, and bandwidth capacity. When the requirement matched, the component was deployed in the Fog node, otherwise, the search was repeated to find a compatible Fog node. The author implemented a preprocessing procedure to reduce the search time of the Fog node.

### E. QoS of Latency, Round Trip Time (RTT), Delay and Response Time

As far as Industrial IoT is concerned, a minimal delay is the most expected QoS metric. Even Fog suffers the delay caused by the VM boot time. Hence, virtual containers that consumed less memory and instantiation time was suggested as Fog resource in [7]. The Gaussian Process Regression for Fog-Cloud Allocation (GPRFCA) was employed to decide, whether a request is to be processed in Fog or Cloud in [59]. A QoS-aware Fog Service Placement Problem (FSPP) that reduced execution cost and response time was recommended by [60].

### F. Fog Radio Access Network (Fog-RAN)

The scarcity of Fog resources was overcome by employing the fronthaul devices of the cellular network as fog devices in [39]. A loosely coupled architecture for emerging 5G networks of Fog-RAN was recommended by [39]. The architecture encouraged the participation of more Fog nodes to lessen the burden of the fronthaul on cellular networks.

A RA scheme with the radio spectrum and Fog nodes as the resource was implemented through the student project matching algorithm in [61]. The service provider maintained the list of radio spectrum and Fog resource pair to which the request was matched as per the preference of the users. The base transceiver stations, Wi-Fi access points, and femtocell routers upgraded with CPU and memory capacity served as Fog nodes to deliver ultra-high-speed latency for IoT applications in [61].

TABLE VIII. CLASSIFICATION OF RASP PAPERS IN FOG COMPUTING

Paper-ID	Reference	Author	Architecture based	Algorithm-based	Policy			Problem Addressed						
					Reactive	Proactive	Hybrid	Cost aware	Resource Utilization	QoE	Bandwidth	Latency	Fog-RAN	QoS-SLA
F1	[8]	Tran et al., 2019	✓		✓			✓						
F2	[52]	Nguyen et al., 2019		✓	✓				✓					
F3	[55]	Kim, 2019		✓	✓					✓				
F4	[57]	Gill et al., 2019	✓		✓						✓			
F5	[53]	Abedin et al., 2019	✓		✓				✓					
F6	[56]	Shah-Mansouri & Wong, 2018		✓	✓					✓				
F7	[59]	da Silva & Fonseca, 2018		✓		✓						✓		
F8	[7]	Yin et al., 2018		✓	✓							✓		
F9	[61]	Y. Gu et al., 2018		✓	✓								✓	
F10	[39]	Rahman et al., 2018		✓	✓								✓	
F11	[60]	Skarlat et al., 2017	✓		✓							✓		
F12	[49]	Mulla et al., 2017	✓		✓			✓						
F13	[58]	Brogi & Forti, 2017	✓		✓						✓			
F14	[62]	Sun & Zhang, 2017	✓		✓									✓
F15	[50]	Ni et al., 2017		✓	✓			✓						
F16	[51]	L.Gu et al., 2017		✓	✓			✓						
F17	[63]	Alsaffar et al., 2016	✓		✓									✓
F18	[54]	Do et al., 2015	✓		✓				✓					

G. QoS-SLA based RASP in Fog Computing

With scalability being a challenge to Fog, the author suggested sharing computing resources from mobile users as Fog nodes in [62]. Incentives were provided to the mobile owners who contribute to the resource pool. A Fog-Cloud federated IoT RASP architecture that optimized resource utilization and data distribution was presented in [63]. Table IXA and IXB tabulate the analysis of Fog based RASP works

VII. DISCUSSION AND CONCLUSION

A. Identified Research Gaps and Future Enhancements

The survey explores different strategies to solve the RASP problem under various domains viz., Cloud, Fog, RL, and

EEC. In the effort to solve the RASP problem arises many sub problems. Resource scalability, over-provision/under-provision of resources, violation of cost, budget, and time constraints are some of the subproblems that need to be addressed while implementing an effective RASP system. Especially, in the case of IoT applications where the requirements are stochastic and delay-sensitive.

Most of the RASP works were carried out using reactive policy. Though reactive policy incurs less cost, its case-driven programming approach does not withstand the time-sensitive requirements of IoT applications. Hence, adapting machine learning-based proactive and hybrid policies gives an effective.

TABLE IX. A. ANALYSIS OF RASP WORKS IN FOG COMPUTING

Paper ID	Ref.	Problem addressed	Objective	Algorithm	Performance metrics addressed
F1	[8]	Optimization of IoT task placement on fog	Maximize task deployment in fog & minimize response time, energy consumption, and operational cost	Empirical approach	Latency, energy, network load, operational cost.
F2	[52]	Allocation of capacity limited fog nodes to competing requests with diverse preferences.	Maximize resource utilization of fog under budget constraint	Market equilibrium (ME) solution with service requests as buyers and fog resources as goods.	Resource utilization.
F3	[55]	Inefficient coordination among mobile devices and Fog Controller in allocating resources	Maximize QoE and resource utilization, minimize task failure rate.	2 phase Gaussian model-based BVG and NBS resource allocation	Task failure probability, QoE, resource utilization at Fog Access Point (FAP)
F4	[57]	Response time issue in Fog-Cloud federated resource allocation for smart home	Optimize performance parameters through a fitness function	Particle Swarm Optimization algorithm	Response time, Bandwidth, latency, energy consumption
F5	[53]	Limited bandwidth in fog network resource allocation	Maximize fog network resource utilization for IoT applications	Analytics hierarchy process (AHP) based QoS prioritization through two-sided matching game best fit	Resource utilization, throughput, bandwidth, efficiency, job-delay
F6	[56]	Pure Nash Equilibrium problem in RA for IoT applications	Maximize QoE, minimize energy and delay	Near-optimal RA algorithm to tackle Pure Nash Equilibrium	Computation delay, average QoE, Number of IoT users benefited
F7	[59]	IoT service placement in Fog/cloud	Minimize energy consumption, request blocking, and latency.	Gaussian process regression fog-cloud allocation (GPRFCA).	Energy consumption, request block ratio, and latency.
F8	[7]	Delay due to limited resource capacity of fog in real-time analysis of smart manufacturing	Maximize Fog utilization, minimize task delay	A heuristic algorithm-based fixed threshold (FT), dynamic threshold (DT) with fixed and reallocation quota.	Number of accepted tasks, delay, execution time
F9	[61]	Instability in the allocation of channel bandwidth and computational resource for IoT in Fog	Maximize user satisfaction in terms of cost performance subject to delay, transmission quality, and power control	Student Project matching algorithm combined with user-oriented cooperation (UOC)	Latency, Service provider's revenue, data size, delay
F10	[39]	Restricted fronthaul capacity and computing delay increases the latency	To achieve ultra-low latency and optimized transmission rate	Jointly distributed computing algorithm and distributed content clustering algorithm	Delay, number of users served in fog
F11	[60]	QoS violation and execution cost	Maximize fog resource utilization with response time less than the deadline	constraint based empirical algorithm	Fog Utility, response time, make span
F12	[49]	Fault tolerance, overflow/underflow problem in resource allocation	Maximize Fog utilization	Empirical approach	Response time, DC processing time, total cost (VM cost + data transfer cost)
F13	[58]	QoS aware IoT task placement	Minimum latency and maximum task placement.	Back tracking and heuristic search	Latency and bandwidth
F14	[62]	Integration of spare resources from end-users to fog resource pool	Maximize resource utilization and income of fog broker	crowd funding algorithm approach refining Nash equilibrium	Failure rate of SLA, Task Completion time
F15	[50]	Price cost and time cost issues involved in allocating resources to IoT task in fog	Maximize resource utilization, profit of fog service providers and satisfy QoS requirements	Priced Timed Petri Nets	Task completion cost, make span

F16	[51]	Cost hike due to the unstable and long delay communication link between the medical device and datacentre	Minimize the cost of communication, delay, processing, and deployment to ensure QoS	Mixed Integer Linear Programming (MILP) through joint optimization using 2- phase LP-based heuristic algorithm	Total cost (cost of uplink comm., deployment, processing)
F17	[63]	Assurance of SLA/QoS in IoT service placement and RA in the fog-cloud federation	Improve RA and Optimization of Big data distribution	Decision rules of Linear decision tree approach	Response time, number of VMs used, Number of SLA met
F18	[54]	Joint optimization of resource allocation and carbon footprint issue	Maximize Fog utility and minimize cost with reduced carbon emission	Alternative direction method of multipliers (ADMM) as the proximal algorithm	Fog Utility and carbon emission rate

B. ANALYSIS OF RASP WORKS IN FOG COMPUTING

Paper ID	Ref.	Experiment	Evaluation	Workload	Limitations
F1	[8]	iFogSim with 28 NW configurations for task placement in fog landscape. 2)Test bed to emulate Intelligent transport system	Validated with IBM CPLEX optimization solver results	Simulated data & 65 applications from the Intelligent Transport System (ITS) with 28 scenarios tested.	Applications with independent tasks alone are considered.
F2	[52]	Amazon EC2 instances test bed coded using MATLAB, CVX/MOSEK	evaluated with five allocation schemes GEG, EG, PROP, SWM, MM benchmarks	Data set	Maximum resource capacity of fog nodes not mentioned while max. resource demand used
F3	[55]	Test bed with 25 FAP and 100 mobile devices.	evaluated with SDFC, SSEC, CFIC scheme	Mobile device generated service request (data set)	Due to reactive policy scalability issue arises.
F4	[57]	CloudSim, iFogSim	Validated with IoT based Smart Home application (SHA)	Real time- Small scale smart home automation experiment case study	PSO do not address dynamic scalability
F5	[53]	Test bed with 50 IoT devices and 10 fog devices	Validated for stability, complexity and convergence	Enhanced Mobile Broadband (eMBB) services, Ultra Reliable Low Latency Communication (URLLC) services-delay & BER (Bit Error Rate) intensive	Performance measured only for specific services
F6	[56]	Numerical Experiment and Test bed simulation	QoE at equilibrium with price of anarchy compared with social optimal cost	Simulated mobile request data set	Number of user request and computing services considered constant
F7	[59]	iFogSim, GPR implemented with gptool of python	Fog only tasks compared with fog-cloud	Remote VM application and augmented reality application.	Mobility of accessing device not considered
F8	[7]	Test bed set up	Evaluated with fixed and dynamic threshold for varying resource quota	GNOME to simulate concurrent request	Scalability issue
F9	[61]	Test bed set up with 45 to 210 IoT users	SPA, Random resource allocation, Energy Consumption and delay performance (EDM)	IoT device requests	Reactive policy restricts scalability
F10	[39]	Simulated experiment	Compared with fixed power allocation scheme and random fog clustering scheme	20 requests from 5 users for 20 fog access points	The transmission delay between fog nodes considered negligible
F11	[60]	iFogSim	evaluated with IBM Cplex solver, compared with first fit baseline & pure cloud models	Motion, video, audio, temperature-based applications	The reactive policy does not scale and fails to address stochastic requirements

F12	[49]	Cloud analyst	Efficient resource allocation (ERA) compared with existing Optimize response time (ORT) and Reconfigure dynamically with load balancing (RDLB)	Simulated data	Cannot address stochastic requirements
F13	[58]	Fog torch prototype, a proof of concept java tool.	Evaluated for expected QoS profile in 50 fog nodes	Fire alarm IoT application offered by an insurance company to its customers.	A single application tested for task placement. Scalability problem.
F14	[62]	Test bed with 50 smart phones	Validated with Minimum Migration and MBFD (Modified Best Fit Decreasing)	Test data for pressure application generated by JMeter	The static approach does not support scalability
F15	[50]	Test bed set up with dawn-3000 parallel machine with ten Linux cluster to model fog computing environment	MFR (Mapping Fog Resource to user directory scheme) compared with MinMin and MaxMin algorithm	Random function generated service requests	As resources are mapped to user price, the waiting time for a resource, increases the delay of completing user tasks.
F16	[51]	Test bed set up of 300x300 network size with 80 users and 50 Base stations.	Total cost evaluated across several base stations and 2-phase LP compared with the greedy algorithm	The medical device-generated data traffic	VM deployment in the base station is application-specific
F17	[63]	CloudSim	Internally compared among shared and reserved allocation.	The workload of multimedia big data from fog-cloud broker to use smart devices	Static number of requests and data considered for the experiment
F18	[54]	Mathematical model	Convergence rate of proximal algorithm and ADMM	Video streaming request from Akamai- the world's largest content delivery network	Only Theoretical proof of mathematical model analyzed

Solution. In general, the existing works were from the service provider's point of view saving their cost. A RASP strategy that prioritizes consumer's profit, needs focus. Deployment of multi-tier and parallel applications in fog nodes is another issue that needs attention.

The unexpected network traffic and access rate of the hosted applications were not foreseen during SLA. This leads not only in the violation of QoS requirements but some catastrophic failures of resource access. Hence dynamic provision, to monitor and configure the resources automatically with intelligence is the need for such a situation. Research on autonomic computing that possesses self-management capability will enhance the RASP strategy.

The proliferation of IoT requires unlimited bandwidth. The huge number of heterogeneous geo-distributed devices involved in the fog layer that handles IoT consumes enormous energy. Instead of draining the available energy, fog nodes that work on solar and green energy should be brought into usage. Hence, a Fog-based RASP solution that supports green environmental sustainability needs focus.

The manufacturing units in Industry, nowadays depend on Fog services for instantaneous processing. But, the protocol interoperability problem between the assembling units and Fog devices causes a delay that is not tolerable in Industrial IoT. With fewer works carried out in this area, it remains yet another open challenge in Fog research.

Findings show that based on the delay constraint of the applications, the arriving requests are segregated among the Cloud and Fog for processing. But, the question arises how the decision is made when the delay constraint is not explicitly mentioned. One possible approach is that the Cloud/Fog center can be decided based on the application type. Service requests

from critical health-care, disaster management, real-time chemical reactors, and Industrial IoT can be considered as emergent applications that need to be processed in the Fog layer.

Further, the efficiency of the RASP system can be escalated by clustering the fog nodes on application basis for processing. Instead of making all fog nodes available for processing, certain fog nodes can be employed for general purposes while the rest of the fog nodes can be reserved exclusively for emergent applications. Algorithms are to be devised that ensure maximum utilization of the fog nodes. The idle fog cluster can be employed either for the migrated emergent applications or for the local non-emergent applications during peak hours. As Fog computing is still in its infancy stage, standard protocols are yet to be explored.

## VIII. CONCLUSION

The survey elaborates various RASP strategies in Fog and Cloud environments. The survey investigated the individual work from the viewpoint of, the problem defined, objective set, algorithm adopted, performance metrics addressed, experiment and evaluation tools employed, and the workloads used for testing. The tabulated information presents an exhaustive analysis of the individual work with their limitations projected as open challenges.

Although review articles exclusive to Cloud and Fog exists, the proposed survey explores the RASP problem, in Cloud and Fog for IoT applications. The survey stands unique to employ techniques like Reinforcement Learning (RL) and Energy Efficient Computing (EEC) to save cost and energy respectively. Sure enough, the survey will motivate the researchers to focus on the research gaps and helps them to conceive innovative RASP solutions in the Fog-Cloud federation.

REFERENCES

- [1] Z.Alhara, F.Alvares, H.Bruneliere, J.Lejeune, C.Prud'Homme, and T.Ledoux, "CoMe4ACloud:Anend-to-end framework for autonomic Cloud systems," *Future Gener. Comput. Syst.*,vol. 86, pp. 339–354,Sep. 2018.
- [2] M. R. Anawar, S. Wang, M. Azam Zia, A. K. Jadoon, U. Akram, and S. Raza, "Fog Computing: An Overview of Big IoT Data Analytics," *Wirel. Commun. Mob. Comput.*, vol. 2018, pp. 1–22, 2018.
- [3] R. K. Naha et al., "Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions," *ArXiv180700976 Cs*, Jul. 2018, Accessed: Oct. 29, 2019.
- [4] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 1, pp. 416–464, 2018.
- [5] A. Hameed et al., "A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems," *Computing*, vol. 98, no. 7, pp. 751–774, Jul. 2016.
- [6] M. Cheng, J. Li, and S. Nazarian, "DRL-cloud: Deep reinforcement learning-based resource provisioning and task scheduling for cloud service providers," in *2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC)*, Jeju, Jan. 2018, pp. 129–134.
- [7] L. Yin, J. Luo, and H. Luo, "Tasks Scheduling and Resource Allocation in Fog Computing Based on Containers for Smart Manufacturing," *IEEE Trans. Ind. Inform.*, vol. 14, no.10,pp. 4712–4721, Oct. 2018.
- [8] M.-Q. Tran, D. T. Nguyen, V. A. Le, D. H. Nguyen, and T. V. Pham, "Task Placement on Fog Computing Made Efficient for IoTApplication Provision,"*Wirel. Commun.Mob.Comput.*,vol.2019, pp.1–17,Jan. 2019.
- [9] S. Soltani, P. Martin, and K. Elgazzar, "A hybrid approach to automatic IaaS service selection," *J. Cloud Comput.*, vol. 7, no. 1, Dec. 2018.
- [10] A. Singh and Y. Viniotis, "Resource allocation for IoT applications in cloud environments," in *2017 Inter Conf on Computing, Networking and Communications*, Silicon Valley, CA, USA, Jan. 2017, pp. 719–723.
- [11] T. Bhardwaj and S. C. Sharma, "Fuzzy logic-based elasticity controller for autonomic resource provisioning in parallel scientific applications: A cloud computing perspective," *Comput. Electr. Eng.*, vol. 70, pp. 1049–1073, Aug. 2018.
- [12] E.I.Djebbar and G.Belalem,"Tasks Scheduling and Resource Allocation for High Data Mgmt in ScientificCloud Computing Environment,"in *Mobile, Secure, andProgrammable Networking*, vol. 10026, S.Boumerdassi, É.Renault, and S.Bouzeffrane, Eds.Cham: Springer Inter. Publishing, 2016, pp. 16–27.
- [13] H. Atlam, R. Walters, and G. Wills, "Fog Computing and the Internet of Things: A Review," *Big Data Cogn. Comput.*, vol. 2, no. 2, p. 10, Apr. 2018.
- [14] A. S. Gowri and P. Shanthi Bala, (2020). Fog Resource Allocation Through Machine Learning Algorithm. In Goundar, S., Bhushan, S. B., & Rayani, P. K. (Ed.), *Architecture and Security Issues in Fog Computing Applications* (pp. 1-41) ch001. IGI Global.
- [15] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions," in *Internet of Everything*, B. Di Martino, K.-C. Li, L. T. Yang, and A. Esposito, Eds. Singapore: Springer Singapore, 2018, pp. 103–130.
- [16] Q. D. La, M. V. Ngo, T. Q. Dinh, T. Q. S. Quek, and H. Shin, "Enabling intelligence in fog computing to achieve energy and latency reduction," *Digit. Commun. Netw.*, vol. 5, no. 1, pp. 3–9, Feb. 2019.
- [17] H. Duan, C. Chen, G. Min, and Y. Wu, "Energy-aware scheduling of virtual machines in heterogeneous cloud computing systems," *Future Gener. Comput. Syst.*, vol. 74, pp. 142–150, Sep. 2017.
- [18] T.Thein,M.M.Myo,S.Parvin, and A. Gawanmeh, "Reinforcement learning based methodology for energy-efficient resource allocation in cloud data centers," *J. King Saud Univ.- Comput. Inf. Sci.*,Nov. 2018.
- [19] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong, "Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing," *J. Netw. Comput. Appl.*, vol. 59, pp. 46–54, Jan. 2016.
- [20] R. Basmadjian, H. Meer, R. Lent, and G. Giuliani, "Cloud computing and its interest in saving energy: the use case of a private cloud," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 1, no. 1, p. 5, 2012.
- [21] M. Xu and R. Buyya, "Brownout Approach for Adaptive Management of Resources and Applications in Cloud Computing Systems: A Taxonomy and Future Directions," *ACM Comput. Surv.*, vol. 52, no. 1, pp. 1–27, Jan. 2019.
- [22] M. Hosseini Shirvani, A. M. Rahmani, and A. Sahafi, "A survey study on virtual machine migration and server consolidation techniques in DVFS-enabled cloud datacenter: Taxonomy and challenges," *J. King Saud Univ. - Comput. Inf. Sci.*, Jul. 2018.
- [23] M. Zakarya and L. Gillam, "Energy efficient computing, clusters, grids and clouds: A taxonomy and survey," *Sustain. Comput. Inform. Syst.*, vol. 14, pp. 13–33, Jun. 2017.
- [24] S. Zahoor and R. N. Mir, "Resource management in pervasive Internet of Things: A survey," *J. King Saud Univ. - Comput. Inf. Sci.*, Sep. 2018.
- [25] M. Ghobaei-Arani, A. Soury, and A. A. Rahmani, "Resource Management Approaches in Fog Computing: a Comprehensive Review," *J. Grid Comput.*, Sep. 2019.
- [26] J. Rao, X. Bu, C.-Z. Xu, and K. Wang, "A Distributed Self-Learning Approach for Elastic Provisioning of Virtualized Cloud Resources," in *IEEE 19th International Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems*,Singapore, Singapore, Jul. 2011, pp. 45–54.
- [27] A. Keshavarzi, A. Toroghi Haghghat, and M. Bohlouli, "Adaptive Resource Management and Provisioning in the Cloud Computing: A Survey of Definitions, Standards and Research Roadmaps," *KSII Trans. Internet Inf. Syst.*, vol. 11, no. 9, Sep. 2017.
- [28] P. D. Kaur and I. Chana, "A resource elasticity framework for QoS-aware execution of cloud applications," *Future Gener. Comput. Syst.*, vol. 37, pp. 14–25, Jul. 2014.
- [29] K.RahimiZadeh,M.AnaLoui, P. Kabiri, and B. Javadi,"Performance modeling and analysis of virtualized multi-tier applications under dynamic workloads," *J. Netw.Comput.Appl.*,vol.56,pp.166–187, Oct. 2015.
- [30] G.Ismayilov and H.R.Topcuoglu,"Neuralnetworkbased multi-objectiveevolutionary algorithm for dynamic workflow scheduling in cloud," *Future Gener. Comput. Syst.*, vol. 102, pp. 307–322, Jan. 2020.
- [31] S. Islam, J. Keung, K. Lee, and A. Liu, "Empirical prediction models for adaptive resource provisioning in the cloud," *Future Gener. Comput. Syst.*, vol. 28, no. 1, pp. 155–162, Jan. 2012.
- [32] A. Ashraf, "Automatic Cloud Resource Scaling Algorithm based on Long Short-Term Memory Recurrent Neural Network," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 12, 2016.
- [33] Dr. A. Agarwal and S. Jain, "Efficient Optimal Algorithm of Task Scheduling in Cloud Computing Environment," *Int. J. Comput. Trends Technol.*, vol. 9, no. 7, pp. 344–349, Mar. 2014.
- [34] J. Espadas, A. Molina, G. Jiménez, M. Molina, R. Ramírez, and D. Concha, "A tenant-based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures," *Future Gener. Comput. Syst.*, vol. 29, no. 1, pp. 273–286, Jan. 2013.
- [35] E. Casalicchio and L. Silvestri, "Mechanisms for SLA provisioning in cloud-based service providers," *Comput. Netw.*, vol. 57, no. 3, pp. 795–810, Feb. 2013.
- [36] H. Xu and B. Li, "Anchor: A Versatile and Efficient Framework for Resource Management in the Cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1066–1076, Jun. 2013.
- [37] A. Nassar and Y. Yilmaz, "Reinforcement Learning for Adaptive Resource Allocation in Fog RAN for IoT With Heterogeneous Latency Requirements," *IEEE Access*, vol. 7, pp. 128014–128025, 2019.
- [38] F.Bahrpeyma,H.Haghighi, and A.Zakerolhosseini, "An adaptive RL based approach for dynamic resource provisioning in Cloud virtualized data centers," *Computing*, vol. 97, no. 12, pp. 1209–1234, Dec. 2015.
- [39] G. M. S. Rahman, M. Peng, K. Zhang, and S. Chen, "Radio Resource Allocation for Achieving Ultra-Low Latency in Fog Radio Access Networks," *IEEE Access*, vol. 6, pp. 17442–17454, 2018.

- [40] K. Gai and M. Qiu, "Optimal resource allocation using reinforcement learning for IoT content-centric services," *Appl. Soft Comput.*, vol. 70, pp. 12–21, Sep. 2018.
- [41] Xiangping Bu, Jia Rao, and Cheng-Zhong Xu, "Coordinated Self-Configuration of Virtual Machines and Appliances Using a Model-Free Learning Approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 4, pp. 681–690, Apr. 2013.
- [42] C.-Z. Xu, J. Rao, and X. Bu, "URL: A unified reinforcement learning approach for autonomic cloud management," *J. Parallel Distrib. Comput.*, vol. 72, no. 2, pp. 95–105, Feb. 2012.
- [43] X. Dutreilh, S. Kirgizov, O. Melekhova, J. Malenfant, and N. Rivierre, "Using Reinforcement Learning for Autonomic Resource Allocation in Clouds: Towards a Fully Automated Workflow," p. 8, 2011.
- [44] A. Beloglazov, J. Abawajy, and R. Buyya, "Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing," *Future Gener. Comput. Syst.*, vol. 28, no. 5, pp. 755–768, May 2012.
- [45] M. Shelar, S. Sane, V. Kharat, and R. Jadhav, "Autonomic and energy-aware resource allocation for efficient management of cloud data centre," in *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*, Vellore, Apr. 2017, pp. 1–8.
- [46] C.-M. Wu, R.-S. Chang, and H.-Y. Chan, "A green energy-efficient scheduling algorithm using the DVFS technique for cloud datacenters," *Future Gener. Comput. Syst.*, vol. 37, pp. 141–147, Jul. 2014.
- [47] F. Fargo, C. Tunc, Y. Al-Nashif, A. Akoglu, and S. Hariri, "Autonomic Workload and Resources Management of Cloud Computing Services," in *2014 Inter. Conf. on Cloud and Autonomic Computing*, United Kingdom, Sep. 2014, pp. 101–110.
- [48] Z. Zhang, Q. Guan, and S. Fu, "An adaptive power management framework for autonomic resource configuration in cloud computing infrastructures," in *2012 IEEE 31st International Performance Computing and Communications Conference (IPCCC)*, Austin, TX, USA, Dec. 2012, pp. 51–60.
- [49] M. Mulla, M. Satabache, and N. Purohit, "An Efficient Architecture for Resource Provisioning in Fog Computing," *Int. J. Sci. Res. IJSR*, vol. 6, no. 1, pp. 2065–2069, Jan. 2017.
- [50] L. Ni, J. Zhang, C. Jiang, C. Yan, and K. Yu, "Resource Allocation Strategy in Fog Computing Based on Priced Timed Petri Nets," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1216–1228, Oct. 2017.
- [51] L. Gu, D. Zeng, S. Guo, A. Barnawi, and Y. Xiang, "Cost Efficient Resource Management in Fog Computing Supported Medical Cyber-Physical System," *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 1, pp. 108–119, Jan. 2017.
- [52] D. T. Nguyen, L. B. Le, and V. Bhargava, "A Market-Based Framework for Multi-Resource Allocation in Fog Computing," *ArXiv180709756 Cs*, Apr. 2019, Accessed: Oct. 29, 2019.
- [53] S. F. Abedin, Md. G. R. Alam, S. M. A. Kazmi, N. H. Tran, D. Niyato, and C. S. Hong, "Resource Allocation for Ultra-Reliable and Enhanced Mobile Broadband IoT Applications in Fog Network," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 489–502, Jan. 2019.
- [54] C.T.Do,N.H.Tran, Chuan Pham, Md. G. R. Alam, Jae Hyeok Son, and C. S. Hong, "A proximal algorithm for joint resource allocation and minimizing carbon footprint in geo-distributed fog computing," in *Inter Conf. on Information Networking (ICOIN)*, Cambodia, Jan. 2015, pp. 324–329.
- [55] S. Kim, "Novel Resource Allocation Algorithms for the Social Internet of Things Based Fog Computing Paradigm," *Wirel. Commun. Mob. Comput.*, vol. 2019, pp. 1–11, Feb. 2019.
- [56] H. Shah-Mansouri and V. W. S. Wong, "Hierarchical Fog-Cloud Computing for IoT Systems: A Computation Offloading Game," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3246–3257, Aug. 2018.
- [57] S. S. Gill, P. Garraghan, and R. Buyya, "ROUTER: Fog enabled cloud based intelligent resource management approach for smart home IoT devices," *J. Syst. Softw.*, vol. 154, pp. 125–138, Aug. 2019.
- [58] A. Brogi and S. Forti, "QoS-Aware Deployment of IoT Applications Through the Fog," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1185–1192, Oct. 2017.
- [59] R.A.C.daSilvaand N. L. S. da Fonseca, "Resource Allocation Mechanism for a Fog-Cloud Infrastructure," in *2018 IEEE Inter Conference on Communications (ICC)*, Kansas City, MO, May 2018, pp. 1–6.
- [60] O.Skarlat,M. Nardelli,S.Schulte,and S.Dustdar,"Towards QoS-Aware Fog Service Placement," in *IEEE 1st International Conf.rence on Fog and Edge Computing (ICFEC)*, Madrid, Spain, May 2017, pp. 89–96.
- [61] Y. Gu, Z. Chang, M. Pan, L. Song, and Z. Han, "Joint Radio and Computational Resource Allocation in IoT Fog Computing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7475–7484, Aug. 2018.
- [62] Y. Sun and N. Zhang, "A resource-sharing model based on a repeated game in fog computing," *Saudi J. Biol. Sci.*, vol. 24, no. 3, pp. 687–694, Mar. 2017.
- [63] A. A. Alsaffar, H. P. Pham, C.-S. Hong, E.-N. Huh, and M. Aazam, "An Architecture of IoT Service Delegation and Resource Allocation Based on Collaboration between Fog and Cloud Computing," *Mob. Inf. Syst.*, vol. 2016, pp. 1–15, 2016.

# Performance Analysis of Deep Neural Network based on Transfer Learning for Pet Classification

Bhavesh Jaiswal<sup>1</sup>, Nagendra Gajjar<sup>2</sup>

Department of Electronics and Communication Engineering  
Institute of Technology, Nirma University, SG Highway  
Ahmedabad, Gujarat, India

**Abstract**—Deep learning frameworks have progressed beyond human recognition capabilities and, now it's the perfect opportunity to optimize them for implementation on the embedded platforms. The present deep learning architectures support learning capabilities, but they lack flexibility for applying learned knowledge on the tasks in other unfamiliar domains. This work tries to fill this gap with the deep neural network-based solution for object detection in unrelated domains with a focus on the reduced footprint of the developed model. Knowledge distillation provides efficient and effective teacher-student learning for a variety of different visual recognition tasks. A lightweight student network can be easily trained under the guidance of the high-capacity teacher networks. The teacher-student architecture implementation on binary classes shows a 20% improvement in accuracy within the same training iterations using the transfer learning approach. The scalability of the student model is tested with binary, ternary and multiclass and their performance is compared on basis of inference speed. The results show that the inference speed does not depend on the number of classes. For similar recognition accuracy, the inference speed of about 50 frames per second or 20ms per image. Thus, this approach can be generalized as per the application requirement with minimal changes, provided the dataset format compatibility.

**Keywords**—Machine learning; knowledge distillation; transfer learning; domain adaptation

## I. INTRODUCTION

Deep neural networks are thriving, due to vast data availability, newer complex models, and heterogeneous compute capacity. The data accumulation ease and its open-source availability are opening new doors for the research community. So new models are popping up almost every day on how to solve real-world problems using that data. Now crunching the data is also getting cheaper day by day, and one does not require a personal high-end custom configured system for this job. It is offloaded to cloud-based solutions provided by Amazon, Google, and Microsoft. Traditional machine learning & data mining algorithms make predictions using statistical models and trained on labelled or unlabelled training datasets. As the labelled data may be too few in practical applications; so to build a good classifier; semi-supervised classification done by using a large amount of unlabelled data and a small amount of labelled data [1], [2], [3]. In [4], the problem of how to deal with the noisy-class label is explored. Similarly, in [5], cost-sensitive learning is considered. In [6], it is shown that having a minimum depth to the network is vital

for the model performance. All these approaches assumed that the distributions of the labelled and unlabelled data were the same.

For implementation on edge-based devices, the model size could be cut down by the compression techniques at various levels in the model, data, and computation. The classic Alexnet [7] was trained on the Imagenet dataset and performed 2.27 billion operations with 238MB of memory usage for storing the model data itself. In the compressed model, Squeezenet [8] performs 2.17 billion of operation but with a smaller footprint of 4.8MB, while Darknet [9], an open source for the Yolo [10], does less than 1 billion operations with 28MB of the footprint. Note that this comparison is assuming a baseline accuracy of 80 per cent in recognizing the labelled visuals. It does not include the run time memory requirements while performing the computation, which is not directly proportional to the number of operations performed as neural networks are non-linear models. Also, compression-decompression takes more computation power. Mobilenet [11] tries to address this problem to an extent. Though the model size is reduced from the storage perspective but while performing the inference on a lightweight platform, they may fail to give the real-time response due to resource constraints. To make them predict with a high confidence value [12] the semantic segmentation approach from [13], [14] is used by [15], [16], [17].

The practical implementation of the deep neural network in real-life scenarios is quite the opposite of the earlier description. IoT based heterogeneous devices have resource constraints that limit their use on them. They mostly offload this to the cloud, but that solution is not always feasible due to the latency involved. This work explores the knowledge distillation approach in deep neural networks for IoT edge devices for real-time applications. The contribution of this work is to train a smaller model for a lightweight target platform with a negligible loss of accuracy. The proposed lightweight model can be easily customized to the different domains and can be easily ported to IoT based edge devices. Section 2 details why deep learning on heterogeneous edge devices is difficult to implement. In Section 3, the state of the art approaches for model reduction is presented. Section 4 delves into the knowledge distillation approach and how it can be used on the edge-based device followed by experimental setup and performance analysis of the implementation.

## II. DEEP LEARNING ON EDGE DEVICES

Convolution Neural Networks models have evolved to surpass the human capabilities in image classification task but when it comes to their deployment on the edge devices, there use is limited due to various resource constraints as described below:

### A. Limited Data

The large dataset is not available in all circumstances for the training of the network and even it is available it may be quite expensive in terms of time and feasibility. Data privacy is another factor which forces to work with lesser data locally on the device itself.

### B. Limited Model Footprint

Models which thrusted the growth of DNN with their accuracy limits surpassing humans are quite bulky in terms of memory requirements for storage. This memory could be either for storage of the model or for the storage of the millions of the weights calculated during the runtime. For practical implementation, the memory footprint of the application should be small enough to fit into any embedded device.

### C. Limited Computation

Even with lesser data and smaller models the solution does not work out. Because of the millions of intermediate weights computation, it involves during the model run, it may require a desktop/server capability to finish the task in real time. The computational latency is not tolerable in the practical application involving the heterogeneous edge device. Now as the heterogeneous edge devices has limited capabilities, one need to devise the ways to eliminate or reduce these limitation causes. The next section describes this in detail.

## III. DEEP NEURAL NETWORK REDUCTION

Though DNNs have the tremendous diversity of structures, still the core computation of a network is the variations of matrix-multiplications or more precisely multiply-and-accumulate (MAC) operations. The factors which effect the MAC operations are batch size, image dimensions, filter type, no. of channels, kernel size and activation size. These combined for every neuron to neuron connections make the millions of hyper-parameters of the DNN.

To reduce these transformation functions parameterized by learnable weights, researchers worldwide have developed their own various model compression techniques, but only some of the well-researched approaches are covered here for brief overview.

### A. Pruning

The hyper parameter space of the DNN is reduced by trimming the network physically or pruning the network itself in various ways.

The unimportant weight connections can be pruned if they are below a predefined threshold or if they are redundant. About 50% of the weights can be pruned without fine-tuning and with fine-tuning, more than 80% of the weights can be pruned [18]. The pruning of the weights can be driven by energy distribution for the network [19]. In Energy Inference

Engine [20], the sparse weights after pruning can also be compressed to reduce memory access bandwidth. Huffman coding is used to reduce storage and bandwidth requirements for weights by 20-30% [21].

Another approach to trim the individual neurons is that if they are redundant [22]. As these are basic element of the network so the associated connections of the neuron will also be obliterated. In the literature many ways are researched to do this type of pruning, even some of the neuron layers which do not contribute much in the network updation can also be removed [23].

Convolutional filters are applied to the data and according to their importance, they can be eliminated from the network. The filter's importance can be known by their influence on the weight calculation or L1/L2 norm [24]. Other methods are also researched in the literature which is not the scope of this work.

### B. Quantization

The network architecture can be improved in many ways e.g. by reducing the quantity of weights and number of operations. The large convolution operation can be replaced with a number of smaller convolution operators having fewer weights in total, keeping the effective receptive field same i.e. large filters can be emulated with several of the smaller size filters in cascade e.g. convolution of size  $n$  by  $n$  can be made by combining 1 by  $n$  convolution with  $N$  by 1 convolution [21]. SqueezeNet [25] uses this approach to achieve an overall reduction in number of weights up to 50x compared to AlexNet, while keeping the accuracy in similar range.

Weights of fully connected layers can be quantized using Regularization technique [26], [27]. Clustering by 'k-means' [28] achieved more than 20x compression with negligible loss of accuracy. Hashed Nets [29] use a low-cost hash function to group weights into hash buckets to share parameters.

### C. Knowledge Distillation

Knowledge distillation (KD) was introduced by [30] as:

- Train a large model that performs and generalizes very well. This is called the teacher model.
- Take all the data you have and compute the predictions of the teacher model. The total dataset with these predictions is called the knowledge, and the predictions themselves are often referred to as soft targets. This is the knowledge distillation step.
- Use the previously obtained knowledge to train the smaller network, called the student model.

Fig. 1 summarizes this pictorially.

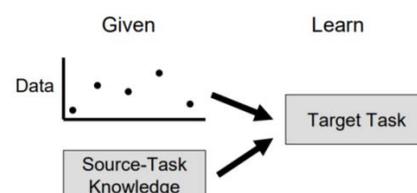


Fig. 1. Example of a Transfer Learning Model.

#### IV. TEACHER-STUDENT LEARNING

Knowledge distillation starts with training a larger model, the teacher 'T'. As it is trained on a heavier platform (GPU), it achieves high performance. Then a lightweight model known as student 'S' is deployed to learn from 'T'. Now, 'S' is supposed to give comparable performance as 'T' but with less memory and more speed.

To improve knowledge transfer from teacher to student various types of methods are researched. Assuming a trained 'T' has already eliminated some label errors contained in the ground truth data, the authors in [29] treated the hard label predicted by 'T' as the underlying knowledge. While in [30], the soft label produced by 'T', i.e., the classification probabilities, are focused to provide more information to transfer. In general, knowledge is transferred from the 'T' to 'S' by minimizing a loss function in which the target is the distribution of class probabilities predicted by 'T'. This probability distribution has the correct class at a very high probability (close to '1') with all other class probabilities very close to '0'. As such, it does not provide much information beyond the ground truth labels already provided in the dataset. For this, Hinton [30], introduced the concept of "softmax temperature". As it grows, the probability distribution generated by the softmax function becomes softer, providing more information as to which classes 'T' found more like the predicted class. This is the "dark knowledge" embedded in the 'T' and transferred to 'S' in the distillation process. The distillation related work can be categorized as below:

- Feature Map: The feature map across channel dimension can be averaged to obtain spatial attention map [31]. The inner product of two feature maps can be used for the inter-layer flow [32]. The author in [33] improved this idea with singular value decomposition (SVD). A recent work [34] demonstrated the effectiveness of mimicking feature map directly in distillation.
- Transfer strategy: FitNets [35] selected a hidden layer from 'T' and 'S' to be hint layer and guided layer respectively. 'S' can get a better initialization through pre-training the guided layer with the hint layer as supervision. Net2net [36] proposed a function-preserving transformation, which makes it possible to directly reuse it from 'T' to initialize the hyperparameters of 'S'.
- Hybrid strategy: Adversarial learning is used with distillation by using a comparator to check the outputs of 'S' and 'T' are close enough or not [37]. The author in [38] exploited reinforcement learning to search the best network structure of 'S' under the influence of 'T'. In [39] and [40] progressive or lifelong learning is referred to make knowledge transfer step by step.

Looking to this a novel approach to developing deep learning models for various domains is proposed. As every student in a class distribution may not have a similar capability or generally it a Gaussian curve. To flatten the curve on the higher side of learning capability, the model tries to imbibe the relative knowledge which can be used on the lightweight students to perform the object detection task with comparable performance. The aim is, to provide a generic solution to the problem with the assumption that the model can only be transferred successfully using the smaller dataset avoiding the limitations of the domain transfer.

#### V. EXPERIMENTAL EVALUATION AND DISCUSSION

A popular framework Caffe [41] is chosen for the binary image classification task. The Redux Dogs vs. Cats competition dataset [42] is used for training and testing purpose on NVIDIA GTX 770 with 1536 GPU cores [43]. The training data consists of 12500 images of each for Cats and Dogs. For testing phase 12500 images random images from the dataset are chosen.

The model calculates the probability of a pet and assigns a numeric value between 0 and 1 for the predicted class. Currently the implementation involves binary classification; cat and dog, but it can be extended easily to include other types of pets. For that the model will give the probability values for each class and the highest value is the closest. The accuracy of the implemented training models depends on the model training parameters and varies with change in hyper parameters that itself is a separate research area. The log-loss formula can be used to represent the accuracy of any model:

$$\text{Logloss} = -\frac{1}{n} \sum_{i=1}^n [y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i)] \quad (1)$$

Where, n represents the number of images in the test set. y the prediction probability for the dog and y^ equals to '1' if the current image is identified as a dog or equals to '0' if a current image is predicted as cat. The log-loss probability is calculated for each run and note that a smaller value of log loss is desired.

First, the complex teacher model is trained using labeled data and then same is tested with the unlabeled data to classify the pet either cat or dog. Fig. 2(a) shows the learning curve of the teacher model achieving 75% validation accuracy in 1500 iterations which occurred in about 2 and ½ hours. Further, the weights from the teacher model are used to pass to the student model as per knowledge distillation criteria, i.e., the student model is initialized with the pre-trained data/weights from the teacher model. Fig. 2(b) shows the training/learning curve of the student model achieving a 95% validation accuracy in about 1000 iterations which occurred in less than 2 hours.

In Table I, while doing transfer learning, the accuracy has jumped from 75% to 95% that too in lesser run time. The log loss value also comes down close to unity, the ideal log loss value for this problem.

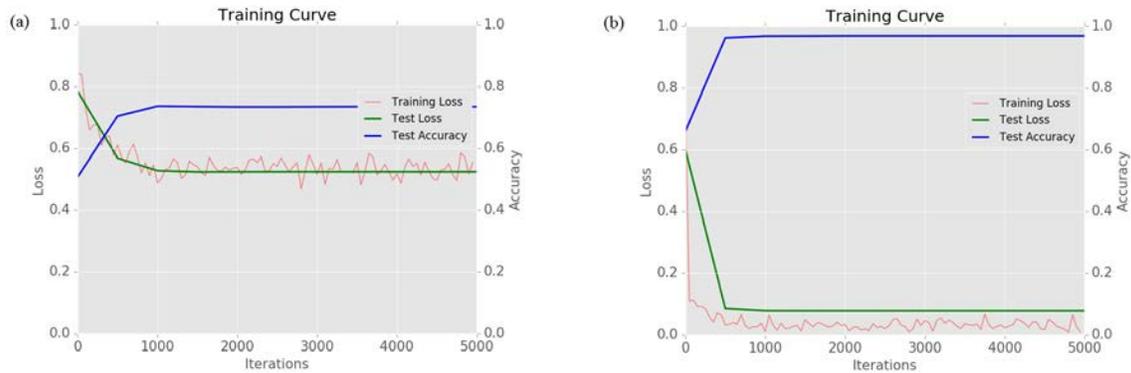


Fig. 2. Learning Curve for (a) Teacher Model; (b) Student Model.

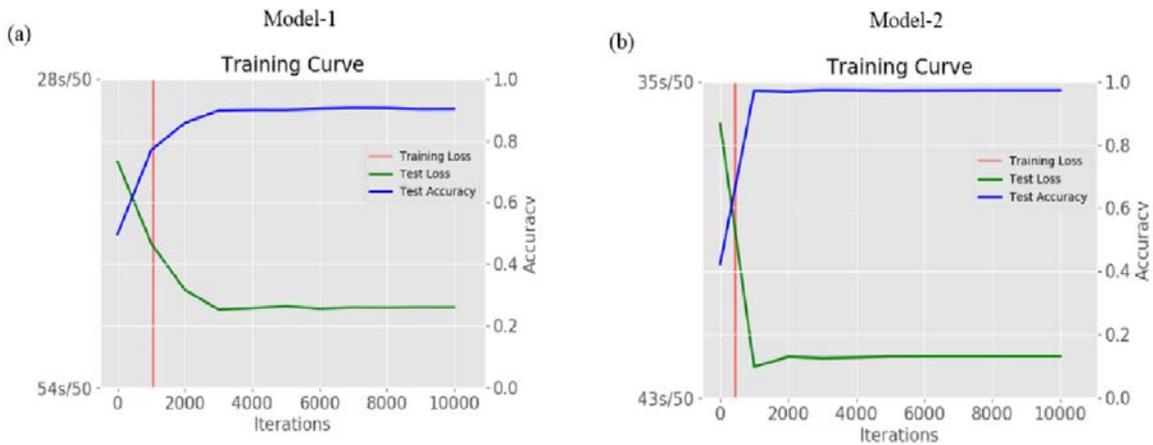


Fig. 3. Learning Curve for the GPU with Previous (a) Teacher Model; (b) Student Model.

TABLE I. PERFORMANCE COMPARISON FOR TWO MODELS

Parameters	Teacher (Training run)	Student (Transfer learning)
Accuracy (%)	75	95
Iteration	1500	1000
Time Taken (minutes)	155	110
Log Loss	8.9	1.1

To validate the transfer learning results further multiple runs are conducted on the higher capacity single GPU (NVIDIA GTX 1080Ti with 3584 cores) [44] configuration and with dual GPU configuration. The results are shown in Fig. 3 and summarized in Table II. It shows the comparison matrix from all the test runs on various GPU platforms. In model 1, using the GPU with significantly greater number of cores reduces the number of iterations to achieve the similar results and it converges faster. On the other hand, with model 2, the results are similar both in terms of accuracy and number of iterations irrespective of the platform availability. It indicates that transfer learning-based approach comes out as a clear winner for limited resource environment.

Next, the task is performed for binary, ternary, and multiclass identification and their performance is compared on basis of inference speed. The results show in Table III that the inference speed does not depend on the number of classes. The

multiple domains are also considered to prove that for similar recognition accuracy the inference speed achieved is about 50 frames per second or 20ms per image.

TABLE II. RESULTS FROM VARIOUS GPU CORES

Platform NVIDIA GPU core count	Model-1 (Training)		Model-2 (Transfer Learning)	
	Accuracy (%)	Number of Iterations	Accuracy (%)	Number of Iterations
1536	75	1500	95	1000
3584	75/90	1000/4000	96	1000
3584 x 2	75/90	1000/4000	96	<1000

TABLE III. PERFORMANCE COMPARISON FOR MULTICLASS DETECTION

Classification	Object Labelled	Inference Speed
Binary	Cat and Dog	1.5fps 0.663s/image
Ternary1	Date, fig and hazelnut	2.95 fps 0.339s/image
Ternary2	Platelets, RBC, and WBC	142 fps 0.007s/image
Multi-class (5-classes)	Docks, Boats, Lifts, Jetskis, and Cars	48 fps 0.020s/image

## VI. CONCLUSION

It can be safely concluded that using transfer learning approach a student model converges faster than the original complex teacher model. This directly translates to the saving in resource for each run of the learning which is exactly what is required for the implementation of CNN on heterogeneous embedded platform with lesser resources as now the lesser powerful embedded GPU (compared to discrete ones) can achieve similar accuracy. The results will make deployment and inferencing of DNN in heterogeneous devices easier and devices friendly. General-purpose experimentation platforms like raspberry-pi can be also used for the same. For the future work Nvidia latest platform like Jetson-TK [45] can be considered for real time implementation of this approach.

GPU acceleration and model compression are orthogonal to each other. How much a model can be compressed and accelerated subject to given resource constraints (storage, computational power, and energy) and user-specified performance goals (accuracy, latency) is open research question. The development of the generalized model compression and acceleration framework would add another value to it. More research in this area can lead to trade-off between model compression and acceleration dynamically.

## ACKNOWLEDGMENTS

The first author would like to thank the faculty/staff of Institute of Technology, Nirma University for the laboratory work support.

## REFERENCES

- [1] A. S. Razavian, H. Azizpour, J. Sullivan, and S. Carlsson, "CNN Features off-the-shelf: An Astounding Baseline for Recognition," *arXiv.org*, 2014. <https://arxiv.org/abs/1403.6382v3>.
- [2] J. Donahue, et.al., "DeCAF: A Deep Convolutional Activation Feature for Generic Visual Recognition," *Proceedings of the 31st International Conference on Machine Learning*, vol. 32, pp. 647-655, 2014.
- [3] M. D. Zeiler and R. Fergus, "Visualizing and Understanding Convolutional Networks," *Computer Vision, ECCV 2014*, pp. 818-833, 2014.
- [4] X. Zhu, X. Wu, "Class Noise vs. Attribute Noise: A Quantitative Study," *Artificial Intelligence Review* 22, pp. 177-210, 2004.
- [5] Qiang Yang, C. Ling, X. Chai, and Rong Pan, "Test-cost sensitive classification on data with missing values," *IEEE Transactions on Knowledge and Data Engineering*, vol. 18, no. 5, pp. 626-638, 2006.
- [6] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, "How transferable are features in deep neural networks?" *Advances in Neural Information Processing Systems*, vol. 27, 2014.
- [7] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," *Advances in Neural Information Processing Systems*, vol. 25, 2012.
- [8] F. N. Iandola, et.al., "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size," *arXiv.org*, 2016. <https://arxiv.org/abs/1602.07360>.
- [9] J. Redmon, "Darknet: Open Source Neural Networks in C," [online] <http://pjreddie.com/darknet/>, 2013-2016.
- [10] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, doi: 10.1109/cvpr.2016.91.
- [11] A. G. Howard, et.al., "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," *arXiv.org*, 2017. <https://arxiv.org/abs/1704.04861>.
- [12] J. Long, E. Shelhamer, and T. Darrell, "Fully Convolutional Networks for Semantic Segmentation," *CVPR 2015*. *arXiv.org* <https://arxiv.org/pdf/1411.4038v2.pdf>.
- [13] A. Nguyen, J. Yosinski, and J. Clune, "Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images," *arXiv.org*, 2015. <https://arxiv.org/abs/1412.1897v4>.
- [14] L. C. Chen, et.al., "Semantic Image Segmentation with Deep Convolutional Nets and Fully Connected CRFs," *arXiv.org*, 2014. <https://arxiv.org/abs/1412.7062v4>. *ICLR2015*.
- [15] R. Girshick, "Fast R-CNN," *IEEE International Conference on Computer Vision (ICCV)*, 2015.
- [16] S. Ren, et.al., "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 6, pp. 1137-1149, Jun. 2017.
- [17] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Mask R-CNN," *arXiv.org*, *ICCV*, 2017. <https://arxiv.org/abs/1703.06870v3>.
- [18] Han, S., Pool, J., Tran, J., Dally, W. Learning both weights and connections for efficient neural network. *Advances in neural information processing systems*, 28, pp. 1135-1143, 2015.
- [19] Yang, T.-J., Chen, Y.-H., Sze, V. "Designing energy-efficient convolutional neural networks using energy-aware pruning", *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 6071-6079, 2017.
- [20] Han, S., Liu, X., Mao, H., Pu, J., Pedram, A., Horowitz, M.A., Dally, W. "EIE: efficient inference engine on compressed deep neural network", *ACM/IEEE 43rd Annual International Symposium on Computer Architecture (ISCA)*, pp. 243-254, 2016.
- [21] Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., Wojna, Z. "Rethinking the inception architecture for computer vision", *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 2818-2826, 2016.
- [22] Srinivas S., Babu R.V. "Data-free parameter pruning for deep neural networks", *British Machine Vision Conference (BMVC)*, pp. 31.1-31.12, 2015.
- [23] Chen S., Zhao, Q. "Shallowing deep networks: layer-wise pruning based on feature representations", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41, 12, 3048-3056, 2018.
- [24] Li H., Kadav A., Durdanovic I., Samet H., Graf H.P. "Pruning filters for efficient convnets", 5<sup>th</sup> International Conference on Learning Representations (ICLR), 2017.
- [25] Iandola, F.N., Moskewicz, M.W., Ashraf, K., Han, S., Dally, W.J., Keutzer, K. "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <1 MB model size", 5<sup>th</sup> International Conference on Learning Representations (ICLR), 2017.
- [26] Bucila, C., Caruana, R., Niculescu-Mizil, A. "Model compression", *Proceedings of the 12<sup>th</sup> ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 535-541, 2006.
- [27] Souli'e, G., Gripon, V., Robert, M. "Compression of deep neural networks on the fly", *International Conference on Artificial Neural Networks*, *Lecture Notes in Computer Science*, 9887, pp. 153-160, 2016.
- [28] Gong, Y., Liu, L., Yang, M., Bourdev, L. "Compressing deep convolutional networks using vector quantization," 2014. <https://arxiv.org/abs/1412.6115>.
- [29] Ba, J., Caruana, R. "Do deep nets really need to be deep?" *Proceedings of the 27th International Conference on Neural Information Processing Systems (NIPS'2014)*, 2, pp. 2654-2662, 2014.
- [30] Hinton, G., Vinyals, O., Dean, J. "Distilling the knowledge in a neural network," 2015. <https://arxiv.org/abs/1503.02531>.
- [31] Zagoruyko, S., Komodakis, N. "Paying more attention to attention: Improving the performance of convolutional neural networks via attention transfer", 5<sup>th</sup> International Conference on Learning Representations (ICLR), 2017.
- [32] Yim, J., Joo D., Bae, J., Kim, J. "A gift from knowledge distillation: Fast optimization, network minimization and transfer learning", *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 7130-7138, 2017.

- [33] Lee, S. H., Kim, D. H., Song, B. C. "Self-supervised knowledge distillation using singular value decomposition", European Conference on Computer Vision (ECCV), pp. 339-354, 2018.
- [34] Gao, M., Shen, Y., Li, Q., Yan, J., Wan, L., Lin, D., Loy, C. C., Tang, X. "An embarrassingly simple approach for knowledge distillation," 2018, arXiv:1812.01819
- [35] Romero, A., Ballas, N., Kahou, S. E., Chassang, A., Gatta, C., Bengio, Y. "Fitnets: Hints for thin deep nets", 3rd International Conference on Learning Representations (ICLR), 2015.
- [36] Chen, T., Goodfellow, I., Shlens J. "Net2net: Accelerating learning via knowledge transfer", 4<sup>th</sup> International Conference on Learning Representations (ICLR) 2016.
- [37] Belagiannis, V., Farshad, A., Galasso, F. "Adversarial network compression", European Conference on Computer Vision (ECCV), pp. 431-449, 2018.
- [38] Ashok, A., Rhinehart, N., Beainy, F., Kitani, K. M. "N2n learning: Network to network compression via policy gradient reinforcement learning", 6th International Conference on Learning Representations (ICLR), 2018.
- [39] Wang, H., Zhao, H., Li, X., Tan, X. "Progressive blockwise knowledge distillation for neural network acceleration", Proceedings of the 27th International Joint Conference on Artificial Intelligence (IJCAI), pp.2769-2775, 2018.
- [40] Gao, Mengya, et al. "Residual knowledge distillation", arXiv preprint arXiv:2002.09168. 2020.
- [41] Jia, Y., Shelhamer, E., Donahue, J., Karayev, S., Long, J., Girshick, R., Guadarrama, S. "Caffe: convolutional architecture for fast feature embedding", Proceedings of the 22nd ACM International Conference on Multimedia, pp. 675-678, 2014.
- [42] Kaggle's Dogs Versus Cats Competition. or <https://www.kaggle.com/c/dogs-vs-cats-redux-kernels-edition/>.
- [43] NVIDIA GTX 770, <https://www.nvidia.com/en-us/geforce/graphics-cards/geforce-gtx-770/specifications/>.
- [44] NVIDIA GTX 1080Ti, <https://www.nvidia.com/en-sg/geforce/products/10series/geforce-gtx-1080-ti/>.
- [45] NVIDIA Jetson-TK1 developer kit, <https://developer.nvidia.com/embedded/jetson-tk1-developer-kit>.

# Multi-objective based Optimal Network Reconfiguration using Crow Search Algorithm

Surender Reddy Salkuti

Department of Railroad and Electrical Engineering, Woosong University, Daejeon, South Korea

**Abstract**—This paper presents an optimal network reconfiguration (ONR)/feeder reconfiguration (FRC) approach by considering the total operating cost and system power losses minimizations as objectives. The ONR/FRC is a feasible approach for the enhancement of system performance in distribution systems (DSs). FRC alters the topological structure of feeders by changing the close/open status of the tie and sectionalizing switches in the system. Apart from the power received from the main grid, this paper considers the power from distributed generation (DG) sources such as wind energy generators (WEGs), solar photovoltaic (PV) units, and battery energy storage (BES) units. The proposed multi-objective-based ONR/FRC problem has been solved by using the multi-objective crow search algorithm (MO-CSA). The proposed methodology has been implemented on two (14 bus and 17 bus) distribution systems with three feeders.

**Keywords**—Battery storage; distributed generation; evolutionary algorithms; network reconfiguration; renewable energy; uncertainty

## NOMENCLATURE

$S_{SS}$	Apparent power flowing through the substation transformer
$S_{SS}^{max}$	Maximum apparent power flowing through the substation transformer
$I_f$	Current magnitude of feeder
$I_f^{max}$	Maximum current magnitude of feeder
$v_r$	Rated wind speed
$P_B^{Ch}$	Battery charging power
$P_B^{Disch}$	Battery discharging power
$P_T^{Demand}$	Total power demand in the system
$P_T^{loss}$	Total power losses in the system
$v_{co}$	Cut-out wind speed
$P_W^r$	Rated power of wind turbine (WT)
$P_{PV}^r$	Rated solar PV power output
$G_c$	Certain solar irradiation (say 150 W/m <sup>2</sup> )
$v_{ci}$	Cut-in wind speed
$G_{std}$ (1000	Solar irradiation at standard test environment

	W/m <sup>2</sup> )
$C_i$ grid)	Cost of power from the i <sup>th</sup> feeder (from the main grid)
$P_i$ grid)	Power output from the i <sup>th</sup> feeder (from the main grid)
$C_{Wj}$	Cost of power from the j <sup>th</sup> wind energy generator (WEG)
$P_{Wj}$	Power output from the j <sup>th</sup> WEG
$C_{PVk}$	Cost of power from the k <sup>th</sup> solar PV unit
$P_{PVk}$	Power output from the k <sup>th</sup> solar PV unit
$C_{Bb}$	Cost of power from the b <sup>th</sup> battery storage unit
$P_{Bb}$	Power output from the b <sup>th</sup> battery storage unit
$N_F$	Number of feeders
$N_W$	Number of WEGs
$N_{PV}$	Number of solar PV units
$N_B$	Number of battery storage units
$N_{Bus}$	Number of buses

## I. INTRODUCTION

Generally, the power losses in the distribution network are significantly high compared to those in the transmission system due to the high resistance/reactance (R/X) ratio. Distribution systems (DSs) operate at high currents and low voltages which lead to high power loss and poor voltage profile. Another reason is due to the radial topology of distribution systems when compared to transmission systems [1]. The requirement of enhancing the overall efficiency of power delivery has forced the power utilities to reduce the losses at the distribution level. Many arrangements can be worked out to reduce these losses such as feeder reconfiguration (FRC)/optimal network reconfiguration (ONR), shunt capacitor switchings, etc. The FRC or ONR is the process of changing the topological structure of feeders by varying the positions of tie/sectional (generally open/closed) switches [2]. For a fixed network configuration of a distribution system with varying load conditions, it is observed that the power losses are not optimum. FRC/ONR has several advantages, such as managing network overloading, voltage profile improvement, optimization of system power losses and system operating cost, restoration of service during feeder faults, and system maintenance through

planned outages. Therefore, there is a pressing requirement for the ONR/FRC to optimize system power losses and relieve network overloading. Recently, the electricity demand is rapidly increasing due to population exploitation and urbanization. Conventional electricity generation utilizes fossil fuels. But, the overutilization of fossil fuels causes depletion of fuels and affects the environment [3]. To overcome these issues, this work utilizes renewable energy resources (RERs), such as wind energy generators (WEGs), solar PV units, and battery energy storage (BES) units.

An ONR approach by considering the power loss minimization and improvement of voltage profile has been proposed in [4]. In [5] proposes the ONR approach by optimally allocating distributed generation (DG) and soft open points simultaneously. In [6] proposes an ONR and phase balancing methodology for minimizing the power losses in conventional distribution systems (DSs) and microgrids (MGs) using the particle swarm optimization (PSO) algorithm. Optimal DG allocation and ONR have been presented in [7] to improve the loss profile and voltage stability of the radial distribution systems (RDSs) considering the DGs and probabilistic loads which are operated at varying power factors. An optimal multi-criterion of FRCs with solar PV and wind-based RERs using the weight factor approach considering the reliability has been proposed in [8]. An optimal dispatching and control of all hybrid MG sources such as conventional generators, RERs, demand-manageable loads, and energy storage system have been presented in [9]. In [10] proposes an ONR of DSs under a multi-objective optimization (MOO) model to minimize power losses and to enhance the reliability of DSs. A MOO based on ONR in parallel with renewable DGs allocation and sizing for optimizing the active power loss, annual operation costs (maintenance, installation, and active power loss costs), and emissions have been proposed in [11]. A mixed PSO technique for the minimization of active power loss and the enhancement of voltage profile in the DS has been proposed in [12]. A multiscale formation generation problems are introduced and solved as the generalizations in [13].

From the above literature review, it can be observed that there is a pressing requirement for simultaneously optimizing the total operating cost (TOC) and power loss minimization objectives in the RDS using the ONR/FRC. Optimal FRC alters the feeder topological structure by changing the close/open status of the tie switches and sectionalizing in the system [14, 15]. Apart from the power received from the main grid, this paper considers the power from the DG units such as wind energy generators (WEGs), solar PV units, and battery energy storage (BES) units. The proposed multi-objective-based ONR problem has been solved by using the multi-objective crow search algorithm (MO-CSA). The proposed methodology has been implemented on 14 bus and 17 bus distribution systems.

The paper presented is as follows: Section II explains the mathematical modeling of DG sources, such as wind, solar PV, and battery storage. In section III multi-objective-based problem formulation with system power losses and operating cost objectives has been described. Section IV presents the description of the multi-objective crow search algorithm (MO-

CSA). The performance of the proposed model on 14 bus and 17 bus DSs is presented in the results and discussion in Section V. Section VI concludes the paper.

## II. MODELING OF DISTRIBUTED GENERATION (DG) UNITS

This section presents the modeling of RERs based DG sources, i.e., WEGs, solar PV units, and BES units.

### A. Modeling of Wind Power

In the WEG, the kinetic energy (KE) of wind is going to be converted into electrical power. The power output from a wind turbine ( $P_W$ ) depends on variations in wind speed ( $v$ ), and it can be expressed as [16],

$$P_W = \begin{cases} 0 & \text{if } v \leq v_{ci} \text{ and } v \geq v_{co} \\ av^3 - bP_W^r & \text{if } v_{ci} \leq v < v_r \\ P_W^r & \text{if } v_r \leq v < v_{co} \end{cases} \quad (1)$$

Where  $a = \frac{P_W^r}{v_r^3 - v_{ci}^3}$  and  $b = \frac{v_{ci}^3}{v_r^3 - v_{ci}^3}$ . Generally, the stochastic nature of wind speed ( $v$ ) is modeled using the Weibull probability distribution speed function (PDF). From the knowledge of wind speed distribution, the wind power ( $P_W$ ) is derived and it is depicted in Fig. 1.

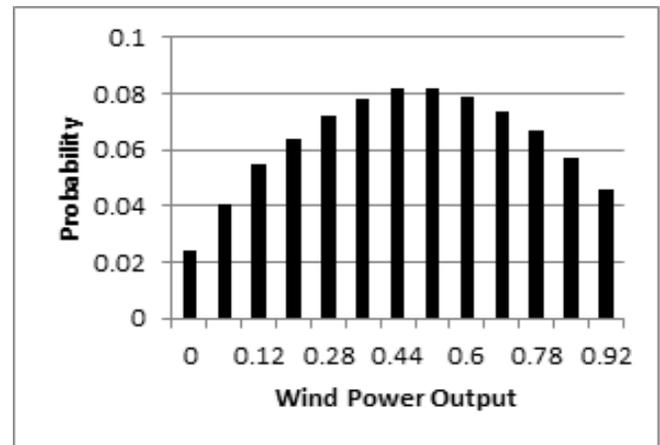


Fig. 1. Wind Power Distribution.

The uncertain nature of wind speed ( $v$ ) can be expressed as [17],

$$f(v) = \left(\frac{k}{c}\right) \left(\frac{v}{c}\right)^{k-1} e^{-\left(\frac{v}{c}\right)^k} \quad \text{for } 0 \leq v \leq \infty \quad (2)$$

The uncertain nature of wind power ( $P_W$ ) using Weibull PDF can be expressed as [17],

$$f(P_W) = \frac{k(v_r - v_{ci})}{c^k P_W} \left( v_{ci} + \frac{P_W}{P_W^r} (v_r - v_{ci}) \right)^k - v_{ci}^{(k-1)} e^{-\left(\frac{v_{ci} + \frac{P_W}{P_W^r} (v_r - v_{ci})}{c}\right)^k} \quad (3)$$

### B. Modeling of Solar PV Power

The amount of power output from solar PV unit ( $P_{PV}$ ) depends on the solar irradiation ( $G$ ), and it can be expressed as [18],

$$P_{PV} = \begin{cases} \frac{G^2 P_{PV}^r}{G_{std} G_c} & \text{for } 0 \leq G < G_c \\ \frac{G P_{PV}^r}{G_{std}} & \text{for } G_c \leq G < G_{std} \\ P_{PV}^r & \text{for } G \geq G_{std} \end{cases} \quad (4)$$

In this paper, the uncertainty modeling of the solar PV unit is modeled by using the Beta distribution function, and its value is in the interval [0, 1]. It is modeled using,

$$f(G) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} G^{\alpha-1} (1-G)^{\beta-1} \quad (5)$$

The parameters  $\alpha$  and  $\beta$  are calculated by using mean ( $\mu$ ) and variance ( $\sigma$ ) of solar irradiance data, and they are calculated using,

$$\beta = (1-\mu) \left[ \frac{\mu(1+\mu)}{\sigma^2} - 1 \right] \quad (6)$$

$$\alpha = \left( \frac{\mu\beta}{1-\mu} \right) \quad (7)$$

### C. Modeling of Battery Energy Storage (BES)

The BES unit provides the flexibility to handle the uncertainty of wind and solar PV units. The operational constraints of battery storage are presented next:

The battery storage power ( $P_B$ ) is limited by [19],

$$-P_B^{max} \leq P_B \leq P_B^{max} \quad (8)$$

Battery power is positive during the charging mode and negative during the discharging mode. The state of charge (SoC) of battery at time  $t$  is expressed as [20],

$$SoC_t = SoC_{t-1} + \left( \frac{P_B}{P_B^{max}} \right) \quad (9)$$

The limit on SoC presents the excessive discharging and charging of the battery, and it can be expressed as,

$$SoC^{min} \leq SoC_t \leq SoC^{max} \quad (10)$$

Where  $SoC^{min}$  and  $SoC^{max}$  are 0.2 and 0.9, respectively.

## III. PROBLEM FORMULATION: MATHEMATICAL MODELING OF ONR/FRC

Optimal network reconfiguration (ONR) is an important tool to operate the distribution system (DS) at a minimum operating cost and/or minimum system power losses and for the enhancement of system security/reliability [21]. The ONR is a complicated problem as they have several candidate switching (both sectional and tie switches) combinations, which makes it a discrete optimization problem [22]. In this work, two important technical objectives, i.e., total operating

cost (TOC) and system power loss minimizations are considered.

### A. Objective 1: Total Operating Cost (TOC) Minimization

The TOC objective includes the cost due to power from the grid (i.e., the power to the feeders), cost due to wind power, solar PV power, and BES units. This TOC objective can be formulated as [23],

Minimize,

$$TOC = \sum_{i=1}^{N_F} (C_i \times P_i) + \sum_{j=1}^{N_W} (C_{Wj} \times P_{Wj}) + \sum_{k=1}^{N_{PV}} (C_{PVk} \times P_{PVk}) + \sum_{b=1}^{N_B} (C_{Bb} \times P_{Bb}) \quad (11)$$

### B. Objective 2: System Power Losses Minimization

Usually, the distribution networks are radial to reduce the protection complexities, and they have a high R/X ratio and hence they have high active power loss [24]. It is very important to reduce the system power losses for increasing the operational efficacy of the system. Fig. 2 depicts the single line diagram (SLD) of the radial distribution system (RDS) with one main feeder and  $N_{BUS}$  number of buses [25]. The formulation of this objective can be formulated next:

The active power losses obtained in the section of line between the bus  $j$  and bus  $(j+1)$ , and can be expressed by [26],

$$P_{(j,j+1)}^{loss} = \left( \frac{P_{(j,j+1)}^2 + Q_{(j,j+1)}^2}{|V_j|^2} \right) R_{(j,j+1)} \quad (12)$$

The reactive power losses obtained in the section of line between the bus  $j$  and bus  $(j+1)$ , and can be expressed by [27],

$$Q_{(j,j+1)}^{loss} = \left( \frac{P_{(j,j+1)}^2 + Q_{(j,j+1)}^2}{|V_j|^2} \right) X_{(j,j+1)} \quad (13)$$

Total active power losses ( $P_T^{loss}$ ) occurred in the RDS can be expressed as [28],

$$P_T^{loss} = \sum_{j=0}^{N_{BUS}-1} \left( \frac{P_{(j,j+1)}^2 + Q_{(j,j+1)}^2}{|V_j|^2} \right) R_{(j,j+1)} \quad (14)$$

The system power loss minimization objective can be formulated as [29],

$$\text{minimize } P_T^{loss} \quad (15)$$

To perform the ONR/FRC problem in DSs, the system needs to satisfy certain equality and inequality constraints. The mathematical representation of those constraints is presented in the following subsection.

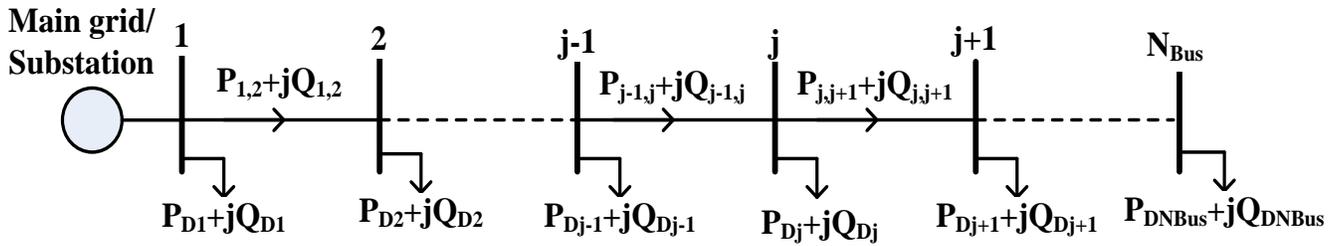


Fig. 2. Single Line Diagram (SLD) of the Radial Distribution System (RDS) with  $N_{Bus}$  Number of Buses.

### C. Constraints

The power balance equation states that the total active power generation from WEGs, solar PV units, power from main grid/substation, and batteries discharging power must be equal to total active power demand, total power losses, and battery charging power [30]. This power flow constraint can be expressed as,

$$\sum_{i=1}^{N_F} P_i + \sum_{j=1}^{N_W} P_{Wj} + \sum_{k=1}^{N_{PV}} P_{PVk} + \sum_{b=1}^{N_B} P_{Bb}^{Disch} = P_T^{Demand} + P_T^{Loss} + \sum_{b=1}^{N_B} P_{Bb}^{Ch} \quad (16)$$

The bus voltage at each bus must be within the minimum and maximum bus voltage limits, and this constraint can be expressed as [31],

$$V_b^{min} \leq V_b \leq V_b^{max} \quad b = 1, 2, 3, \dots, N_{Bus} \quad (17)$$

Power in each feeder is limited by [32],

$$P_i \leq P_i^{max} \quad i = 1, 2, 3, \dots, N_F \quad (18)$$

Power in each WEG is limited by,

$$P_{Wj} \leq P_{Wj}^{max} \quad j = 1, 2, 3, \dots, N_W \quad (19)$$

Power in each solar PV unit is limited by [32],

$$P_{PVk} \leq P_{PVk}^{max} \quad k = 1, 2, 3, \dots, N_{PV} \quad (20)$$

Thermal limits of substation/main grid are limited by [33],

$$S_{ss} \leq S_{ss}^{max} \quad (21)$$

Thermal limits of feeders are limited by,

$$I_f \leq I_f^{max} \quad (22)$$

In this paper, the single objective-based ONR/FRC problem has been solved by using the crow search algorithm (CSA) and the MOO-based ONR/FRC problem has been solved by using the MO-CSA.

### IV. MULTI-OBJECTIVE CROW SEARCH ALGORITHM (MO-CSA)

The crow search algorithm (CSA) is a population-based nature-inspired technique that mimics the crow's behavior and social interaction. Crows live in flock/group and their foods in some hiding places. These intelligent crows memorize these

places and retrieve the hidden foods even after several months. The crows in the flock represent the solution in the population of size  $N$ . The following steps are involved during the implementation of CSA [34].

#### A. Position Initialization

Let  $S_i^t$  represents the position of each crow  $i$  in  $t^{th}$  iteration and it can be expressed as,

$$S_i^t = [S_{i,1}^t, S_{i,2}^t, S_{i,3}^t, \dots, S_{i,n}^t] \quad (23)$$

Where  $n$  is the problem dimension.

#### B. Memory Initialization

Let  $m_i^t$  represents the memory of each crow  $i$  in  $t^{th}$  iteration and it can be expressed as [34],

$$m_i^t = [m_{i,1}^t, m_{i,2}^t, m_{i,3}^t, \dots, m_{i,n}^t] \quad (24)$$

Each solution in the population is evaluated by calculating the fitness by using the objective function/fitness function  $f(S_i^{(t+1)})$ .

#### C. Position Update

Suppose crow  $i$  follows crow  $j$  and the crow  $j$  doesn't watch crow  $i$ , then crow  $i$  will discover food's hiding place of crow  $j$ . In this case, the position of crow  $i$  is updated by using [34],

$$S_i^{t+1} = S_i^t + [r_i fl_i^t (m_j^t - S_i^t)] \quad (25)$$

Where  $S_i^{t+1}$  is the new/updated position of crow  $i$  at  $(t+1)^{th}$  iteration,  $r$  is a random number between 0 and 1, and  $fl_i$  is flight length. Suppose crow  $i$  follows crow  $j$  and the crow  $j$  knows that crow  $i$  is watching it, then crow  $j$  moves randomly to fool crow  $i$ . This process can be expressed by using [35],

$$S_i^{t+1} = \begin{cases} S_i^t + [r_i fl_i^t (m_j^t - S_i^t)] & \text{if } r_j \geq P_c^t \\ \text{A random position} & \text{Otherwise} \end{cases} \quad (26)$$

#### D. Memory Update

Each crow updates its memory based on its fitness value. The fitness of new crow's position (i.e.,  $f(S_i^{(t+1)})$ ) is better than the current memory's value (i.e.,  $f(m_i^t)$ ) then it will update its memory ( $m_i^{t+1}$ ) to  $S_i^{t+1}$ , otherwise, it will not change its memory ( $m_i^{t+1} = m_i^t$ ). This can be expressed as [36],

$$m_i^{t+1} = \begin{cases} S_i^{t+1} & \text{if } f(S_i^{t+1}) > f(m_i^t) \\ m_i^t & \text{Otherwise} \end{cases} \quad (27)$$

For implementing the MO-CSA, an empty external Pareto set is generated with the maximum size of  $\bar{N}$ . In each iteration, the best non-dominated solutions of the current flock are copied to the external Pareto set ( $\bar{N}$ ). If the size of the external Pareto set exceeds  $\bar{N}$ , then use hierarchical clustering

technique to limit the external population size to  $\bar{N}$ . Update the position and memory of the combined population/flock ( $N+\bar{N}$ ) using the equations (26) and (27), respectively. This process is repeated until the termination criteria are satisfied. The members of the Pareto optimal set offer the required Pareto optimal front. The final best-compromised solution is obtained by using the fuzzy-min-max approach. The flow chart of MO-CSA has been depicted in Fig. 3.

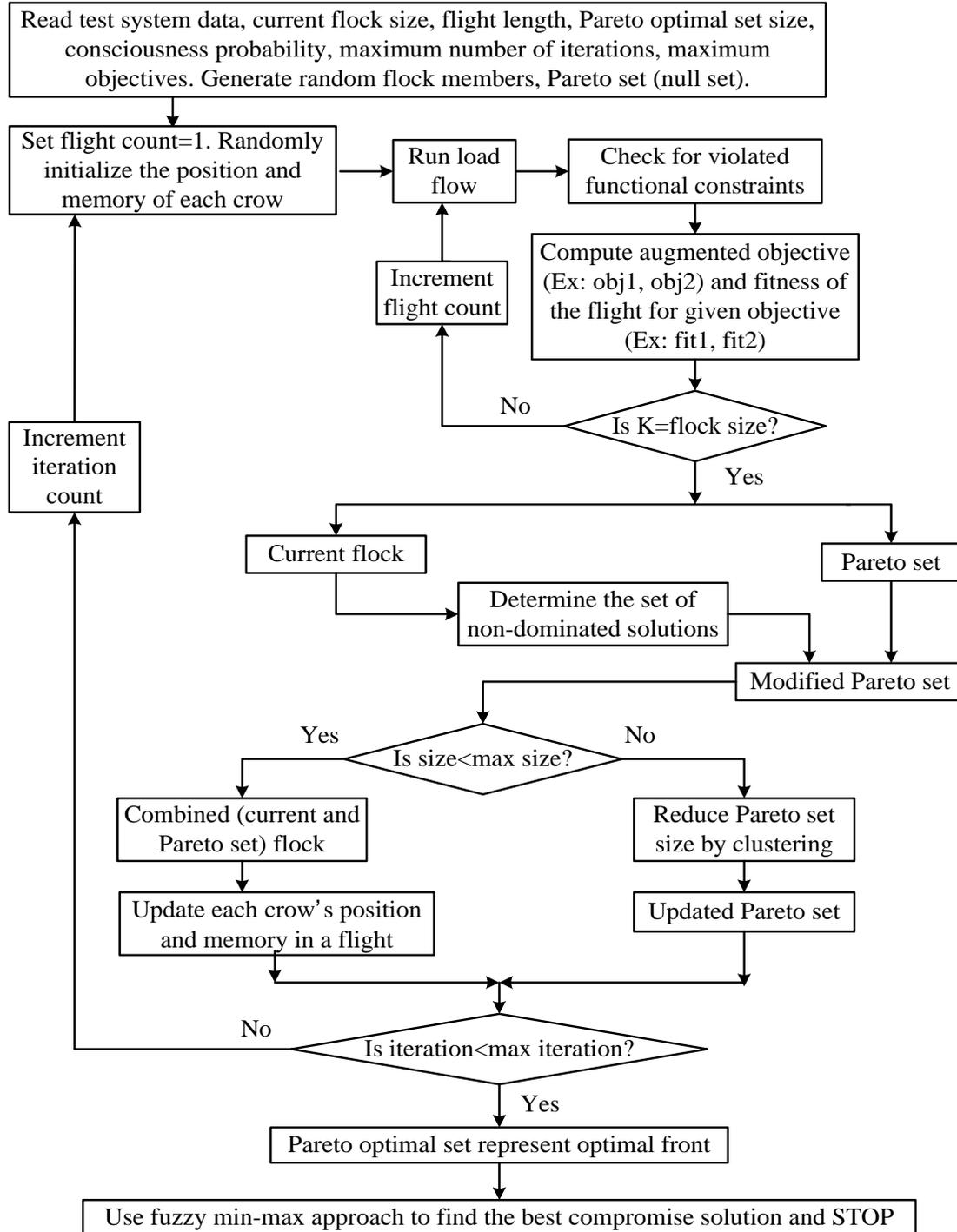


Fig. 3. Flow Chart of MO-CSA.

## V. RESULTS AND DISCUSSION

As mentioned earlier, in this paper the ONR/FRC problem has been implemented on 14 bus and 17 bus DSs. In this work, the single objective-based ONR/FRC problem has been solved using the CSA and the MOO-based ONR/FRC problem has been solved by using MO-CSA. All the optimization programs are codes in MATLAB R2018a software on a personal computer with a 64 bit, 2.5 GHz, Intel Core-i7 processor, and 8 GB RAM. Parameters related to WEG are: cut-in wind speed is 3 m/s, rated wind speed is 12 m/s, cut-out wind speed is 25 m/s, and rated power of WEG is 2 MW. The rated capacities of solar PV units and BES units are 3 MW and 1 MW, respectively.

### A. Simulation Results on 14 Bus Distribution System

The 14 bus distribution system consists of 16 branches, 3 feeders, and 3 tie-switches. The active and reactive power demands are 28.7 MW and 17.3 MVar, respectively. In this test system, one WEG is placed at bus 11, one solar PV unit is placed at bus 6, and one BES unit is placed at bus 12. Fig. 4 depicts the SLD of 14 bus distribution system.

Table I presents the power outputs and objective function values for 14 bus system. When the TOC minimization

objective is optimized independently, then the obtained optimum TOC is 668.23 \$/h and the corresponding power loss is 0.63 MW. When the system power loss minimization objective is optimized independently, then the optimum power loss obtained is 0.45 MW, and the corresponding TOC is 715.01 \$/h. From this analysis, it can be observed that when one objective is optimized independently then the other objective has deviated from the optimum. Therefore, there is a pressing requirement for simultaneously optimizing the TOC and system power losses.

In this paper, the MO-CSA is used for solving the proposed MOO problem. When the TOC and system power loss minimization objectives are optimized simultaneously, then the obtained Pareto optimal front/set has been depicted in Fig. 5. The obtained best-compromised solution using the fuzzy min-max approach has the TOC of 683.50 \$/h and system power losses of 0.50 MW. The opened lines after the ONR/FRC are line 6 (connected between buses 2 and 6), line 9 (connected between buses 3 and 8), and line 10 (connected between buses 8 and 12). Fig. 6 depicts the SLD of 14 bus DS after the ONR/FRC.

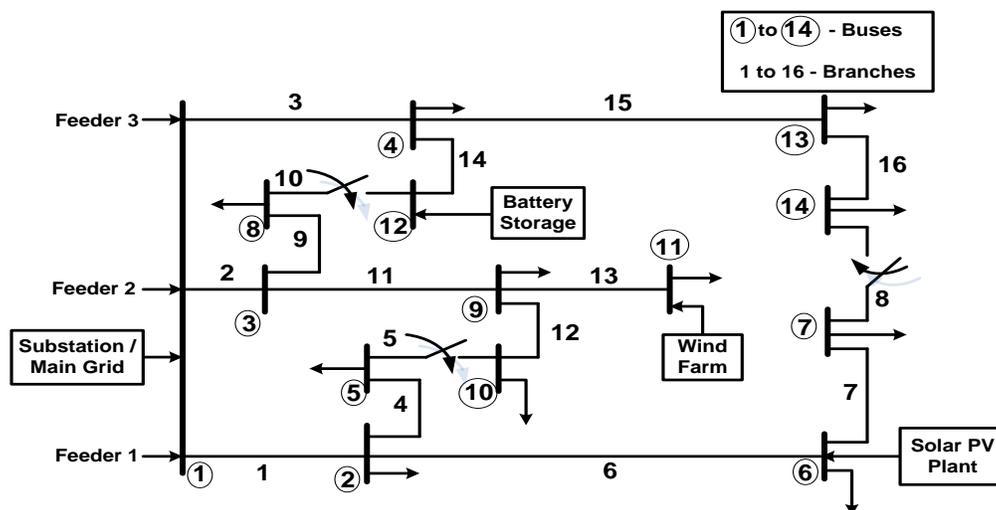


Fig. 4. SLD of 14 Bus Distribution System.

TABLE I. OBJECTIVE FUNCTION VALUES FOR 14 BUS DS

Power outputs and objective function values	Single objective-based ONR		MOO based ONR
	TOC Minimization	Power loss Minimization	TOC and Power loss minimization
Power output from feeders (MW)	24.07	24.35	24.60
Power output from WEGs (MW)	1.92	1.85	1.89
Power output from solar PV unit (MW)	1.79	1.64	1.80
Power output from BES unit (MW)	0.92	0.86	0.91
<b>Total operating cost (TOC) (\$/h)</b>	<b>668.23</b>	715.01	<b>683.50</b>
<b>System power losses (MW)</b>	0.63	<b>0.45</b>	<b>0.50</b>

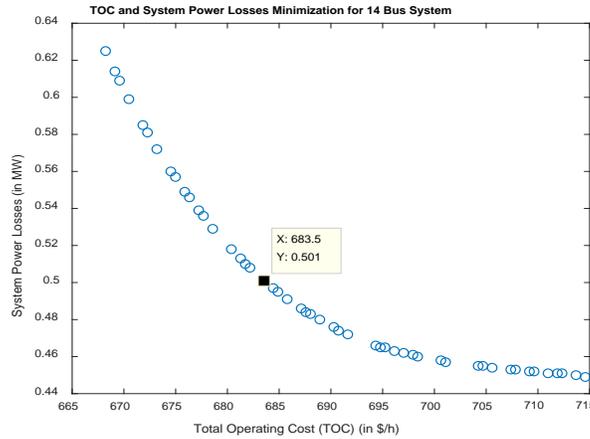


Fig. 5. Pareto Optimal Front of TOC and System Power Losses for 14 bus System.

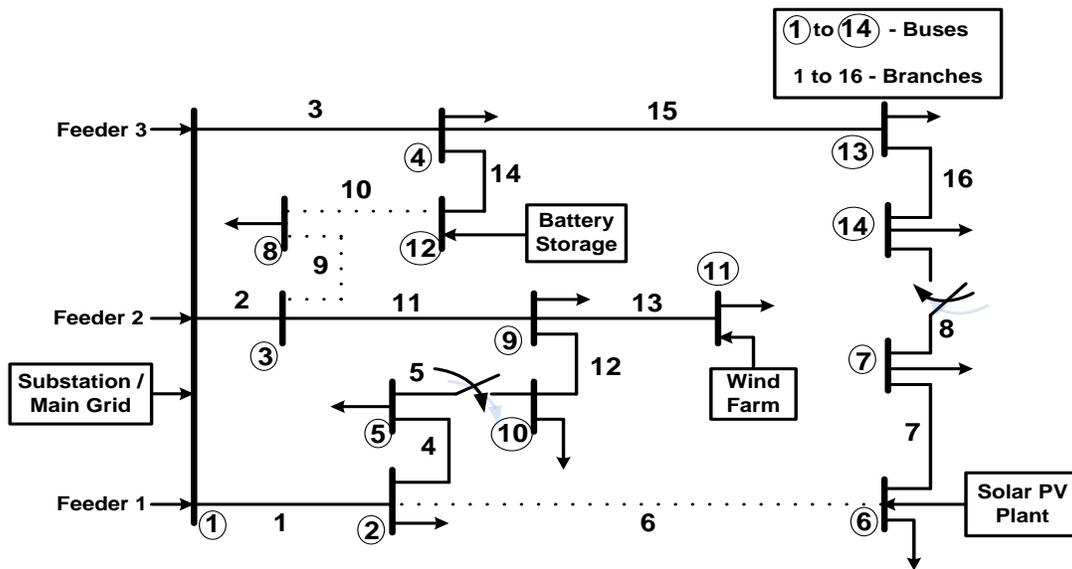


Fig. 6. SLD of 14 Bus DS after Optimal Network Reconfiguration (ONR) / FRC.

**B. Simulation Results on 17 Bus Distribution System**

The 17 bus DS consists of 17 buses, 19 branches, 3 feeders, and 3 tie-switches. Three transformers of rating 115kV/13.2kV of  $\Delta - Y_g$  connection with the leakage impedance of (0.01+j0.05) p.u. are connected at the beginning of 3 feeders. The active and reactive power demands of 17 bus system are 86.10 MW and 51.90 MVAR, respectively. The SLD of 17 bus DS has been depicted in Fig. 7.

Table II presents the power outputs and objective function values for the 17 bus system. When the TOC minimization objective is optimized independently, then the obtained optimum TOC is 1862.06 \$/h and the corresponding power loss is 2.76 MW. When the system power loss minimization objective is optimized independently, then the optimum power loss obtained is 1.95 MW, and the corresponding TOC is

1903.12 \$/h. From this analysis, it can be observed that when one objective is optimized independently then the other objective has deviated from the optimum. Therefore, there is a pressing requirement for simultaneously optimizing the TOC and system power loss objectives.

In this paper, the MO-CSA is used for solving the proposed MOO problem. When the TOC and system power losses are optimized simultaneously, then the obtained Pareto optimal front has been depicted in Fig. 8. The obtained best-compromised solution using the fuzzy min-max approach has the TOC of 1874.02 \$/h and system power losses of 2.26 MW. The opened lines after the ONR/FRC are line 7 (connected between buses 5 and 8), line 9 (connected between buses 5 and 9), and line 12 (connected between buses 6 and 11). Fig. 9 depicts the SLD of 17 bus DS after the ONR/FRC.

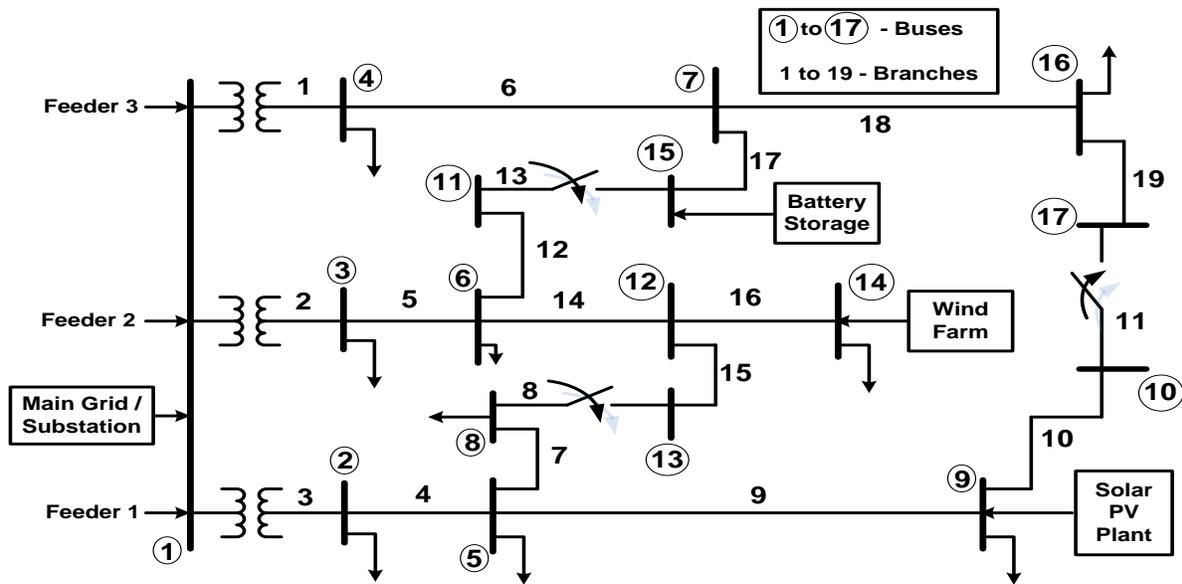


Fig. 7. SLD of 17 Bus Distribution System.

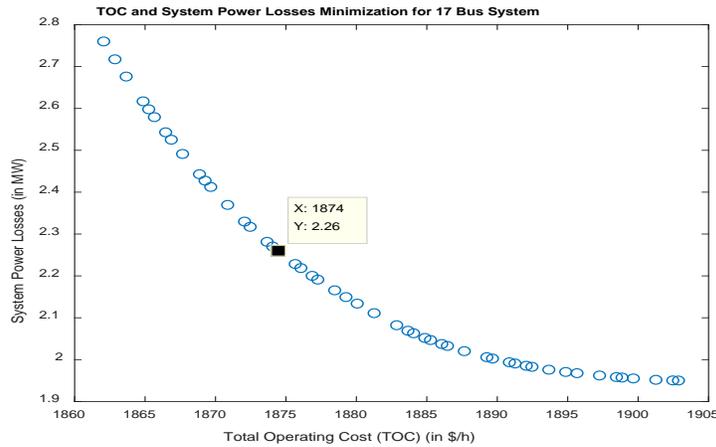


Fig. 8. Pareto Optimal Front / Set of TOC and System Power Losses for 17 Bus System.

TABLE II. OBJECTIVE FUNCTION VALUES FOR 17 BUS DS.

Power outputs and objective function values	Single objective-based ONR		MOO based ONR
	TOC Minimization	Power loss Minimization	TOC and Power loss minimization
Power output from feeders (MW)	82.35	81.87	82.09
Power output from WEGs (MW)	2.82	2.68	2.75
Power output from solar PV unit (MW)	2.74	2.59	2.60
Power output from BES unit (MW)	0.95	0.91	0.92
<b>Total operating cost (TOC) (\$/h)</b>	<b>1862.06</b>	1903.12	<b>1874.02</b>
<b>System power losses (MW)</b>	2.76	<b>1.95</b>	<b>2.26</b>

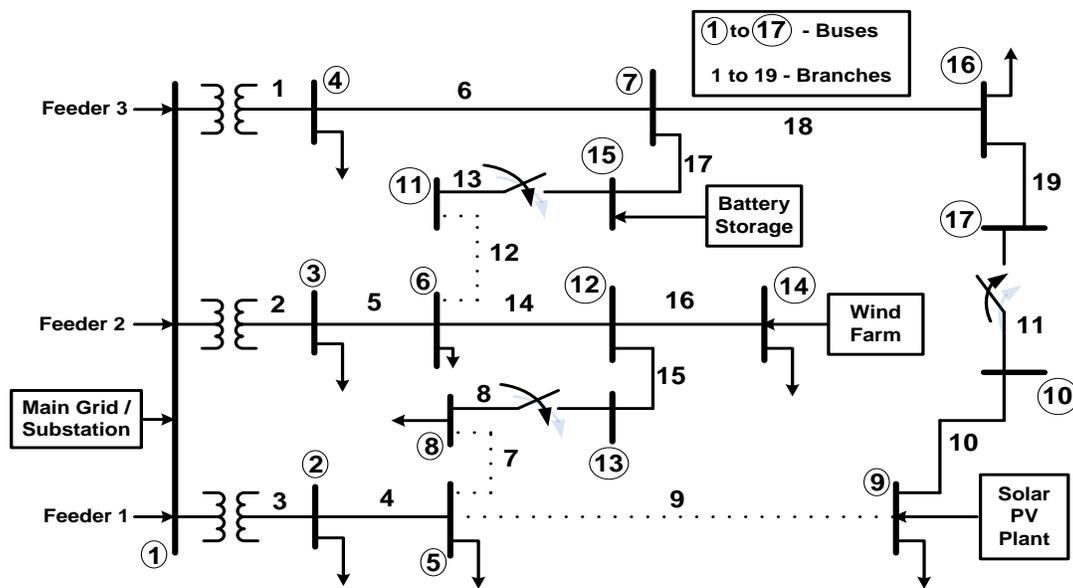


Fig. 9. SLD of 17 Bus Distribution System after ONR / FRC.

## VI. CONCLUSIONS

This paper proposes a multi-objective-based optimal network reconfiguration (ONR)/feeder reconfiguration (FRC) approach considering the multiple energy sources, and it has been solved by using the multi-objective crow search algorithm (MO-CSA). This ONR/FRC approach considers the total operating cost and system power losses minimization as objectives. Apart from the power received from the main grid, this paper considers the power from distributed generation (DG) such as wind energy generators (WEGs), solar PV units, and battery energy storage (BES) units. The stochastic nature of solar PV and wind power generation models is developed using the probabilistic approach in which the uncertainties associated with generation patterns have been modeled using the probability distribution functions. The proposed methodology has been implemented on two test systems, i.e., 14 bus and 17 bus distribution systems with 3 feeders.

## ACKNOWLEDGMENT

This research work was funded by “Woosong University’s Academic Research Funding – 2021”.

## REFERENCES

- [1] S. Naveen, K. Sathish Kumar, K. Rajalakshmi, “Distribution system reconfiguration for loss minimization using modified bacterial foraging optimization algorithm,” *International Journal of Electrical Power & Energy Systems*, vol. 69, pp. 90-97, 2015.
- [2] T.T. The, D.V. Ngoc, N.T. Anh, “Distribution Network Reconfiguration for Power Loss Reduction and Voltage Profile Improvement Using Chaotic Stochastic Fractal Search Algorithm,” *Complexity*, vol. 2020, pp. 1-15, 2020.
- [3] C.T. Su, C.F. Chang, C.S. Lee, “Distribution Network Reconfiguration for Loss Reduction by Hybrid Differential Evolution”, *Electric Power Components and Systems*, vol. 33, no. 12, pp. 1297-1312, 2005.
- [4] A.O. Salau, Y.W. Gebru, D. Bitew, “Optimal network reconfiguration for power loss minimization and voltage profile enhancement in distribution systems,” *Heliyon*, vol. 6, no. 6, 2020.
- [5] I. Diaaeldin, S. Abdel Aleem, A. El-Rafei, A. Abdelaziz, A.F. Zobaa, “Optimal Network Reconfiguration in Active Distribution Networks

with Soft Open Points and Distributed Generation,” *Energies*, vol. 12, 2019.

- [6] W.T. Huang, T.H. Chen, H.T. Chen, J.S. Yang, K.L. Lian, Y.R. Chang, Y.D. Lee, Y.H. Ho, “A Two-stage Optimal Network Reconfiguration Approach for Minimizing Energy Loss of Distribution Networks Using Particle Swarm Optimization Algorithm” *Energies*, vol. 8, pp. 13894-13910, 2015.
- [7] A. Uniyal, S. Sarangi, “Optimal network reconfiguration and DG allocation using adaptive modified whale optimization algorithm considering probabilistic load flow,” *Electric Power Systems Research*, vol. 192, 2021.
- [8] A.J. Nowdeh, M. Babanezhad, S.A. Nowdeh, A. Naderipour, H. Kamyab, Z.A. Malek, V.K. Ramachandaramurthy, “Meta-heuristic matrix moth-flame algorithm for optimal reconfiguration of distribution networks and placement of solar and wind renewable sources considering reliability,” *Environmental Technology & Innovation*, vol. 20, 2020.
- [9] M.I. Pathan, M. Al-Muhaini, S.Z. Djokic, “Optimal reconfiguration and supply restoration of distribution networks with hybrid microgrids,” *Electric Power Systems Research*, vol. 187, 2020.
- [10] M.A.T.G. Jahani, P. Nazarian, A. Safari, M.R. Haghifam, “Multi-objective optimization model for optimal reconfiguration of distribution networks with demand response services,” *Sustainable Cities and Society*, vol. 47, 2019.
- [11] I.B. Hamida, S.B. Salah, F. Msahli, M.F. Mimouni, “Optimal network reconfiguration and renewable DG integration considering time sequence variation in load and DGs,” *Renewable Energy*, vol. 121, pp. 66-80, 2018.
- [12] S. Essallah, A. Khedher, “Optimization of distribution system operation by network reconfiguration and DG integration using MPSO algorithm,” *Renewable Energy Focus*, vol. 34, pp. 37-46, 2020.
- [13] Y. Shang, “Resilient Multiscale Coordination Control against Adversarial Nodes”, *Energies*, vol. 11, no. 7, 2018.
- [14] G. Chicco, A. Mazza, “Assessment of optimal distribution network reconfiguration results using stochastic dominance concepts,” *Sustainable Energy, Grids and Networks*, vol. 9, pp. 75-79, 2017.
- [15] S. Das, D. Das, A. Patra, “Reconfiguration of distribution networks with optimal placement of distributed generations in the presence of remote voltage controlled bus,” *Renewable and Sustainable Energy Reviews*, vol. 73, pp. 772-781, 2017.
- [16] S.S. Reddy, J.A. Momoh, “Realistic and Transparent Optimum Scheduling Strategy for Hybrid Power System”, *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3114-3125, Nov. 2015.

- [17] S.S. Reddy, P.R. Bijwe, A.R. Abhyankar, "Joint Energy and Spinning Reserves Market Clearing for Wind-Thermal Power System Incorporating Wind Generation and Load Forecast Uncertainties", *IEEE Systems Journal*, vol. 9, no. 1, pp. 152-164, Mar. 2015.
- [18] S.S. Reddy, P.R. Bijwe, A.R. Abhyankar, "Real Time Economic Dispatch Considering Renewable Power Generation Variability and Uncertainty Over Scheduling Period", *IEEE Systems Journal*, vol. 9, no. 4, pp. 1440-1451, Dec. 2015.
- [19] S.S. Reddy, P.R. Bijwe, A.R. Abhyankar, "Optimum Day-Ahead Clearing of Energy and reserve Markets with Wind Power Generation using Anticipated Real-Time Adjustment Costs", *International Journal of Electrical Power & Energy Systems*, vol. 71, pp. 242-253, Oct. 2015.
- [20] S.S. Reddy, "Day-ahead thermal and renewable power generation scheduling considering uncertainty", *Renewable Energy*, vol. 131, pp. 956-965, Feb. 2019.
- [21] D. Sudha Rani, N. Subrahmanyam, M. Sydulu, "Multi-Objective Invasive Weed Optimization – An application to optimal network reconfiguration in radial distribution systems," *International Journal of Electrical Power & Energy Systems*, vol. 73, pp. 932-942, 2015.
- [22] V. Rafi, P.K. Dhal, "Maximization savings in distribution networks with optimal location of type-I distributed generator along with reconfiguration using PSO-DA optimization techniques," *Materials Today: Proceedings*, vol. 33, no. 7, pp. 4094-4100, 2020.
- [23] R. Fathi, B. Tousi, S. Galvani, "A new approach for optimal allocation of photovoltaic and wind clean energy resources in distribution networks with reconfiguration considering uncertainty based on info-gap decision theory with risk aversion strategy," *Journal of Cleaner Production*, vol. 295, 2021.
- [24] R. Sanjay, T. Jayabarathi, T. Raghunathan, V. Ramesh, N. Mithulananthan, "Optimal allocation of distributed generation using hybrid grey wolf optimizer," *IEEE Access*, vol. 5, pp. 14807-14818, 2017.
- [25] A.M. Imran, M. Kowsalya, D.P. Kothari, "A novel integration technique for optimal network reconfiguration and distributed generation placement in power distribution networks," *International Journal of Electrical Power & Energy Systems*, vol. 63, pp. 461-472, 2014.
- [26] E. Kianmehr, S. Nikkiah, A. Rabiee, "Multi-objective stochastic model for joint optimal allocation of DG units and network reconfiguration from DG owner's and DisCo's perspectives," *Renewable Energy*, vol. 132, pp. 471-485, 2019.
- [27] A. Tiguercha, A.A. Ladjici, M. Boudour, "Optimal radial distribution network reconfiguration based on multi objective differential evolution algorithm," *IEEE Manchester PowerTech*, Manchester, 2017, pp. 1-6.
- [28] M. Buhari, V. Levi, A. Kapetanaki, "Cable Replacement Considering Optimal Wind Integration and Network Reconfiguration," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5752-5763, Nov. 2018.
- [29] Y. Liu, J. Li, L. Wu, "Coordinated Optimal Network Reconfiguration and Voltage Regulator/DER Control for Unbalanced Distribution Systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2912-2922, May 2019.
- [30] Y. Fu, H. Chiang, "Toward Optimal Multiperiod Network Reconfiguration for Increasing the Hosting Capacity of Distribution Networks," *IEEE Transactions on Power Delivery*, vol. 33, no. 5, pp. 2294-2304, Oct. 2018.
- [31] T. Altun, R. Madani, A.P. Yadav, A. Nasir, A. Davoudi, "Optimal Reconfiguration of DC Networks," *IEEE Transactions on Power Systems*, vol. 35, no. 6, pp. 4272-4284, Nov. 2020.
- [32] M.A. Samman, H. Mokhlis, N.N. Mansor, H. Mohamad, H. Suyono, N.M. Sapari, "Fast Optimal Network Reconfiguration With Guided Initialization Based on a Simplified Network Approach," *IEEE Access*, vol. 8, pp. 11948-11963, 2020.
- [33] C. Yong, X. Kong, Y. Chen, Zhijun E, K. Cui, X. Wang, "Multiobjective Scheduling of an Active Distribution Network Based on Coordinated Optimization of Source Network Load," *Applied Sciences*, vol. 8, 2018.
- [34] A. Askarzadeh, "A novel meta-heuristic method for solving constrained engineering optimization problems: crow search algorithm", *Computers and Structures*, vol. 169, pp. 1-12, 2016.
- [35] P. Díaz, M.P. Cisneros, E. Cuevas, O. Avalos, J. Gálvez, S. Hinojosa, D. Zaldivar, "An Improved Crow Search Algorithm Applied to Energy Problems," *Energies*, vol. 11, 2018.
- [36] A.K. Pandey, S. Kirmani, "Multi-Objective Optimal Location and Sizing of Hybrid Photovoltaic System in Distribution Systems Using Crow Search Algorithm", *International Journal of Renewable Energy Research*, vol. 9, no.4, Dec. 2019.

# Applying Synthetic Minority Over-sampling Technique and Support Vector Machine to Develop a Classifier for Parkinson's disease

Haewon Byeon<sup>1</sup>

Department of Medical Big Data  
College of AI Convergence, Inje University  
Gimhae 50834, Gyeongsangnamdo, South Korea

Byungsoo Kim<sup>2\*</sup>

Department of Statistics  
Inje University, Gimhae 50834  
Gyeongsangnamdo, South Korea

**Abstract**—As the number of Parkinson's disease patients increases in the elderly population, it has become a critical issue to understand the early characteristics of Parkinson's disease and to detect Parkinson's disease as soon as possible during normal aging. This study minimized the imbalance issue by employing Synthetic Minority Over-sampling Technique (SMOTE), developed eight Support Vector Machine (SVM) models for predicting Parkinson's disease using different kernel types {(C-SVM or Nu-SVM)×(Gaussian kernel, linear, polynomial, or sigmoid algorithm)}, and compared the accuracy, sensitivity, and specificity of the developed models. This study evaluated 76 senior citizens with Parkinson's disease (32 males and 44 females) and 285 healthy senior citizens without Parkinson's disease (148 males and 137 females). The analysis results showed that the linear kernel-based Nu-SVM had the highest sensitivity (62.0%), specificity (81.6%), and overall accuracy (71.3%). The major negative relationship factors of the Parkinson's disease prediction model were MMSE-K, Stroop Test, Rey Complex Figure Test (RCFT), verbal memory test, ADL, IADL, 70 years old or older, middle school graduation or below, and women. When the influence of variables was compared using "functional weight", RCFT was identified as the most influential variable in the model for distinguishing Parkinson's disease from healthy elderly. The results of this study implied that developing a prediction model by using linear kernel-based Nu-SVM would be more accurate than other kernel-based SVM models for handling imbalanced disease data.

**Keywords**—Kernel type; Rey complex figure test; support vector machine; SMOTE; Parkinson's disease

## I. INTRODUCTION

As the elderly population increases, the occurrence of senile diseases is also increasing. Among these diseases, Parkinson's disease particularly continues to increase. Health Insurance Review and Assessment Service (2018) [1] reported that the increased rate of Parkinson's disease incidence was the second-highest following that of dementia incidence in South Korea. The number of Parkinson's disease patients increased 2.5 folds over 12 years, from 40,000 in 2004 to 96,000 in 2016, and it reached 100,716 in 2017. As the number of Parkinson's disease patients increases in the elderly population, it has become a critical issue to understand the early characteristics of Parkinson's disease and to detect Parkinson's disease as soon as possible during normal aging.

Motor-symptoms (e.g., resting tremor, rigidity (slowing body movements down) are commonly observed in the early stage of Parkinson's disease [2,3,4]. Over the past 20 years, many studies [5,6,7] have focused on nonmotor-symptoms such as autonomic nervous system dysfunction, dysesthesia, and cognitive impairment, which are observed in the early stages of Parkinson's disease. Shulman et al.(2001)[8] reported that these nonmotor-symptoms were found in 88% of Parkinson's disease patients. Patients with Parkinson's disease do not need any help in performing their daily activities in the early stages [9] because their symptoms can be well controlled with a small amount of medication. However, as Parkinson's disease progresses, since their cognitive and motor functions decline a lot, it becomes difficult to conduct their daily activities and eventually lose the ability to perform them independently [10]. As a result, they must rely on others [10]. In addition, diminished cognitive functions have been reported as a factor causing both the patient and the family to fall into despair and depression along with the gradual decline in Parkinson's disease patients' physical function and uncertainty about the progression of the disease [11,12]. Particularly, nonmotor-symptoms of Parkinson's disease such as cognitive impairment are major predictors for the morbidity of Parkinson's disease dementia [7,13]. Therefore, it is necessary to detect them as soon as possible, which requires to accurately distinguish the cognitive decline in normal aging from that in Parkinson's disease.

Previous studies [14,15,16] that evaluated the difference in cognitive functions between the healthy elderly and Parkinson's disease patients without dementia reported that cognitive issues of Parkinson's disease patients were mainly associated with frontal lobe dysfunction. Cooper et al. (1991) [17] reported that Parkinson's disease patients had difficulty in processing information due to frontal lobe dysfunction and they could show impaired performance or inappropriate behaviors for the situation due to decline concentration. These results imply that the function of the frontal lobe is the key cognitive ability to detect and predict Parkinson's disease [18,19]. Nevertheless, there are not enough large-scale studies on the nonmotor-symptoms of Parkinson's disease in South Korea [13], and efforts to predict Parkinson's disease using machine learning are even scarcer.

\*Corresponding Author

In addition, it is difficult to detect Parkinson's disease in the early stage because abnormal symptoms progress slowly, the nature of a degenerative disease, and it is often hard to tell the onset of a symptom [7]. It is very common that even Parkinson's disease patients do not know exactly when the abnormal symptoms began to occur and they do not recognize a progressing mild cognitive problem [20]. Even if they recognize it, they often think that the symptom is due to aging [20]. Furthermore, it is hard to diagnose Parkinson's disease with only one neurological examination. The diagnosis of Parkinson's disease requires several consecutive measurements regarding the reaction to medications and the progression of the disease. Consequently, it is even harder to detect Parkinson's disease in the early stage.

Many recent studies [21,22,23] have widely used support vector machine (SVM), a supervised learning algorithm, as a way to classify and predict complex risk factors of diseases. When developing a prediction model using binary data like a disease, it is highly likely to encounter an imbalanced issue because the number of patients is smaller than that of people without the disease [24]. The imbalanced issue may cause a prediction error in the process of conducting machine learning and degrade the performance of the model. Consequently, it needs an additional imbalanced data processing technique using sampling in order to resolve the prediction error due to the imbalanced data. Previous studies [25,26] have reported that synthetic minority over-sampling technique (SMOTE) has less overfitting than oversampling or undersampling. This study minimized the imbalance issue by employing SMOTE, developed eight SVM models for predicting Parkinson's disease using different kernel types ((C-SVM or Nu-SVM)×(Gaussian kernel, linear, polynomial, or sigmoid algorithm)), and compared the accuracy, sensitivity, and specificity of the developed models.

## II. METHODS AND MATERIALS

### A. Subjects

This study evaluated 76 senior citizens with Parkinson's disease (32 males and 44 females) and 285 healthy senior citizens without Parkinson's disease (148 males and 137 females) living in Seoul, Incheon, and Gwangju, while a senior citizen was defined as people equal to or older than 60 years and equal to or younger than 74 years. In this study, Parkinson's disease was defined as patients diagnosed with idiopathic Parkinson's disease according to the diagnostic criteria of the United Kingdom Parkinson's Disease Society Brain Bank [27]. The selection criteria for healthy seniors were (1) those who did not have a history of neurological diseases such as stroke and Parkinson's disease, (2) those who received at least 24 points from the Korean version of Mini-Mental State Exam (K-MMSE) and judged as normal, and (3) those who did not have a visual or hearing impairment while taking the test.

The power of this study was examined using G-Power version 3.1.9.7 (Universität Mannheim, Mannheim, Germany). The results showed that, when the number of predictors was 19, alpha=0.05, power (1-B)= 0.95, and the effect size (f2) was 0.15, the required number of samples was 217. Therefore, it

was concluded that the number of this study's samples (n=361) was enough to test statistical significance (Fig. 1 and 2).

### B. Measurements and Definitions of Variables

This study measured the cognitive levels for each subtype using the Cognition Scale for Older Adults (CSOA) [28], which could measure cognitive function comprehensively considering age and education level. The CSOA is a standardized test that can comprehensively measure cognitive function while considering the age and education level of the elderly in South Korea. The CSOA is a survey tool that diagnoses dementia or cognitive disorders by evaluating each cognitive domain (sub-test) targeting the elderly suspected of having dementia or a cognitive disorder. Kim (2011) [29] reported that the reliability of CSOA (Cronbach's alpha) was 0.932. CSOA is composed of eight subtests: Mini-Mental Status Examination in the Korean Version (MMSE-K), Verbal Memory Test, Stroop Test, General Information, Digit Span Test, Rey Complex Figure Test (RCFT), Confrontation Naming Test, and Verbal Fluency Test. This study transformed the raw scores of the eight subtests into standardized scores with a mean of 100 and a standard deviation of 15, and used them to develop prediction models.

MMSE-K: MMSE-K is a test to examine the overall cognitive level and it can evaluate while considering the age and education level of the subject. It is composed of seven sub-domains: orientation of time, orientation of place, memory registration, attention and calculation, memory recall, language function, and composition (construction). Scores range from 0 to 30 points.

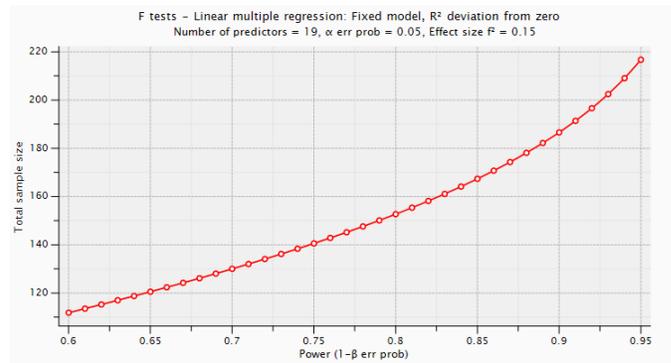


Fig. 1. The Power of this Study.

F tests - Linear multiple regression: Fixed model, R<sup>2</sup> deviation from zero

Analysis: A priori: Compute required sample size

Input:	Effect size f <sup>2</sup>	=	0.15
	α err prob	=	0.05
	Power (1-β err prob)	=	0.95
	Number of predictors	=	19
Output:	Noncentrality parameter e	=	32.5500000
	Critical F	=	1.6395969
	Numerator df	=	19
	Denominator df	=	197
	Total sample size	=	217
	Actual power	=	0.9503271

Fig. 2. Results of Estimating the Appropriate Sample Size to Verify the Statistical Significance Level.

**Verbal Memory Test:** The Verbal Memory Test uses 10 picture cards. The test is performed in the order of immediate recall trial, delayed recall trial, and delayed recognition trial. It evaluates the memory function index comprehensively. Delayed recall trial shall be conducted 15-20 minutes after performing the immediate recall trial. Delayed recognition trial shall be examined immediately after implementing delayed recall trial. The three types of raw scores are calculated: immediate recall, delayed recall, and delayed recognition. The immediate recall trial counts correct responses of each trial, and the total score ranges from 0 to 30 points. The raw score of delayed recall trial is the number of correct responses, and it ranges from 0 to 10 points. The raw score of delayed recognition trial is calculated by subtracting the number of "false positive" (answering "yes" to the picture that was actually shown before) from that of "true positive" (answering "yes" to a picture that was not shown before). If the score is negative, it is treated as 0. The total score ranges from 0 to 10.

**Stroop Test:** It consists of Stroop simple trial and Stroop interference trial. The Stroop simple trial measures the reaction time that takes to state each color of 24 circles. The Stroop interference trial measures the reaction time that takes to state each color of 24 color names. The score is calculated according to the formula based on the raw score of the Stroop simple trial and that of the Stroop interference trial.

**General Information:** It consists of 20 questions asking common sense, and the mark of each question is 1. The total score ranges from 0 to 20 points.

**Digit Span Test:** For this test, when the tester calls out a number, the test subject listens to it and repeats it immediately. There are digit span test-forward and digit span test-backward. Each test starts with an item with a shortlist of numbers and progresses to an item with a longer list of numbers gradually. The raw score of each test is the sum of items, and the total score ranges from 0 to 14 points.

**RCFT:** It is a test that asks a subject to copy Rey complex figure (RCF), and the copied drawing is used as a measure of visuospatial ability. The recalled drawing is used as a measure of memory function. RCF can be divided into 18 elements and each element is scored. Each element is evaluated while considering shape and location, and the raw score ranges from 0 to 36 points.

**Confrontation Naming Test:** It is a question and answer type test. It asks a subject to see a picture and name it. It consists of 24 items. The raw score ranges from 0 to 24 points.

**Verbal Fluency Test:** It consists of two trials. In the first trial, the test subject shall say animal names as many as possible. In the second trial, the test subject shall say crop names as many as possible. The time limit for each trial is 1 minute, and the raw score is calculated by adding summing the number of correct responses in the first trial and that in the second trial.

### C. Explanatory Variable

Explanatory variables were gender (male or female), age, an education level (middle school graduation or below, or high school graduation or above), economic activity (yes or no), mean monthly household income (<1.5 million KRW, 1.5-3 million KRW, and  $\geq 3$  million KRW), living with a spouse (living together, bereavement/separation, or single), smoking (non-smoking or smoking), drinking (non-drinking, or drinking), subjective stress (yes or no), activities of daily living (ADL; total score), instrumental activities of daily living (IADL; total score), MMSE-K, Verbal Memory Test, Stroop Test, general information, digit span test, RCFT, confrontation naming test, and verbal fluency test.

### D. SMOTE

In the Parkinson's disease data used in this study, the proportion of healthy elderly people without Parkinson's disease was 78.9%, and that of those with Parkinson's disease was 21.1%. Consequently, an imbalance issue was found in the class of y variable. Classifiers trained from these skewed data are more likely to produce biased results because they try to predict classes with higher weight. Accuracy may increase due to it. However, it is highly likely that the precision for a low frequency variable becomes lower and the reproduction of the class may decrease as well. This study used SMOTE to overcome the imbalance issue of this binary dataset. SMOTE finds  $n$  nearest neighbors, belong to the same minor class, for any value of a minor class, draws a straight line with that neighbor, and creates random values until they show a synthetic ratio. SMOTE's algorithm is presented in Fig. 3.

```
Algorithm SMOTE( $T, N, k$ )
Input: Number of minority class samples  $T$ ; Amount of SMOTE  $N\%$ ; Number of nearest neighbors  $k$ 
Output:  $(N/100) * T$  synthetic minority class samples
1. (* If  $N$  is less than 100%, randomize the minority class samples as only a random percent of them will be SMOTEd. *)
2. if  $N < 100$ 
3.   then Randomize the  $T$  minority class samples
4.      $T = (N/100) * T$ 
5.      $N = 100$ 
6. endif
7.  $N = (int)(N/100)$  (* The amount of SMOTE is assumed to be in integral multiples of 100. *)
8.  $k =$  Number of nearest neighbors
9.  $numattrs =$  Number of attributes
10.  $Sample[ ] [ ]$ : array for original minority class samples
11.  $newindex$ : keeps a count of number of synthetic samples generated, initialized to 0
12.  $Synthetic[ ] [ ]$ : array for synthetic samples
    (* Compute  $k$  nearest neighbors for each minority class sample only. *)
13. for  $i \leftarrow 1$  to  $T$ 
14.   Compute  $k$  nearest neighbors for  $i$ , and save the indices in the  $nnarray$ 
15.   Populate( $N, i, nnarray$ )
16. endfor

Populate( $N, i, nnarray$ ) (* Function to generate the synthetic samples. *)
17. while  $N \neq 0$ 
18.   Choose a random number between 1 and  $k$ , call it  $nn$ . This step chooses one of the  $k$  nearest neighbors of  $i$ .
19.   for  $attr \leftarrow 1$  to  $numattrs$ 
20.     Compute:  $dif = Sample[nnarray[nn]][attr] - Sample[i][attr]$ 
21.     Compute:  $gap =$  random number between 0 and 1
22.      $Synthetic[newindex][attr] = Sample[i][attr] + gap * dif$ 
23.   endfor
24.    $newindex++$ 
25.    $N = N - 1$ 
26. endwhile
27. return (* End of Populate. *)
End of Pseudo-Code.
```

Fig. 3. Algorithm of Synthetic Minority Over-Sampling Technique.

E. Development of Prediction Model

Models were developed using SVM to predict Parkinson’s disease. SVM is a linear separation model that optimally separates the learning data on hyperplane, and it is a machine learning algorithm that finds the optimal decision boundary [30]. The concept of hyperplane is presented in Fig. 4. Although SVM has higher accuracy and is less likely to cause over-fitting than other models such as decision tree, the prediction performance varies by kernel type [31]. Therefore, this study developed eight SVM models according to the kernel type (C-SVM or Nu-SVM)×(Gaussian kernel, linear, polynomial, or sigmoid algorithm) to identify the SVM model with the best prediction performance and compared their prediction performance (accuracy, sensitivity, and specificity). The concept of kernel function is presented in Fig. 5.

This study randomly divided the data into train data and test data at a ratio of 7:3 to examine the prediction performance of the developed eight SVM models. Moreover, this study calculated overall accuracy, sensitivity, and specificity using the test data. In this study, sensitivity refers to the proportion of true positive, while specificity refers to that of true negative. This study defined the best performance model as the model with the best accuracy, while sensitivity and specificity were 0.6 or higher, by comparing the prediction performance of each model, and the best model was selected as the final model for predicting Parkinson’s disease. All analyses were performed using Python version 3.8.0 (<https://www.python.org>) and R version 4.0.2 (Foundation for Statistical Computing, Vienna, Austria).

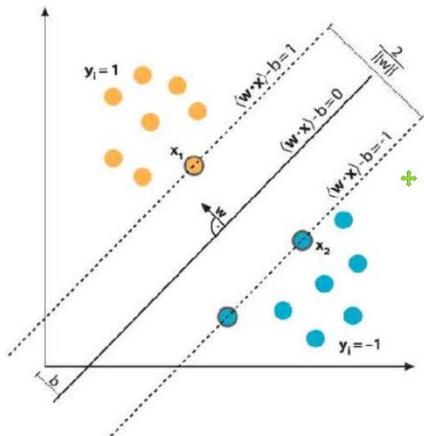


Fig. 4. The Hyperplane in SVM [32].

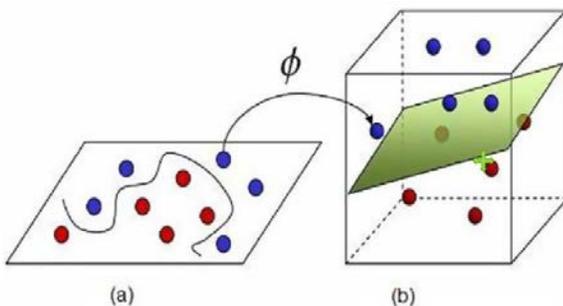


Fig. 5. SVM Kernel Function [33].

III. RESULTS

A. Comparing Daily Living Abilities between the Healthy Group and the Parkinson’s Disease Group

Table I shows the results of descriptive statistics on the cognitive function, ADL, and IADL of the healthy senior citizens and Parkinson’s disease senior citizens.

TABLE I. RESULTS OF DESCRIPTIVE STATISTICS ON THE COGNITIVE FUNCTION, ADL, AND IADL OF THE HEALTHY SENIOR CITIZENS AND PARKINSON’S DISEASE SENIOR CITIZENS (MEAN±SD)

Characteristics	Healthy senior citizens	Parkinson’s disease senior citizens
MMSE-K	113.1±14.5	93.3±25.1
Stroop Test	107.4±14.2	72.5±20.0
Digit Span Test	112.8±15.1	107.1±22.8
General Information	106.6±12.9	101.3±20.7
Verbal Fluency Test	104.6±12.1	98.3±20.1
RCFT	119.6±13.7	97.2±21.1
Verbal Memory Test	118.9±13.6	96.1±20.2
ADL(original score)	7.0±0.0	9.8±3.3
IADL(original score)	10.0±0.0	14.4±4.6

B. Comparing the Accuracy of Parkinson’s Disease Prediction Models according to SVM Classification Algorithm

This study compared the accuracy, sensitivity, and specificity of eight SVMs to confirm the prediction performance of a model by a kernel type (Table II). The analysis results showed that the liner kernel-based Nu-SVM had the highest sensitivity (62.0%), specificity (81.6%), and overall accuracy (71.3%). It was noteworthy that the polynomial-based C-SVM showed the highest specificity (86.5%) among the eight SVM models with the lowest sensitivity (28.8%). The linear kernel-based C-SVM had the lowest overall accuracy (Fig. 6).

TABLE II. THE OVERALL ACCURACY, SENSITIVITY, AND SPECIFICITY OF PARKINSON’S DISEASE PREDICTION MODELS BY SVM KERNEL TYPE

Type of algorithm	Overall accuracy (%)	Sensitivity (%)	Specificity (%)
C-SVM: linear	62.5	56.6	73.3
C-SVM: polynomial	63.0	28.8	86.5
C-SVM: radial basis function	68.5	61.0	70.3
C-SVM: sigmoid	67.0	68.0	61.0
Nu-SVM: linear	71.3	62.0	81.6
Nu-SVM: polynomial	63.5	58.0	73.3
Nu-SVM: radial basis function	65.0	67.0	63.3
Nu-SVM: sigmoid	63.3	61.2	65.7

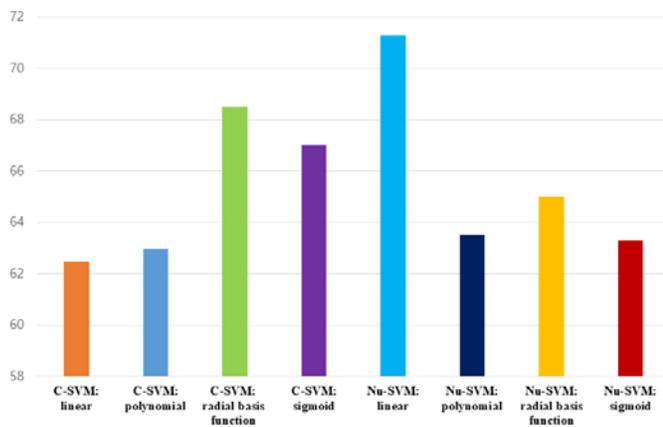


Fig. 6. The Overall Accuracy of Parkinson's Disease Prediction Models by SVM Kernel Type.

### C. Key Variables for the Classification of Parkinson's Disease in the Final SVM Model

This study assumed that the linear kernel-based Nu-SVM algorithm was the best model for predicting Parkinson's disease, which had the highest sensitivity and overall accuracy. This study also calculated the importance of variables in the kernel-based Nu-SVM model, which utilized 83 support vectors. Although it is impossible to simply compare the magnitude of the influence or importance between variables, it is possible to identify whether the relationship between a predictor and an outcome variable is positive or negative. The major negative relationship factors of the Parkinson's disease prediction model were MMSE-K, Stroop Test, RCFT, verbal memory test, ADL, IADL, 70 years old or older, middle school graduation or below, and women. When the influence of variables was compared using "functional weight", RCFT was identified as the most influential variable in the model for distinguishing Parkinson's disease from healthy elderly.

## IV. DISCUSSION

In this study, MMSE-K, Stroop Test, RCFT, verbal memory test, ADL, IADL, 70 years old or older, middle school graduation or below, and women were the main predictors of Parkinson's disease. Among them, RCFT was the most influential variable. It is believed that RCFT was identified as the most important predictor in discriminating Parkinson's disease from the elderly [34] because the task of describing a complex figure requires the function of the frontal lobe in addition to the spatio-temporal composition ability, even though this test reflects spatio-temporal composition ability [35].

Another important finding of this study was that the prediction accuracy of the linear kernel-based Nu-SVM algorithm was the highest when the prediction accuracy of the eight SVM classification algorithms was compared to evaluate the SVM performance by kernel type. The performance of nonlinear SVM is affected by the employed kernel function and the parameters constituting it [36].

## V. CONCLUSION

The results of this study implied that developing a prediction model by using linear kernel-based Nu-SVM would

be more accurate than other kernel-based SVM models for handling imbalanced disease data. Additional studies are needed to compare the accuracy using data from various fields to prove the prediction performance of linear kernel-based Nu-SVM.

## ACKNOWLEDGMENT

This work was supported by a grant from Research year of Inje University in 2018(20180020).

## REFERENCES

- [1] National Health Insurance Statistics, <https://nhiss.nhis.or.kr>. National Health Insurance Statistics, Gangwon.
- [2] K. R. Chaudhuri, L. Yates, and P. Martinez-Martin, The non-motor symptom complex of Parkinson's disease: a comprehensive assessment is essential. *Current Neurology and Neuroscience Reports*, vol. 5, no. 4, pp. 275-283, 2005.
- [3] C. R. Baumann, Epidemiology, diagnosis and differential diagnosis in Parkinson's disease tremor. *Parkinsonism & Related Disorders*, vol. 18, pp. S90-S92, 2012.
- [4] J. M. Marjama-Lyons, and W. C. Koller, Parkinson's disease. Update in diagnosis and symptom management. *Geriatrics (Basel, Switzerland)*, vol. 56, no. 8, pp. 24-5, 29-30, 33-5, 2001.
- [5] K. Seppi, K. Ray Chaudhuri, M. Coelho, and S. H. Fox, R. Katzenschlager, S. Perez Lloret, D. Weintraub, C. Sampaio, and the collaborators of the Parkinson's Disease Update on Non-Motor Symptoms Study Group on behalf of the Movement Disorders Society Evidence-Based Medicine Committee Search for more papers by this author, Update on treatments for nonmotor symptoms of Parkinson's disease—an evidence-based medicine review. *Movement Disorders*, vol. 34, no. 2, pp. 180-198, 2019.
- [6] S. R. Kim, H. Y. So, E. Choi, J. H. Kang, H. Y. Kim, and S. J. Chung, Influencing effect of non-motor symptom clusters on quality of life in Parkinson's disease. *Journal of the Neurological Sciences*, vol. 347, no. 1-2, pp. 310-315, 2014.
- [7] H. Byeon, Development of a depression in Parkinson's disease prediction model using machine learning. *World Journal of Psychiatry*, vol. 10, no. 10, pp. 234-244, 2020.
- [8] L. M. Shulman, R. L. Taback, J. Bean, and W. J. Weiner, Comorbidity of the nonmotor systems of Parkinson's disease. *Movement Disorders*, vol. 16, no. 3, pp. 507-510, 2001.
- [9] P. A. Koplas, H. B. Gans, M. P. Wisely, M. Kuchibhatla, T. M. Cutson, D. T. Gold, C. T. Taylor, and M. Schenkman, Quality of life and Parkinson's disease. *Journal of Gerontology*, vol. 54, no. 4, pp. M197-M202, 1999.
- [10] D. A. Cahn, E. V. Sullivan, P. K. Shear, A. Pfefferbaum, G. Heit, and G. Silverberg, Differential contributions of cognitive and motor component processes to physical and instrumental activities of daily living in Parkinson's disease. *Archives of Clinical Neuropsychology*, vol. 13, no. 7, pp. 575-583, 1998.
- [11] K. Y. Sohng, J. S. Moon, K. S. Lee, and D. W. Choi, The development and effects of a self-management program for patients with Parkinson's disease. *Journal of Korean Academy of Nursing*, vol. 37, no. 6, pp. 891-901, 2007.
- [12] A. J. Jones, R. G. Kuijer, L. Livingston, D. Myall, K. Horne, M. MacAskill, T. Pitcher, P. T. Barrett, T. J. Anderson, and J. C. Dalrymple-Alford, Caregiver burden is increased in Parkinson's disease with mild cognitive impairment (PD-MCI). *Translational Neurodegeneration*, vol. 6, no. 1, pp. 17, 2017.
- [13] H. Byeon, Best early-onset Parkinson dementia predictor using ensemble learning among Parkinson's symptoms, rapid eye movement sleep disorder, and neuropsychological profile. *World Journal of Psychiatry*, vol. 10, no. 11, pp. 245-259, 2020.
- [14] I. Daum, M. M. Schugens, S. Spieker, U. Poser, P. W. Schonle, and N. Birbaumer, Memory and skill acquisition in Parkinson's disease and frontal lobe dysfunction. *Cortex*, vol. 31, no. 3, pp. 413-432, 1995.
- [15] A. J. Lee, and E. Smith, Cognitive deficits in the early stages of Parkinson's disease. *Brain*, vol. 106, no. 2, pp. 257-270, 1983.

- [16] A. E. Taylor, J. A. Saint-Cyr, and A. E. Lang, Frontal lobe dysfunction in Parkinson's disease. The cortical focus of neostriatal outflow. *Brain*, vol. 109, no. 5, pp. 845-883, 1986.
- [17] J. A. Cooper, H. J. Sagar, N. Jordan, N. S. Harvey, and E. V. Sullivan, Cognitive impairment in early, untreated Parkinson's disease and its relationship to motor disability. *Brain*, vol. 114, no. 5, pp. 2095-2122, 1991.
- [18] A. McKinlay, R. C. Grace, J. C. Dalrymple-Alford, and D. Roger, Characteristics of executive function impairment in Parkinson's disease patients without dementia. *Journal of the International Neuropsychological Society : JINS*, vol. 16, no. 2, pp. 268-277, 2010.
- [19] D. Weintraub, P. J. Moberg, W. C. Culbertson, J. E. Duda, I. R. Katz, and M. B. Stern, Dimensions of executive function in Parkinson's disease. *Dementia and Geriatric Cognitive Disorders*, vol. 20, no. 2-3, pp. 140-144, 2005.
- [20] A. Elbaz, and F. Moisan, Update in the epidemiology of Parkinson's disease. *Current Opinion in Neurology*, vol. 21, no. 4, pp. 454-460, 2008.
- [21] S. Lahmiri, and A. Shmuel, Detection of Parkinson's disease based on voice patterns ranking and optimized support vector machine. *Biomedical Signal Processing and Control*, vol. 49, pp. 427-433, 2019.
- [22] S. Haller, S. Badoud, D. Nguyen, V. Garibotto, K. O. Lovblad, and P. R. Burkhard, Individual detection of patients with Parkinson disease using support vector machine analysis of diffusion tensor imaging data: initial results. *American Journal of Neuroradiology*, vol. 33, no. 11, pp. 2123-2128, 2012.
- [23] H. Byeon, Predicting the swallow-related quality of life of the elderly living in a local community using support vector machine. *International Journal of Environmental Research and Public Health*, vol. 16, no. 21, pp. 4269, 2019.
- [24] C. Jian, J. Gao, and Y. Ao, A new sampling method for classifying imbalanced data based on support vector machine ensemble. *Neurocomputing*, vol. 193, pp. 115-122, 2016.
- [25] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, SMOTE: synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, vol. 16, pp. 321-357, 2002.
- [26] D. Elreedy, and A. F. Atiya, A comprehensive analysis of synthetic minority oversampling technique (SMOTE) for handling class imbalance. *Information Sciences*, vol. 505, pp. 32-64, 2019.
- [27] A. J. Hughes, S. E. Daniel, L. Kilford, and A. J. Lees, Accuracy of clinical diagnosis of idiopathic Parkinson's disease: a clinicopathological study of 100 cases. *Journal of Neurology, Neurosurgery and Psychiatry*, vol. 55, no. 3, pp. 181-184, 1992.
- [28] H. K. Kim, and T. Y. Kim, *Cognition Scale for Older Adults; CSOA: manual*. Neuropsych Inc, Daegu, 2007.
- [29] Y. S. Kim, Diabetes and cognitive function in community-dwelling older adults. *Journal of Korean Academy of Community Health Nursing*, vol. 22, no. 4, pp. 377-388, 2011.
- [30] S. Cuentas, R. Peñabaena-Niebles, and E. Garcia, Support vector machine in statistical process monitoring: a methodological and analytical review. *The International Journal of Advanced Manufacturing Technology*, vol. 91, no. 1-4, pp. 485-500, 2017.
- [31] T. S. Furey, N. Cristianini, N. Duffy, D. W. Bednarski, M. Schummer, and D. Haussler, Support vector machine classification and validation of cancer tissue samples using microarray expression data. *Bioinformatics*, vol. 16, no. 10, pp. 906-914, 2000.
- [32] S. Yu, P. Li, H. Lin, E. Rohani, G. Choi, B. Shao, and Q. Wang, Support vector machine based detection of drowsiness using minimum EEG features. In *2013 International Conference on Social Computing*, pp. 827-835, 2013.
- [33] N. J. Nalini, and S. Palanivel, Music emotion recognition: The combined evidence of MFCC and residual phase. *Egyptian Informatics Journal*, vol. 17, no. 1, pp. 1-10, 2016.
- [34] K. W. Walsh, *Understanding brain damage: A primer of neuropsychological evolution*. Churchill Livingstone, New York, 1991.
- [35] A. Kudlicka, L. Clare, and J. V. Hindle, Executive functions in Parkinson's disease: systematic review and meta-analysis. *Movement Disorders*, vol. 26, no. 13, pp. 2305-2315, 2011.
- [36] I. Steinwart, and A. Christmann, *Support vector machines*. Springer Science & Business Media, New York, 2008.

# FishDeTec: A Fish Identification Application using Image Recognition Approach

Siti Nurulain Mohd Rum<sup>1</sup>, Fariz Az Zuhri Nawawi<sup>2</sup>

Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia, Serdang, Selangor, Malaysia

**Abstract**—The underwater imagery processing is always in high demand, especially the fish species identification. This activity is as important not only for the biologist, scientist, and fisherman, but it is also important for the education purpose. It has been reported that there are more than 200 species of freshwater fish in Malaysia. Many attempts have been made to develop the fish recognition and classification via image processing approach, however, most of the existing work are developed for the saltwater fish species identification and used for a specific group of users. This research work focuses on the development of a prototype system named FishDeTec to detect the freshwater fish species found in Malaysia through the image processing approach. In this study, the proposed predictive model of the FishDeTec is developed using the VGG16, is a deep Convolutional Neural Network (CNN) model for a large-scale image classification processing. The experimental study indicates that our proposed model is a promising result.

**Keywords**—Component; Freshwater Fish; fish species recognition; FishDeTec; Convolutional Neural Network (CNN); VGG16

## I. INTRODUCTION

Rivers, ponds, and lakes are full of intrigue and mystery, and the interesting topic has always been the underwater discovery. Estimating the quantity of fish and its presence from image sources may help biologists to understand the underwater habitats and natural environment to aid preservation. There are more than 30,000 species of fish worldwide [1] and it is almost impossible to identify each one by just simply looks at their physical outlook as most of them have similar shapes. There are cases where people die due to the lack of information to differentiate between the non-poison and poison fish and it is happening every day [1-3]. In recent years, image recognition and classification techniques have attracted many scientists to improve the scientific field. It would be time consuming and tedious job for human to analyse and process the massive data generated by the underwater images. In fishery education, minimizing human error during the fish observation and analysis process is important and requires an automatic system detection. Image classification is the process of taking inputs such as images and producing output type categories or probabilities for a particular class. Studies in fish image recognition are as significant area, especially in the marine biology and aquaculture. Fish in general, having a skull and spine, usually breathe through the gills attached to the skin. They have a slender body shape suitable for swimming and fins to make them move faster through the water. The fish category can be

categorized into two types, namely saltwater fish, and freshwater fish. When comparing saltwater with freshwater fish, there are differences between these two types of fish in terms of its physiology, structural adaptation, and size. The freshwater fish is able to survive in a variety of habitats. There are some species can live in mild temperatures at 24 degrees Celsius, while others can survive at very low temperatures, between 5 to 15 degrees Celsius. Freshwater fish can be found in lakes, wetlands, and shallow rivers, where the water salinity is less than 0.05 percent. Saltwater fish can be found in a diversity of habitats, ranging from cold Antarctica and the Arctic Ocean to the warm tropical oceans. The most suitable habitats for saltwater fish include coral reefs, mangroves, salt ponds, deep sea and seagrass beds, and a number of fish thrive in each of these conditions. The size of freshwater fish can be from the small Filipino gobies which is less than an inch in size to the white sturgeon that weighing about 400 pounds, are one of the world's biggest freshwater fish. Freshwater fish include catfish, cisco, charr, gar, mooneye, shiner, trout (blueback, apache, brook, cutthroat and brown), sunfish, pike, whitefish and Salmon [4]. Fig. 1 is some freshwater fish species available in Malaysia. Saltwater fish include certain types of bass, albacore, common dolphin, butterfly, bluefish, eels, flounder, mackerel, cod, herring, marlin, shark, yellowtail, tuna, and snapper [5]. Many studies have been made to detect the fish images especially in saltwater habitat such as [6-8]. Several attempts have been made to recognise the visual images, but it is still an unsolved problem due to segmentation errors, distortion and occlusion and overlap of objects in coloured images [9, 10]. The problem of object classification lies in the main challenge of estimating the prevalence of each species of fish. Solutions to automatically detect the fish classification should be able to overcome problems related to fish size and orientation, feature variability, picture quality and segmentation.

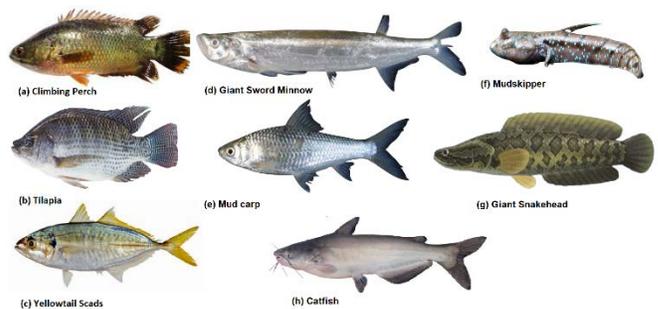


Fig. 1. Some of Freshwater Fish Species available in Malaysia.

Although progress has been made in the field of data generated in real time as well as the improvement of long-distance resolution, the existing works are still limited in their ability to detect or classify the freshwater fish, especially the species found in Malaysia. In other words, a work that specifically provide the identification of Malaysia freshwater fish species through the image processing could not be located. Motivated by this factor, the main objective of this study is to propose the development of a mobile application named FishDeTec to identify and classify the image of freshwater fish species found in Malaysia. In the next sections, we discussed the existing works done by others and followed by the entire processes required for the development of the proposed system.

## II. RELATED WORK

The Convolutional Neural Network (CNN) is a multi-layered/deep neural network designed to detect visual patterns using minimal pre-processing image's pixel. CNN is a unique neural network architecture and consist of two major components, namely convolutional and pooling layers. It can be used to capture the image vision in near-infinite ways. There are number of CNN architectures, which are the key to build algorithms to control and power AI as a whole in the near future. Some of them are LeNet [11], VGGNet [12], AlexNet [13], ZFNet [14], ResNet [15] and GoogLeNet [16]. The VGG16 also known as OxfordNet presented in Fig. 2, is the architecture of CNN is named after the Oxford Visual Geometry Group, which created it. It was used in 2014 to win the ImageNet Large Scale Visual Recognition Challenge (ILSVR) competition (ImageNet).

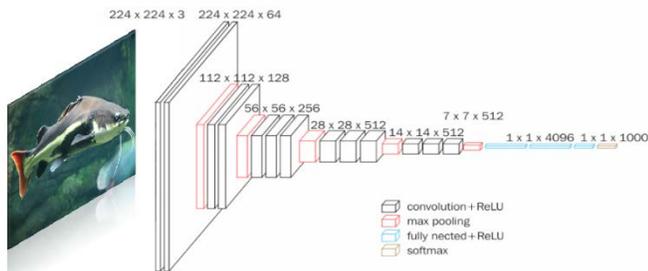


Fig. 2. The Architecture of VGG16.

The VGG16 is a CNN model developed by Karen Simonyan and Andrew Zisserman from the Oxford University [12]. This model has reached the accuracy at 92.7% and is ranked in the top 5 in ImageNet's, which is a data set that has more than 14 million images from 1000 classes. It was one of the popular models submitted to ILSVRC-2014. The improvisation was made by replacing the large size of kernel filters for the first and second convection layer, respectively with 3 x 3 filters to improve the AlexNet [13] model. The VGG16 has been trained for weeks and used the GPU of NVIDIA Titan Black. The differences architectures of VGG16 and AlexNet is presented in Fig. 3. The main reason why VGG16 is a preferred CNN method over the AlexNet CNN in this study is because it supports the processing for a large-scale data set with a deeper network layers and smaller filter to produce a better performance. The VGG16 itself is the improvement of Alex Net. In addition, the

complexity for detecting the fish species from images required an effective modelling approach as most of them have similar shapes and features. The VGG16 has been widely used for Transfer Learning (TL) because of its performance. The main purpose of TL is to transfer the knowledge obtained from the source domain from the large dataset to the target domain, which is a smaller dataset. This is a good criterion for the underwater image's classification specifically the fish recognition. Today, there are several attempts have been made specifically for the development of the fish image recognition model using Machine Learning (ML) and Deep Learning (DL) approaches. The work by Puspa Eosina et al. [17] for example, presents the Sobel's method for detecting and classifying freshwater fish in Indonesia. They used 200 numbers of freshwater images from 10 difference species to evaluate their model. However, to enhance the accuracy of the model, additional techniques are still needed such as texture or colour and retrieval of content-based technique. A study by [18] proposed a DL technique combined the Dense Neural Network (DNN) and Spatial Pyramid Pooling (SPP) by putting the SPP in front of the DenseNet layer.

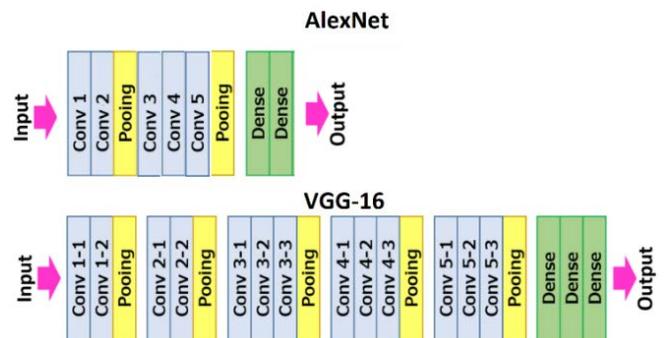


Fig. 3. The Difference Architecture between AlexNet and VGG16 Models.

They proposed a method to remove the noise in the dataset before the training step taken into action through the image processing implementation. This can eliminate the underwater obstacles, dirt, and non-fish bodies from the images. They use the DL approach by implementing the CNN model for the fish species classification. They also provide in their article the description of the performance of the different activation functions with the comparison of ReLU, SoftMax, and tanh and the activation function of the ReLU was found to be exceptionally precise. The authors in [6] propose a method for automated classification of fauna images using the CNN on Animal-10 dataset, with the accuracy at 91.84%. They discuss the implementation of the VGG16 architecture of CNN and the activation role of Leaky ReLU in image classification. The neural network learned to categorize the animal's image. The proposed classification of fauna images using a CNN can be widely used for the classification of fauna images, which would enable the ecologists and researchers to further analyze to preserve the environment and habitats. They used six different species of freshwater fish to test the model. The work by [19] demonstrates 96.29% accuracy for the automatic classification of aquatic fish species relative to traditional approaches. They emphasize on the image of the fish outside of the water, this is to get minimal background noises of the image such as distortion, occlusion, and image quality. The

FishApp [20] is a cloud based application for fish species recognition. It consists of a smartphone application designed for the Android and iOS mobile operating systems that allows the user to take and send photographs of a whole fish for remote inspection and a remote cloud-based computing system that incorporates a sophisticated image processing pipeline and a DL neural network to interpret images and identify them into predefined fish classes. The DeepFish [21] is a framework developed to classify fish from photographs collected in the marine observation network installed underwater cameras. In their work, they used the low rank matrices and sparse to extract the foreground. The deep neural network is used to extract the image of fish. The principal component analysis known as PCA is used in this architecture specifically in two layers of convolutional and block wise histograms in pooling layer and in a non-linear layer, it used binary hashing. They used the linear SVM for the classification and achieved the accuracy at 98.64%. Apart from the scholarly work, there are also a number of mobile applications available for fish identification such as FishVerify [22] and FishID+ [23]. The FishVerify for example, is a mobile application developed to help the local community in Florida, to identify fish. The users are provided with the instance identification of fish from live scan or photo as well the fishing rules and regulation in Florida. The FishID+ application has the same purpose as FishVerify, however the main target user is the fish collector. It uses the DL to verify the freshwater fish, aquarium fish and focuses only on the small fish. The database contains of more than 240 numbers of species of fish, including cichlids, clownfish, tetras, tangs and many other common aquarium fish. Based on our study, a specific mobile application developed for recognizing freshwater fish in Malaysia could not be located. Motivated by this factor, this study presents the development of FishDeTec, utilizing the Convolutional Neural Network (CNN) for the model development in identifying Malaysia freshwater fish.

### III. METHODOLOGY

In this section, we describe in detail the methodology used to develop the proposed system. The designed methodology is suitable for executing this research work as it supports the TL as introduced in VGG16, in which the knowledge gained from the pre-trained model can be used to improve the generalization about another task. The technologies used to realize this research work is, Python for the programming language, Google Colab as the editing and compiling tool for Python. The TensorFlow Mobile is an open-source library used to perform the image recognition task that can be easily embedded in Android Studio application through the library. The Android Studio is the platform used to develop the android mobile application. While the Firebase database is used to store all the information about the fish as well as the images. The VGG16 is the CNN used for the fish image recognition. This technique is preferred method as it is a network trained on more than a million images from the ImageNet database. Fig. 4 is the steps required for the execution of this study. It is starts with the requirement analysis. During this stage, the limitation of existing work is analyzed from the literature review. Based on the analysis, it

can be concluded that most of the existing models were developed to recognize the saltwater fish, therefore this study is focusing on the development of fish specifically the Malaysia's freshwater fish. The next step is data set preparation and pre-processing. Usually, the process of acquiring data is messy where it comes from different sources. At this stage, images of several freshwater fish species of are collected. Most images used today is 24 bit or higher. The 8-bit gray scale image consists of black and white, and each pixel has a value ranging from 0 to 255. The RGB color picture indicates that the pixel color is a blend of red, green, and blue. The colors vary from 0 to 255 each. This generator of RGB colors demonstrates how RGB can produce any color. A pixel, then, comprises a range of the three RGB values (102, 255, 102) that correspond to color #66ff66. Images with a size of 0.48 megapixels consist of 800 pixels wide and 600 pixels high. However, the VGG16 was originally trained on 224 x 224 size of images.

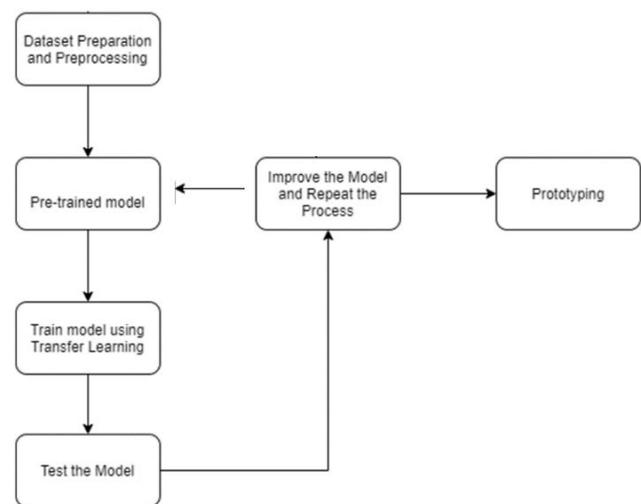


Fig. 4. The Methodology for the Development of FishDeTec.

To feed all images into a neural network model, it requires the cleaning process, standardization, and data augmentation. It is not practical to come up with a specific algorithm to suit different conditions, therefore all images are converted into the form that allows a common algorithm to fix it. A general pre-processing method (e.g., reflection, rotation, histogram, Gaussian blurring, equalization, and translation) requiring the enhancement of current datasets of perturbed copies of existing images is called data augmentation. This task is carried out to enlarge the data set and to expose the neural network to the wide range of image variations. This allows the model to recognize the object when it appears in any shape and form. The data is split into training data and testing data. The total number of images used in this study is 200 for eight type of fish species. The dataset distribution is illustrated in Table I.

The purpose of the ImageDataGenerator is to conveniently import label data into the model. It provides many functions, such as rescale, flip, zoom, rotate etc. The best part of this class is that the data contained on the disk are not affected. This class converts data on the go while feed it to the model.

The next step is to pre-trained the model using the VGG16 neural network. During this stage, the Tensorflow and Keras are used to develop the model. Since we deployed the script using the cloud infrastructure (Google Colab), the memory performance is not an issue. Most of the coding is based on the Keras only, which at the back end uses the TensorFlow. The next step is to train the developed model using TL. The TL is a well-known approach in computer vision as it enables the model accuracy development in a time-saving way[24]. The TL is not a new concept which is very specific in the DL. There is a significant difference between the traditional approach of learning model and ML and using methodologies that adapt the TL principles. In traditional ML, the knowledge is not retained, whereby in TL, learning the new tasks relied on the previous learned tasks. During this step, we do not train all layers of the model. We just freeze all the layers and train the lower layer of the model, which is using the weight of the trained model and this makes retraining very easy. The process is repeated to improve the model. Once, it has achieved the desire target of accuracy, the model is then embedded into the android mobile application development using Java. We have also added the information about the fish species in the Firebase database such as the scientific name, the name of the fish in Malay, etc. Table II is the technologies used to develop the whole system.

TABLE I. THE DISTRIBUTION OF DATASET

Fish	Number of Images in the training set
Climbing Perch	20
Catfish	25
Tilapia	20
Yellowtail Scads	25
Giant Snakehead	25
Giant Sword Minnow	18
Mud carp	25
Mudskipper	20

TABLE II. TECHNOLOGIES USED TO DEVELOP FISHDeTEC

Technology used	Description
Python	The programming language used to develop the fish identification model.
Java	The programming language used to develop the android application
TensorFlow Mobile	The open source library used for the DL purpose.
Keras	The API for the DL used for Python
VGG16	The type of CNN used to detect the fish image species.
Google Colab	The development environment for Python that runs in the browser using Google Cloud.
Android Studio	The integrated development environment for Android operating system.
Firebase Database	The cloud hosted database used to store the information about the fish.

#### IV. RESULT AND DISCUSSION

In this section, we present the performance accuracy of the proposed model. Accuracy is a mechanism for calculating the efficiency of a classification model. Typically, it is presented as a percentage. Accuracy is the value of prediction of which it is equal to the real value and easier to interpret. It is often depicted in graphed to represent the accuracy of a developed model. Whereby a loss function is a prediction value for how much it is varying from true value. It is not represented in percentage; it is the errors sum made for each sample in validation set. The entropy loss and log loss are the most common function for loss. The loss function can be used in regression and classification problems. Fig. 5 is the graph that show the performance of four parameters, namely the accuracy, validation accuracy, loss, and validation loss based on the developed model. When training a model, the accuracy and loss for validation data in the model usually will vary in different situations. Usually, errors should be smaller for each epoch increasing, and accuracy should be greater. Three cases can possibly happen, for the first case, if the loss parameter is start increasing and the accuracy is decreasing, this indicate that the model is not learning. For the second case, if the loss parameters start increasing as well as the accuracy parameter, this may be the cause of diverse probability values or overfitting in cases where softmax is being used in output layer. For third case, if the loss parameter is starts decreasing, the accuracy parameter is starts increasing, this indicate that the built model is learning and working fine. It is clearly showing that in Fig. 5, the proposed model is categorized under the third case.

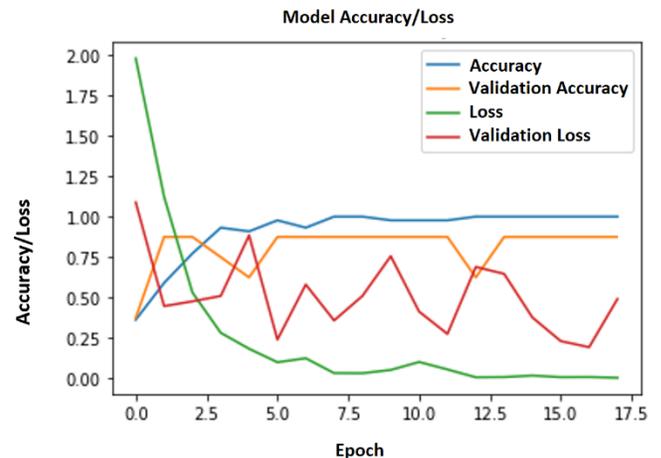


Fig. 5. The Accuracy and Loss Performance of the Proposed Model.

Based on the graph in Fig. 5, after 15 epochs, the model achieved almost 87% accuracy on validation dataset with the training loss 0.0125 and validation loss 0.25. To compare them with the existing works, the experimental result obtained in this study yielded a moderate performance as the accuracy is just between 60 to 80 percent throughout the 15 iterations. This may happen due to some factors such as small size of the data set and lack of image variation in every training sample. However, the accuracy rate obtained is still acceptable as the backend model for the FishDeTec application as shown in Fig. 6. The system is very simple and easy to use. With just one click, the user will be provided with the information about

the fish in English or Bahasa Melayu for every captured fish's image. All user needs to do is to just take picture of the fish and feed it into the system.

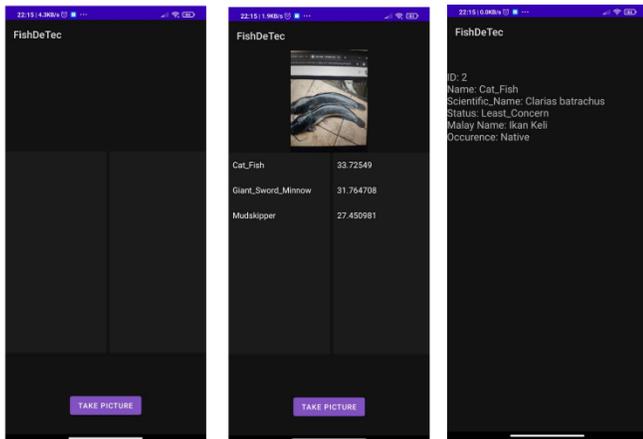


Fig. 6. The Final Look of FishDeTec.

## V. CONCLUSION

In this paper, we have presented the development of FishDeTec, a mobile application for identifying Malaysia freshwater fish. The model for detecting the fish species is developed using the VGG16, a Convolution Neural Network model introduced by K. Simonyan [7]. The TL in VGG16 is used to identify the freshwater fish species. We executed our proposed model using dataset consist of eight different types of freshwater species available in Malaysia, with 178 images in total. To minimize the risk of overfitting in various image variations, we have conducted an augmentation procedure. The foundation of the augmentation techniques used in this research was image transformations such as zoom, rotation, and flipping. The model achieved it's accuracy at 60-80 percent, when tested in the eight different types of species freshwater fish. To compare with the existing works, more works need to be done, especially on the validation accuracy. The validation loss need to be reduced. The experimental results show that the pre-trained modeled yielded the moderate performance. For future work, to resolve and reduce the error rate of the result as well as the limited number of images in the data set, pre-training models on the combination of ImageNet and image enhancement could be used to solve the problem. To increase the model validation, more species with a greater number of images for each species are required.

## REFERENCES

- [1] Y. Yong, L. Quek, E. Lim, and A. Ngo, "A case report of puffer fish poisoning in Singapore," *Case reports in medicine*, vol. 2013, 2013.
- [2] J. K. Sims and D. C. Ostman, "Pufferfish poisoning: emergency diagnosis and management of mild human tetrodotoxication," *Annals of emergency medicine*, vol. 15, pp. 1094-1098, 1986.
- [3] L. Chen, Z. Li, and Z. Zhao, "Forensic medical identification of death due to poisoning of tetrodotoxin in puffer fish," *Fa yi xue za zhi*, vol. 15, pp. 131-2, 189, 1999.
- [4] W. J. Matthews, *Patterns in freshwater fish ecology*: Springer Science & Business Media, 2012.

- [5] W. A. Wurts, "Why can some fish live in freshwater, some in salt water, and some in both," *World Aquaculture*, vol. 29, p. 65, 1998.
- [6] D. A. Kononov, A. Saleh, M. Bradley, M. Sankupellay, S. Marini, and M. Sheaves, "Underwater fish detection with weak multi-domain supervision," *2019 International Joint Conference on Neural Networks (IJCNN)*, 2019, pp. 1-8.
- [7] K. M. Knausgård, A. Wiklund, T. K. Sjørdalen, K. Halvorsen, A. R. Kleiven, L. Jiao, et al., "Temperate Fish Detection and Classification: a Deep Learning based Approach," *arXiv preprint arXiv:2005.07518*, 2020.
- [8] N. E. M. Khalifa, M. H. N. Taha, and A. E. Hassanien, "Aquarium family fish species identification system using deep neural networks," *International Conference on Advanced Intelligent Systems and Informatics*, 2018, pp. 347-356.
- [9] X. Bai, X. Yang, and L. J. Latecki, "Detection and recognition of contour parts based on shape similarity," *Pattern Recognition*, vol. 41, pp. 2189-2199, 2008.
- [10] J.-S. Kim and K.-S. Hong, "Color-texture segmentation using unsupervised graph cuts," *Pattern Recognition*, vol. 42, pp. 735-750, 2009.
- [11] Y. LeCun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, et al., "Backpropagation applied to handwritten zip code recognition," *Neural computation*, vol. 1, pp. 541-551, 1989.
- [12] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.
- [13] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in neural information processing systems*, vol. 25, pp. 1097-1105, 2012.
- [14] M. D. Zeiler and R. Fergus, "Visualizing and understanding convolutional networks," *European conference on computer vision*, 2014, pp. 818-833.
- [15] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770-778.
- [16] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, et al., "Going deeper with convolutions," *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 1-9.
- [17] P. Eosina, G. F. Laxmi, and F. Fatimah, "The Sobel Edge Detection Techniques for Freshwater Fish Image Analysis," *The 4th International Seminar on Sciences*, 2017, p. 83.
- [18] H. Wang, Y. Shi, Y. Yue, and H. Zhao, "Study on Freshwater Fish Image Recognition Integrating SPP and DenseNet Network," *2020 IEEE International Conference on Mechatronics and Automation (ICMA)*, 2020, pp. 564-569.
- [19] D. Rathi, S. Jain, and S. Indu, "Underwater fish species classification using convolutional neural network and deep learning," *2017 Ninth international conference on advances in pattern recognition (ICAPR)*, 2017, pp. 1-6.
- [20] F. Rossi, A. Benso, S. Di Carlo, G. Politano, A. Savino, and P. L. Acutis, "FishAPP: A mobile App to detect fish falsification through image processing and machine learning techniques," *2016 IEEE international conference on automation, quality and testing, robotics (AQTR)*, 2016, pp. 1-6.
- [21] H. Qin, X. Li, J. Liang, Y. Peng, and C. Zhang, "DeepFish: Accurate underwater live fish recognition with a deep architecture," *Neurocomputing*, vol. 187, pp. 49-58, 2016.
- [22] FishVerify. Species Identification and Regulation Guide. Available: [https://www.fishverify.com/#the\\_app](https://www.fishverify.com/#the_app).
- [23] F. ID+. Fish ID+ Fish Identifier for VIC - Apl di Google Play. Available: <https://play.google.com/store/apps/details?id=com.phonegap.fishidplus&hl=ms&gl=US>.
- [24] W. Rawat and Z. Wang, "Deep convolutional neural networks for image classification: A comprehensive review," *Neural computation*, vol. 29, pp. 2352-2449, 2017.

# Predicting the Anxiety of Patients with Alzheimer's Dementia using Boosting Algorithm and Data-Level Approach

Haewon Byeon

Department of Medical Big Data  
College of AI Convergence, Inje University, Gimhae 50834, Republic of Korea

**Abstract**—Since overfitting due to imbalanced data can cause prediction errors during the learning process of machine learning and degrades the prediction performance of the model (e.g., sensitivity), it is necessary to add an additional data sampling technique in the model development step to reduce overfitting to overcome this issue, in addition to selecting a machine learning algorithm suitable for the data. This study examined Alzheimer's patients living in South Korea to understand the predictors of anxiety using boosting algorithms (i.e., AdaBoost and XGBoost) and data-level approach (raw data, undersampling, oversampling, and SMOTE) and confirmed the machine learning algorithm with the best prediction performance. We analyzed 253 elderly people who were diagnosed with Alzheimer's disease (aged from 60 to 74 years old) who visited rehabilitation hospitals for early dementia screening. This study developed models for predicting the anxiety of Alzheimer's dementia patients using AdaBoost and XGBoost. Moreover, this study compared the prediction performance (i.e., accuracy, sensitivity, and specificity) of the models. The results of this study showed that XGBoost based on SMOTE (accuracy=0.84, sensitivity=0.85, and specificity=0.81) was identified as the model with the best prediction performance. Consequently, the results of this study presented that using a SMOTE-XGBoost model may provide higher accuracy than using a SMOTE-Adaboost model for developing a prediction model using outcome variable imbalanced data such as disease data in the future.

**Keywords**—Anxiety; AdaBoost; patients with Alzheimer's dementia; SMOTE; XGBoost

## I. INTRODUCTION

The number of people with dementia increases worldwide, and that increases in South Korea as well. It has been reported that the number of dementia elderly was 750,000 in South Korea in 2019, and it has been forecasted to increase to 1.96 million by 2040 [1]. The increase of people with dementia indicates an increase in the number of elderly people who need long-term care [2]. Since dementia is accompanied by physical, cognitive, and behavioral issues, people with dementia require the help of a caregiver [3]. Therefore, managing the elderly with dementia is an important issue not only for the patient, but also for the family, society, and the country.

Dementia is an irreversible disease that mostly occurs in old age. It has been reported that the prevalence of dementia is one out of ten elderly people over 65 years old and one out of

two elderly people over 85 years old [4]. Dementia can be classified into Alzheimer's disease, frontotemporal dementia, and Parkinson's dementia. Among them, Alzheimer's disease accounts for 60% of dementia patients, and it is difficult to detect early because the symptoms of it progress gradually and slowly [5]. The characteristic of Alzheimer's disease is to lose the memory of recent events [6]. Moreover, as the disease progresses further, people with it cannot remember the names of familiar people, names of objects, or places [7,8].

Additionally, apathy, depression, and anxiety were reported as the behavioral and psychological symptoms of dementia (BPSD), which are frequently observed in dementia as well as cognitive disorders [9,10]. BPSD including anxiety cause considerable pain to patients with Alzheimer's disease, which decreases the quality of life [11]. Lyketsos et al. (2000) [12] reported that 70-95% of dementia elderly residing in care facilities for the elderly and 60% of dementia elderly treated at home experienced BPSD. The BPSD of patients can lead to death by decreasing cognitive functions and/or exacerbating physical dysfunction [13]. Furthermore, it can not only negatively affect the lives of supporting family members, but also cause drastic pain [14,15]. In particular, BPSD including anxiety increase the medical expenses of dementia patients considerably: it has been reported that 30% of dementia-related medical expenses were for managing BPSD, and treating dementia patients with anxiety was much more expensive than treating those without anxiety [16].

Since it is easier to treat BPSD including anxiety than cognitive impairments, it is possible to improve the quality of life of dementia patients and their caregivers by detecting and treating these symptoms early appropriately [15, 17]. Consequently, detecting the anxiety of dementia patients as soon as possible is an important topic in geriatrics, and it requires developing a prediction model that can explore the risk factors of anxiety symptoms while considering a range of factors such as demographic characteristics, cognitive function, and ability to perform daily activities.

For the past 20 years, most studies on dementia have focused on the cognitive dysfunction of dementia, and relatively fewer studies aimed to identify the factors associated with BPSD [13]. Moreover, previous studies [18,19] mainly used regression analysis methods to identify risk factors for behavioral and psychological symptoms. Regression analysis methods are useful only for identifying

individual risk factors, but they are limited in identifying multiple risks [20]. In particular, only a few studies conducted in South Korea evaluated BPSD. Previous studies [21,22] could only grasp the relationship with individual factors such as demographic characteristics as a way to understand the relationship of it with individual factors such as demographic characteristics.

Boosting algorithms such as eXtreme Gradient Boosting (XGBoost) and AdaBoost are widely used to overcome the limitations of these regression models. Although numerous previous studies [5,23] have reported that machine learning is more accurate than traditional statistical techniques such as regression analysis, modeling using disease data is highly likely to suffer from imbalanced data because the number of patients is much smaller than those without a disease. Consequently, the likelihood of overfitting is high [24]. Since overfitting due to these imbalanced data can cause prediction errors during the learning process of machine learning and degrades the prediction performance of the model (e.g., sensitivity), it is necessary to add an additional data sampling technique in the model development step to reduce overfitting to overcome this issue, in addition to selecting a machine learning algorithm suitable for the data [25]. This study examined Alzheimer's patients living in South Korea to understand the predictors of anxiety using boosting algorithms (i.e., AdaBoost and XGBoost) and data-level approach (raw data, undersampling, oversampling, and SMOTE) and confirmed the machine learning algorithm with the best prediction performance.

## II. METHODS AND MATERIALS

### A. Subjects

This study analyzed 253 elderly people who were diagnosed with Alzheimer's disease among 1,553 elderly South Korean (aged from 60 to 74 years old) who visited rehabilitation hospitals and nursing hospitals in Incheon from August 2, 2017, to June 30, 2018, for early dementia screening. The screening conducted an in-depth dementia test, which was composed of sociodemographic information, previous medical history, cognitive function, mood, activities of daily living, interview with subjects and their guardians regarding changes in personality and others, Seoul Neuropsychological Screening Battery (SNSB)[26], and Korean version of Global Deterioration Scale(GDS)[27], for the diagnosis of Alzheimer's disease. A neurologist diagnosed Alzheimer's dementia based on the diagnosis criteria of "Diagnostic and Statistical Manual of Mental Disorder, 5th edition" and "National Institute of Neurological and Communicative Diseases and Stroke/Alzheimer's Disease and Related Disorders Association (Probable Alzheimer's disease)". This study excluded those who had severe visual and hearing impairment for conducting the test, a medical history of stroke, and profound dementia corresponding to CDR 3.

This study tested the power of sample size by using the G-Power program 3.1.9 (Universität Mannheim, Mannheim, Germany). The results showed that the minimum number of samples was 217 when power (1-B)=0.95, alpha=0.05, effect size (f<sup>2</sup>)=0.15, and 19 predictors were applied. Therefore, 253

samples of this study satisfied the condition for testing statistical significance.

### B. Measurements and Definitions of Variables

The outcome variable was defined as anxiety (yes, no). Explanatory variables were gender, age (65-75 for the young-old, and 75 and older for the old-old), an education level (middle school graduation or below, or high school graduation or above), income level (total household income), marital status (married, divorce/separation, or bereavement), smoking (non-smoking, former smoker, or current smoker), drinking habits (non-drinking, former drinker, or current drinker), exercise regularly at least once a week (yes or no), mean monthly social activity participation (less than 1 hour or 1 hour or more), subjective health (good, moderate, or poor), diabetes (yes or no), hypertension (yes or no), family history of dementia (yes or no), cognitive level (K-MMSE)[28], Clinical Dementia Rating (CDR) [29], depression, and activities of daily living (ADL).

Anxiety was measured by using Korean neuropsychiatric inventory (K-NPI)[30]. K-NPI is a standardized test tool that measures the BPSD of patients. It divides the abnormal behaviors of dementia into twelve domains (i.e., delusion, hallucination, aggression, depression, anxiety, euphoria, apathy, disinhibition, irritability, aberrant motor behavior, sleep, and appetite), and evaluates each sub-item. When an abnormal behavior is found in a specific sub-item (e.g., anxiety), frequency (0-4 points) and severity (0-3 points) are measured, and they are multiplied to produce the final value (0- 12 points). A higher score indicates a more anxious state. This study analyzed only the anxiety items in the K-NPI.

Cognitive function: Korean version of Mini-Mental Status Examination (K-MMSE) [28] was used as a tool to measure cognitive functions. K-MMSE includes diverse subcategories including temporal orientation, spatial orientation, memory, attention and computation ability, language ability, and spatiotemporal composition ability. It consists of 30 items (one point per item), and a lower score means more severe cognitive impairment. At the time of developing MMSE, the Cronbach'  $\alpha$  value was 0.82 [31].

Clinical Dementia Rating (CDR): CDR [29] is a tool that is designed to classify the severity of dementia into five levels from a clinical perspective based on the evaluation of six areas (i.e., memory, orientation, judgment, problem-solving ability, social activities, family life and hobby, and hygiene and dressing up. At the time of developing the CDR, the inter-inspector reliability was Kappa=0.86~1.0 [29].

Depression: This study used the Short form of Geriatric Depression Scale Korea (SGDS-K) [33] for depression, which was standardized and developed according to the circumstances of the elderly in South Korea by extracting 15 items out of the 30 items of the Geriatric Depression Scale(GDS)[32]. SGDS-K is composed of a binary scale (yes/no), and ranges from 0 to 15. A higher score means a severe depression level. This study defined the threshold of SGDS-K, defining depression, as 8 points. At the time of developing SGDS-K, Cronbach'  $\alpha$  value was 0.94 [32].

Activities of Daily Living (ADL): Korean version of Barthel Activities of Daily Living Index (K-BADL) [34] is a standardized test tool for measuring the activities of daily living, and this study used this tool. K-BADL consists of 10 sub-categories: bowels, bladder, washing face/hair combing/tooth brushing/shaving, toilet use, eating, transfer, mobility, dressing, going up and down stairs, and bathing. The score ranges from 0 to 20, and a higher score indicates that a person can perform more independently without the help of people around the person (normal level).

### C. Development of Prediction Models and Validation of Predictive Performance

This study developed models for predicting the anxiety of Alzheimer's dementia patients using AdaBoost and XGBoost. Moreover, this study compared the prediction performance (i.e., accuracy, sensitivity, and specificity) of the models. This study randomly divided the data into a training dataset and a test dataset at a ratio of 7:3, developed prediction models, and tested the performance of the models using the test dataset. A 5-fold cross-validation (CV) was performed only on the training dataset, and the test dataset was used to evaluate the prediction performance. Random forest and XGBoost models contain randomness, and models were developed by fixing the seed to "01234". The prediction performance of each model was evaluated by the area under the curve (AUC) of the receiver operating characteristic (ROC) curve (Fig. 1) [35]. The accuracy, sensitivity, and specificity of each model were calculated as evaluation indices for model performance. Accuracy indicates the proportion of successful predictions among all samples. Sensitivity means the true positive rate, indicating that a prediction model predicts a dementia patient with anxiety as anxiety. Specificity means the true negative rate, indicating that a prediction model predicts a dementia patient without anxiety as no-anxiety. This study compared the prediction performance of each model and determined that a model with the highest accuracy with 0.6 or higher sensitivity and specificity as the best model. If models have the same accuracy, the model with the high sensitivity value was selected as the best prediction model. All analyses were carried out using R version 4.0.3 (Foundation for Statistical Computing, Vienna, Austria).

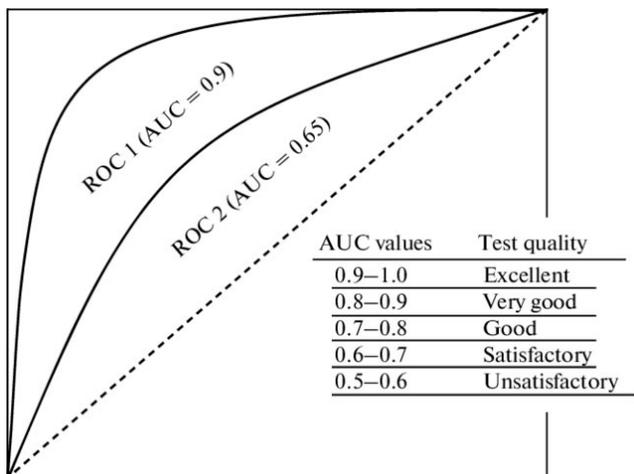


Fig. 1. Concept of Receiver Operating Characteristic Curve [35].

### D. Boosting Algorithm

The boosting algorithm refers to the process of making a strong classifier showing a strong performance by using a linear combination of weak classifiers that have already been given. Freund et al. (1996) [36] introduced an improved technique to apply the boosting idea to actual data analysis in 1995, and it proved that the error rate of the boosting algorithm approached zero as the number of weak classifiers increased. The advantage of the boosting learning method is (1) it has relatively fewer parameters to be predicted compared to other learning methods; (2) a cascade classification model can be easily constructed in the aspect of false positive; (3) the boosting algorithm reduces the bias of the predicted values; and (4) since it is possible to select one specific dimension through a weak classifier, it can be applied as a method of feature selection when using data with many variables. This study developed the model for predicting the anxiety of dementia patients using Adaboost and XGBoost methods among boosting algorithms.

### E. Adaboost

Adaboost is a learning technique that creates a strong classifier by repeatedly training a very weak classifier using samples of two classes. This technique improves the performance of a weak classifier by training the weak classifier while giving the same weight to all samples at first, and then increasing the weight of the sample misclassified by the basic classifier as steps progress. The concept of Adaboost [37] is presented in Fig. 2.

### F. XGBoost

XGBoost is one of the boosting methods. This method uses the observations misclassified while generating trees more in the next model. In other words, it is a boosting algorithm that trains a classifier to have better performance for misclassified observations. The advantages of the XGBoost model are that it can prevent overfitting by minimizing the training loss and it has a faster learning and classification speed than existing gradient boosting models [38] because it is based on parallel and distributed processing. The concept of XGBoost [39] is presented in Fig. 3.

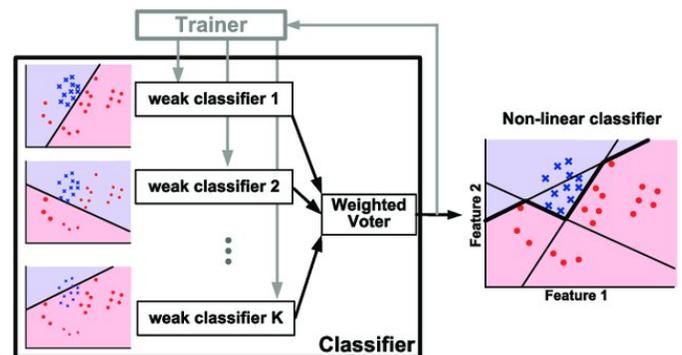


Fig. 2. AdaBoost Algorithm [37].

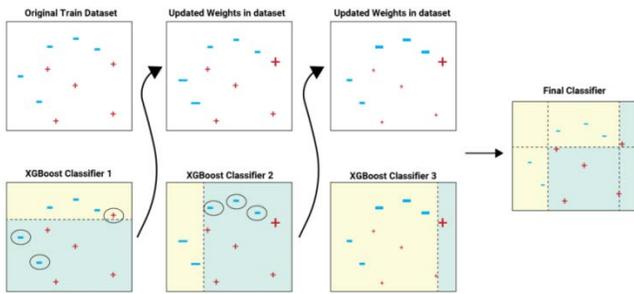


Fig. 3. XGBoost Algorithm [39].

### G. Data-level Approach

Disease data generally have an imbalance issue because the number of patients is smaller than that of healthy people. The data of this study also had an imbalance issue because the results of K-NPI test showed that 90.5% of subjects were Alzheimer's dementia patients without anxiety and 9.5% of them were Alzheimer's dementia patients with anxiety. This study compared prediction performance (accuracy, sensitivity, and specificity) using oversampling [40], undersampling [41], and SMOTE method [42] among various data-level approaches to overcome the data imbalance problem.

Oversampling is a data-level approach that solves the imbalance issue by duplicating data with a small number of classes [43]. For example, if there are 90 0s and ten 1s, 1 can be duplicated to be 90 1s. As a result, the total number of data becomes 180, and the ratio of 0 to 1 becomes 1:1. Generally, it is possible to make a different ratio instead of 1:1. When the number of original data is large, oversampling may take longer to build a model due to a larger sample size, which is a shortfall. Moreover, it may cause an overfitting problem [44]. The concept of oversampling [45] is presented in Fig. 4.

Undersampling is a data-level approach that resolves the data imbalance problem by randomly removing the class with a response variable of 0 [43]. In other words, it randomly removes 0 to make the ratio of 0 and 1 set to be 1:1. In general, it is possible to adjust the data so that the ratio is different, instead of 1:1. Since undersampling is a method of removing data as shown, it may cause information loss, a problem. The concept of undersampling [45] is presented in Fig. 5.

Synthetic minority over-sampling technique (SMOTE) is a method that combines oversampling and undersampling. It randomly selects one of the minor classes among the classes of the response variable, and then it finds  $k$  neighbors of this data. Then, the difference between the selected sample and  $k$  neighbors is calculated, and this difference is multiplied by a random value between 0 and 1. The calculated value is added to the existing sample, and then it is added to the training dataset. Finally, this process is repeated. The SMOTE algorithm is similar to oversampling in the aspect that it increases the data of the minor class. However, it is known that it makes up for the overfitting issue of oversampling, by creating a new sample by appropriately combining the existing data instead of duplicating the same data. The concept of the SMOTE algorithm [46] is presented in Fig. 6.

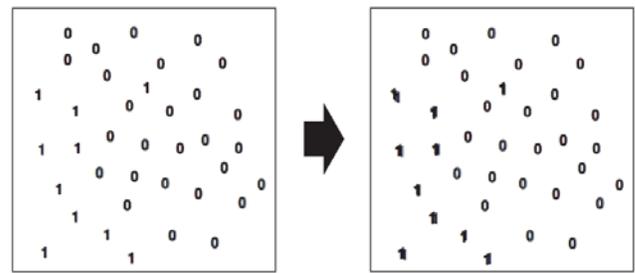


Fig. 4. Example of Oversampling: Replication of 1 [45].

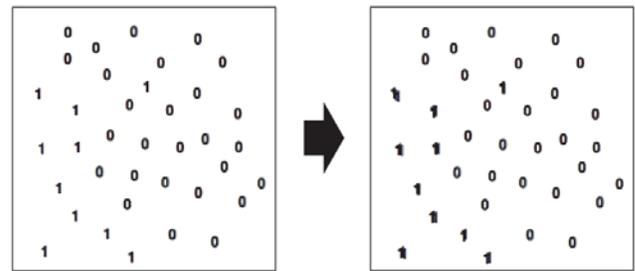


Fig. 5. Example of Undersampling: Removing 0 Randomly [45].

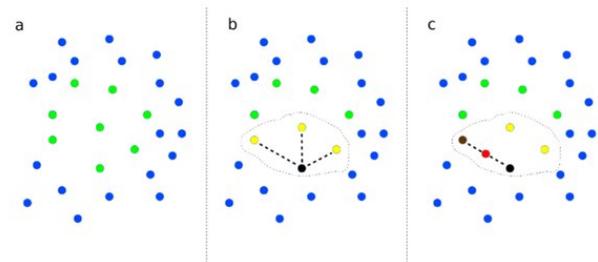


Fig. 6. The Concept of the SMOTE Algorithm [46].

## III. RESULTS

### A. Accuracy of Prediction Models

The accuracy, sensitivity, and specificity of a eight prediction models ((AdaBoost & XGBoost) x (raw data, undersampling, oversampling, and SMOTE)) are presented in Table I. It was found that XGBoost based on SMOTE (accuracy=0.84, sensitivity=0.85, and specificity=0.81) was identified as the model with the best prediction performance (Fig. 7). Anxiety predictors of Alzheimer's dementia patients using SMOTE-XGBoost are presented in Table II. When the normalized importance of variables was analyzed, age, gender, family history of dementia, depression, ADL, K-MMSE, and CDR were confirmed as the major factors for predicting the anxiety of Alzheimer's dementia patients. Among them, depression showed the highest importance.

TABLE I. PERFORMANCE OF PREDICTION MODELS USING DATA-LEVEL APPROACH (ACCURACY, SENSITIVITY, AND SPECIFICITY)

Model		AdaBoost	XGBoost
Raw data	Accuracy	0.85	0.83
	Sensitivity	0.67	0.63
	Specificity	0.95	0.90
Under-sampling	Accuracy	0.75	0.76
	Sensitivity	0.73	0.74
	Specificity	0.79	0.83
Over-sampling	Accuracy	0.76	0.78
	Sensitivity	0.72	0.75
	Specificity	0.80	0.83
SMOTE	Accuracy	0.81	0.84
	Sensitivity	0.79	0.85
	Specificity	0.85	0.81

TABLE II. RESULTS OF MODEL TO PREDICT THE ANXIETY

Model	Factors	Characteristics
XGBoost	7	Age, sex, family history of dementia, depression, ADL, MMSE, CDR

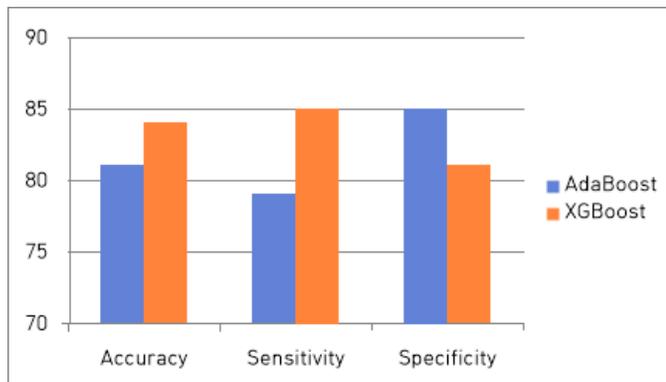


Fig. 7. Accuracy, Sensitivity, and Specificity Comparison of SMOTE-AdaBoost and SMOTE-XGBoost (%).

#### IV. DISCUSSION

This study developed models for predicting the anxiety of Alzheimer's dementia patients using the boosting algorithm and data-level approach. The results of this study showed that age, gender, family history of dementia, depression, ADL, MMSE, and CDR were the major factors in predicting the anxiety of Alzheimer's dementia patients. Previous studies [47,48] also revealed that age was significantly related to the behavioral and psychological symptoms of dementia patients. The results of Mushtaq et al. (2016) [49] showed that it was considerably associated with mood and aggressive behavior for early-onset Alzheimer's disease and it was related to psychosis for late-onset Alzheimer's disease was associated with psychosis.

Gang et al. (2016) [50] reported that a lower cognitive function score indicated a worse behavioral and/or psychological symptom. Cho et al. (2006)[51] also reported

that as the cognitive function decreased, the frequency of anxiety increased. The progression (stage) of dementia was also reported as a predictor of behavioral and psychological symptoms, and the stage of dementia was positively correlated with the number of expressed behavioral and psychological symptoms [52]. Particularly, as shown in this study, Hall et al. (2004) [53] also reported that depression was the most powerful factor influencing the occurrence frequency of behavioral and psychological symptoms such as anxiety. According to the results of this study, if an elderly Alzheimer's disease patient with reduced cognitive functions shows a depression symptom, the patient has a higher risk of anxiety. Therefore, it is necessary to identify and treat anxiety symptoms as soon as possible to maintain the patient's mental health.

This study developed prediction models based on imbalanced data using a boosting algorithm and a data-level approach. The results showed that the SMOTE-XGboost model showed the best prediction performance. Similar to the results of this study, Byeon (2021) [24] also reported that an XGboost model showed superior classification accuracy compared to other boosting algorithms. It is believed that it has good prediction performance in classification and regression domains because XGboost has unique overfitting regularization and early-stopping functions, which GBM does not have, even though XGboost is a tree-based boosting algorithm and it is based on the gradient boosting algorithm (GBM).

#### V. CONCLUSION

Consequently, the results of this study presented that using a SMOTE-XGboost model may provide higher accuracy than using a SMOTE-Adaboost model for developing a prediction model using outcome variable imbalanced data such as disease data in the future.

#### ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07041091, NRF-2019S1A5A8034211).

#### REFERENCES

- [1] Central dementia center, Korea dementia status 2019. Central dementia center, Seoul, 2020.
- [2] D. Figueiredo, A. Barbosa, J. Cruz, A. Marques, and L. Sousa, Empowering staff in dementia long-term care: towards a more supportive approach to interventions. *Educational Gerontology*, vol. 39, no. 6, pp. 413-427, 2013.
- [3] H. Byeon, Development of depression prediction models for caregivers of patients with dementia using decision tree learning algorithm. *International Journal of Gerontology*, vol. 13, pp. 314-319, 2019.
- [4] B. L. Plassman, K. M. Langa, G. G. Fisher, S. G. Heeringa, D. R. Weir, M. B. Ofstedal, J. R. Burke, M. D. Hurd, G. G. Potter, W. L. Rodgers, D. C. Steffens, R. J. Willis, and R. B. Wallace, Prevalence of dementia in the United States: the aging, demographics, and memory study. *Neuroepidemiology*, vol. 29, no. 1-2, pp. 125-132, 2007.
- [5] A. Kumar, and A. Singh, A review on Alzheimer's disease pathophysiology and its management: an update. *Pharmacological Reports*, vol. 67, no. 2, pp. 195-203, 2015.
- [6] H. Jahn, Memory loss in Alzheimer's disease. *Dialogues in Clinical Neuroscience*, vol. 15, no. 4, pp. 445-454, 2013.

- [7] H. Byeon, Developing a random forest classifier for predicting the depression and managing the health of caregivers supporting patients with Alzheimer's Disease. *Technology and Health Care*, vol. 27, no. 5, pp. 531-544, 2019.
- [8] H. Byeon, D. Lee, and S. Cho, Assessment for the model predicting of the cognitive and language ability in the mild dementia by the method of data-mining technique. *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 6, pp. 75-79, 2016.
- [9] H. Byeon, Application of machine learning technique to distinguish Parkinson's disease dementia and Alzheimer's dementia: predictive power of Parkinson's disease-related non-motor symptoms and neuropsychological profile. *Journal of Personalized Medicine*, vol. 10, no. 2, pp. 31, 2020.
- [10] A. L. Byers, and K. Yaffe, Depression and risk of developing dementia. *Nature Reviews Neurology*, vol. 7, no. 6, pp. 323-331, 2011.
- [11] P. J. Seignourel, M. E. Kunik, L. Snow, N. Wilson, and M. Stanley, Anxiety in dementia: a critical review. *Clinical Psychology Review*, vol. 28, no. 7, pp. 1071-1082, 2008.
- [12] C. G. Lyketsos, M. Steinberg, J. T. Tschanz, M. C. Norton, D. C. Steffens, and J. C. Breitner, Mental and behavioral disturbances in dementia: findings from the cache county study on memory in aging. *American Journal of Psychiatry*, vol. 157, no. 5, pp. 708-714, 2000.
- [13] J. Cerejeira, L. Lagarto, and E. Mukaetova-Ladinska, Behavioral and psychological symptoms of dementia. *Frontiers in neurology*, vol. 3, pp. 73, 2012.
- [14] J. Onishi, Y. Suzuki, H. Umegaki, A. Nakamura, H. Endo, and A. Iguchi, Influence of behavioral and psychological symptoms of dementia (BPSD) and environment of care on caregivers'burden. *Archives of Gerontology and Geriatrics*, vol. 41 no. 2, pp. 159-168, 2005.
- [15] H. Byeon, Effects of grief focused intervention on the mental health of dementia caregivers: systematic review and meta-analysis. *Iranian Journal of Public Health*, vol. 49, no. 12, pp. 2275-2286, 2020.
- [16] M. Schnaider Beeri, P. Werner, M. Davidson, and S. Noy, The cost of behavioral and psychological symptoms of dementia (BPSD) in community dwelling Alzheimer's disease patients. *International Journal of Geriatric Psychiatry*, vol. 17, no. 5, pp. 403-408, 2002.
- [17] L. N. Kirk, Neuropsychiatric symptoms in mild cognitive impairment: development and testing of a conceptual model. University of Minnesota, Minneapolis, 2008.
- [18] A. Feast, M. Orrell, I. Russell, G. Charlesworth, and E. Moniz-Cook, The contribution of caregiver psychosocial factors to distress associated with behavioural and psychological symptoms in dementia. *International Journal of Geriatric Psychiatry*, vol. 32, no. 1, 76-85, 2017.
- [19] S. Zhang, Q. Guo, H. Edwards, P. Yates, and C. Li, Self-efficacy moderation and mediation roles on BPSD and social support influences on subjective caregiver burden in Chinese spouse caregivers of dementia patients. *International Psychogeriatrics*, vol. 26, no. 9, pp. 1465-1473, 2014.
- [20] H. Byeon, S. Cha, and K. Lim, Exploring factors associated with voucher program for speech language therapy for the preschoolers of parents with communication disorder using weighted random forests. *IJACSA*, vol. 10, no. 12-19, 2019.
- [21] J. A. Song, and Y. Oh, The association between the burden on formal caregivers and behavioral and psychological symptoms of dementia (BPSD) in Korean elderly in nursing homes. *Archives of Psychiatric Nursing*, vol. 29, no. 5, pp. 346-354, 2015.
- [22] J. H. Kim, D. Y. Lee, S. J. Lee, B. Y. Kim, and N. C. Kim, Predictive relationships between BPSD, ADLs and IADLs of the elders with dementia in Seoul, Korea. *Journal of Korean Gerontological Nursing*, vol. 17, no. 1, pp. 1-9, 2015.
- [23] J. Cerejeira, L. Lagarto, and E. Mukaetova-Ladinska, Behavioral and psychological symptoms of dementia. *Frontiers in Neurology*, vol. 3, pp. 73, 2012.
- [24] H. Byeon, Development of a physical impairment prediction model for Korean elderly people using synthetic minority over-sampling technique and XGBoost. *IJACSA*, vol. 12, no. 1, pp. 36-41, 2021.
- [25] H. Byeon, Predicting the depression of the South Korean elderly using SMOTE and an imbalanced binary dataset. *IJACSA*, vol. 12, no. 1, pp. 74-79, 2021.
- [26] H. J. Ahn, J. Chin, A. Park, B. H. Lee, M. K. Suh, S. W. Seo, and D. L. Na, Seoul Neuropsychological Screening Battery-dementia version (SNSB-D): a useful tool for assessing and monitoring cognitive impairments in dementia patients. *Journal of Korean Medical Science*, vol. 25, no. 7, pp. 1071-1076, 2010.
- [27] S. H. Choi, D. L. Na, B. H. Lee, D. S. Hahm, J. H. Jeong, Y. Jeong, E. J. Koo, C. K. Ha, S. S. Ann, and Korean Dementia Research Group, The validity of the Korean version of Global Deterioration Scale. *Journal of the Korean Neurological Association*, vol. 20, no. 6, pp. 612-617, 2002.
- [28] Y. Kang, D. L. Na, and S. Hahn, A validity study on the Korean Mini-Mental State Examination (K-MMSE) in dementia patients. *Journal of the Korean Neurological Association*, vol. 15, no. 2, pp. 300-308, 1997.
- [29] L. Berg, Clinical dementia rating. *The British Journal of Psychiatry*, vol. 145, no. 3, pp. 339-339, 1984.
- [30] S. H. Choi, D. L. Na, H. M. Kwon, S. J. Yoon, J. H. Jeong, and C. K. Ha, The Korean version of the neuropsychiatric inventory: a scoring tool for neuropsychiatric disturbance in dementia patients. *Journal of Korean Medical Science*, vol. 15, no. 6, pp. 609-615, 2000.
- [31] M. F. Folstein, S. E. Folstein, and G. Fanjiang., MMSE: Mini-Mental State Examination clinical guide. *Psychological Assessment Resources*, Florida , 2001.
- [32] J. A. Yesavage, Geriatric depression scale. *Psychopharmacol Bull*, vol. 24, no. 4, pp. 709-711, 1988.
- [33] J. N. Bae, and M. J. Cho, Development of the Korean version of the Geriatric Depression Scale and its short form among elderly psychiatric patients. *Journal of Psychosomatic Research*, Vol. 57, no. 3, pp. 297-305, 2004.
- [34] S. Y. Kim, C. W. Won, and Y. G. Rho, The validity and reliability of Korean version of Bathel ADL Index. *Journal of the Korean Academy of Family Medicine*, vol. 25, no. 7, pp. 534-541, 2004.
- [35] O. P. Trifonova, P. G. Likhov, and A. I. Archakov, Metabolic profiling of human blood. *Biomeditsinskaya Khimiya*, vol. 60, no. 3, pp. 281-294, 2014.
- [36] Y. Freund, and R. E. Schapire, Experiments with a new boosting algorithm. In *Proceedings of the IEEE International Conference of Machine Learning*, pp. 148-156, 1996.
- [37] Z. Wang, J. Zhang, and N. Verma, Realizing low-energy classification systems by implementing matrix multiplication directly within an ADC. *IEEE Transactions on Biomedical Circuits and Systems*, vol. 9, no. 6, pp. 825-837, 2015.
- [38] J. Nobre, and R. F. Neves, Combining principal component analysis, discrete wavelet transform and XGBoost to trade in the financial markets. *Expert Systems with Applications*, vol. 125, pp. 181-194, 2019.
- [39] C. Hoffstein, XG-Boost model. *Flirting with Models*, Washington, 2020.
- [40] L. Abdi, and S. Hashemi, To combat multi-class imbalanced problems by means of over-sampling techniques. *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, no. 1, pp. 238-251, 2015.
- [41] S. J. Yen, and Y. S. Lee, Cluster-based under-sampling approaches for imbalanced data distributions. *Expert Systems with Applications*, vol. 36, no. 3, pp. 5718-5727, 2009.
- [42] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, SMOTE: synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, vol. 16, pp. 321-357, 2002.
- [43] R. Longadge, and S. Dongre, Class imbalance problem in data mining review. *arXiv preprint arXiv*, vol. 1305. pp. 1707, 2013.
- [44] H. He, and E. A. Garcia, Learning from imbalanced data. *IEEE Transactions on Knowledge and Data Engineering*, vol. 21, no. 9, pp. 1263-1284, 2009.
- [45] H. Kim, and W. Lee, On sampling algorithms for imbalanced binary data: performance comparison and some caveats. *The Korean Journal of Applied Statistics*, vol. 30, no. 5, pp. 681-690, 2009.
- [46] M. Schubach, M. Re, P. N. Robinson, and G. Valentini, Imbalance-aware machine learning for predicting rare and common disease-associated non-coding variants. *Scientific Reports*, vol. 7, no. 1, pp. 1-12, 2017.
- [47] J. H. Kim, D. Y. Lee, S. J. Lee, B. Y. Kim, and N. C. Kim, Predictive relationships between BPSD, ADLs and IADLs of the elders with

- dementia in Seoul, Korea. *Journal of Korean Gerontological Nursing*, vol. 17, no. 1, pp. 1-9, 2015.
- [48] K. Konishi, K. Hori, T. Oda, I. Tominaga, T. Asaoka, M. Hachisu, and T. Shibasaki, Effects of aging on behavioral symptoms in Alzheimer's disease. *Psychogeriatrics*, vol. 9, no. 1, pp. 11-16, 2009.
- [49] R. Mushtaq, C. Pinto, S. Faisal Ahmad Tarfarosh, A. Hussain, S. Shoib, T. Shah, S. Shah, M. Manzoor, M. Bhat, and T. Arif, A comparison of the Behavioral and Psychological Symptoms of Dementia (BPSD) in early-onset and late-onset Alzheimer's disease-a study from South East Asia (Kashmir, India). *Cureus*, vol. 8, no. 5, pp. e635, 2016.
- [50] M. S. Gang, H. O. Park, and H. J. Park, Factors affecting agitation in nursing home patients with dementia. *Journal of Korean Gerontological Nursing*, vol. 18, no. 1, pp. 41-52, 2016.
- [51] M. J. Cho and J. Y. Kim, A study on cross-cultural characteristics of behavioral and psychological symptoms of dementia in Korea. Seoul National University Press, Seoul, 2006.
- [52] J. L. Fuh, S. J. Wang, and J. L. Cummings, Neuropsychiatric profiles in patients with Alzheimer's disease and vascular dementia. *Journal of Neurology, Neurosurgery, and Psychiatry*, vol. 76, no. 10, pp. 1337-1341, 2005.
- [53] K. A. Hall, and D. W. O'connor, Correlates of aggressive behavior in dementia. *International Psychogeriatrics*, vol. 16, no. 2, pp. 141-158, 2004.

# Deep Learning Hybrid with Binary Dragonfly Feature Selection for the Wisconsin Breast Cancer Dataset

Marian Mamdouh Ibrahim<sup>1\*</sup>, Dina Ahmed Salem<sup>2</sup>, Rania Ahmed Abdel Azeem Abul Seoud<sup>3</sup>

PhD researcher - Faculty of engineering, Fayoum University, Egypt, Fayoum<sup>1</sup>

Assistant Professor - Computer Department - Faculty of Engineering  
Misr University for Science and Technology (MUST).Egypt, Cairo<sup>2</sup>

Professor of digital signals at the Department of Electrical Engineering  
Faculty of Engineering Fayoum University Egypt, Fayoum<sup>3</sup>

**Abstract**—Breast cancer is the world's top cancer affecting women. While the danger of the factors varies from a place, lifestyle, and diet. Treatment procedures after discovering a confirmed cancer case can reduce the risk of the disease. Unfortunately, breast cancers that arise in low and middle-income countries are diagnosed at a very late stage in which the chances of survival are impeded and reduced. Early detection is therefore required not only to improve the accuracy of discovering breast cancer but also to increase the chances of making the right decision on a successful treatment plan. There have been several studies tending to build software models utilizing machine learning and soft computing techniques for cancer detection. This research aims to build a model scheme to facilitate the detection of breast cancer and to provide the exact diagnosis. Improving the accuracy of a proposed model has, therefore, been one of the key fields of study. The model is based on deep learning that intends to develop a framework to accurately separate benign and malignant breast tumors. This study optimizes the learning algorithm by applying the Dragonfly algorithm to select the best features and perfect parameter values of the deep learning model. Moreover, it compares deep learning results against that of support vector machine (SVM), random forest (RF), and k nearest neighbor (KNN). Those classifiers are chosen as they are the most reliable algorithms having a solid fingerprint in the field of clinical data classification. Consequently, the hybrid model of deep learning combined with binary dragonfly has accurately classified between benign and malignant breast tumors with fewer features. Besides, deep learning model has achieved better accuracy in classifying Wisconsin Breast Cancer Database using all available features.

**Keywords**—Breast cancer; Wisconsin data set; classifiers; deep learning; feature selection; dragonfly

## I. INTRODUCTION

Breast cancer is the most common cancer in women and, overall, the second most leading to death. In 2019, women were diagnosed with an estimated 268,600 new cases of invasive breast cancer and approximately 2,670 cases were diagnosed in men [1]. An accurate diagnosis for various sorts of cancer plays a great role for doctors to assist them in determining and choosing the proper treatment. Lately, the application of various artificial intelligence (AI) classification methods has been proven in aiding doctors to facilitate their decision-making process [2]. Recently, the use of AI classification techniques in the medical field generally and cancer detection particularly has grabbed the researchers'

attention. AI is beneficial in reducing medical human-errors (because it minimizes possible errors) that might occur due to unskilled doctors [3].

More research is being done on breast cancer diagnosis using the Wisconsin Breast Cancer Database (WBCD)[4]. Many methods have been constantly developed to achieve accurate and efficient diagnosis results and several experiments were performed on the WBCD using multiple classifiers and feature selection techniques. Many of them show a good classification accuracy, for example, in [5] the performance criterion of supervised learning classifiers such as Naïve Bayes (NB), Support Vector Machine (SVM-RBF) kernel, and neural networks (NN) are compared to find the best classifier using the dataset (WBCD), and the SVM-RBF has the best outcome achieving 96.84%. The robustness of the least square Support Vector Machine (SVM) obtained a classification accuracy of 98.53% [6]. In [7] Linear Regression achieved an average training accuracy of 96.093%, whereas Multilayer Perceptron (MLP) is 99.038%, Softmax Regression has an average training accuracy of 97.366573% and the accuracy obtained by SVM (97.13%) is better than the accuracy obtained by KNN [8]. The prediction accuracy of the SVM (linear kernel) in [9] reaches 97.14%, an accuracy of 95.71% using RBF kernel, and 97.14% using RF classifier for Breast Cancer detection. The accuracy obtained from the system which combines rough set theory with backpropagation neural network in [10] is 98.6% on the breast cancer dataset. The first stage handles missing values to obtain a smooth data set and to select appropriate attributes from the clinical dataset by the indiscernibility relation method. The second stage is classification using a backpropagation neural network. The algorithm KNN for classification which is used in [11] with several different types of distances and classification rules is used in the diagnosis and classification of cancer, and these experiments are conducted on the database WBCD. The results advocate the use of the KNN algorithm with both types of Euclidean distance and Manhattan that give the best results (98.70% for Euclidean distance and 98.48% for Manhattan with  $k = 1$ ), these values are not significantly affected even when  $k=1$  is increased to 50. SVM and KNN individually used in [12] achieved the accuracy of 98.57% and 97.14%, respectively. This work aims to automatically design and modify the parameters of the deep learning model hybrid with the Dragonfly algorithm for breast cancer diagnosis.

\*Corresponding Author

## II. MATERIALS AND METHODS

### A. Machine Intelligence Library

The software, developed for implementation in this study is written by using Spyder which is an interactive development environment capable of advanced editing, interactive testing, debugging, and introspection for Python (version 3.7 was used) programming language. Also, Keras [13] neural network API was used for deep learning in the developed method. It is a high-level neural network API, supporting Python which can convert the results rapidly, highly modular, minimalist, and has extensible features. Keras with Google TensorFlow backend is used to implement the deep learning algorithms in this study, with the aid of other scientific computing libraries: matplotlib [14] is a comprehensive library for creating interactive, and animated visualizations in Python, NumPy [15] is a library for the Python programming language, adding support for big, multi-dimensional arrays and matrices, along with a huge collection of high-level mathematical functions to operate on these arrays, and scikit-learn [16] is a free software machine learning library for the Python programming language, where it emphasizes several classifications, regression, and clustering algorithms including support vector machines, k-means, random forests.

### B. Dataset Description

The UCI machine learning repository has been used to download the WBCD [4] for breast cancer classification [17]. This dataset usage is more common among researchers who utilize machine learning methods for the classification of breast cancer. Each dataset is composed of a set of numerical attributes that were assessed by fine needle aspiration (FNA) from human breast cancer tissue. WBCD has 699 instances and 10 attributes including the class attribute. One of the two possible classes is found in each instance; malignant (M) or benign (B). Every attribute has been represented in the form of an integer between 1 and 10. These attributes include: (uniformity of cell size, clump thickness, uniformity of cell shape, single epithelial cell size, marginal adhesion, bare nuclei, normal nuclei, bland chromatin, and mitosis).

### C. Data Preprocessing

Preparing data for use in a machine learning (ML) framework is significant, where data preparation requires at least 80 percent of the total time expected to create an ML system. Data preparation has three main phases: cleaning, normalizing, and encoding, and splitting. Each of the three phases has several steps. Equation (1) is used to normalize dataset attributes.

$$Z = \frac{X - \mu}{\sigma} \quad (1)$$

Where X represents the dataset attributes,  $\mu$  represents the mean value for each dataset attribute  $x(i)$ , and  $\sigma$  represents the corresponding standard deviation. This normalization technique was implemented using the Standard Scaler of scikit-learn.

### D. Principal Component Analysis

Principal Component Analysis (PCA) [18] is a dimension reduction method that includes related features. Dimensionality

reduction [19] is a process used in Data Mining where the numbers of random variables under consideration are reduced. An essential step in the efficient analysis of large high-dimensional data sets is the reduction of dimensions. PCA performs dimensionality reduction whilst maintaining maximum feasible arbitrariness in the high-dimensional space. PCA is probably the oldest and certainly the most popular technique for computing lower-dimensional representations of multivariate data. The technique is linear in the sense that the components are linear combinations of the original variables (features), but non-linearity in the data is preserved for effective visualization. The PCA is a method of statistical data analysis that transforms the initial set of variables into an assorted set of linear combinations, referred to as the principal components (PC), with variance-specific properties. This condenses the system's dimensionality while retaining the variable connections information. The analysis is carried out by calculating and analyzing the data covariance matrix on a data set, its eigenvalues along with its respective eigenvectors systematized in descending order.

### E. Classification Techniques

The classification aims to develop a set of models that can correctly classify the class of different objects. There are three types of inputs to such models, which are: (a) a bunch of objects that are described as training data, (b) the dependent variables, and (c) classes that may be a group of variables describing various characteristics of the objects. Once a classification model is built, it tends to be utilized to classify the class of the objects to which class information is unidentified [20]. There are numerous sorts of classifiers that have been utilized for a cancer diagnosis; some of them are NN, SVM, KNN, NB, and RF. They are used to classify cancer datasets as malignant and benign tumors.

1) *Support vector machine*: Support vector machine (SVM) classifier is a type of supervised machine learning classification algorithm, it is applied in classifying cancer because it is a non-probabilistic binary and nonlinear statistical tool which works by separating space into two regions by a straight line or hyperplane in higher dimensions. It examines the data, recognizes the pattern, and classifies the data based on common attributes by using kernel tricks. The kernel is a set of numerical functions that are used in SVM. The kernel's function is to take data as an input and convert it into the form necessary. Various kinds of kernel functions were utilized by the SVM algorithm. These functions can be different types; for example, linear, nonlinear, polynomial, radial basis (RBF), and sigmoid functions.

2) *Naïve Bayes*: Naïve Bayes (NB) is a probabilistic classifier based on the Bayes theorem. Rather than predictions, it produces probability estimates. For the value of each class, it estimates the probability of each given instance belongs to that class. An advantage of the NB classifier is that it requires a small amount of training data in order to estimate the parameters that are mandatory for classification.

3) *Artificial Neural Network*: Artificial Neural Network (ANN) is a numerical model based on biological neural networks. It comprises an interconnected group of artificial

neurons, and it processes information employing a connectionist approach to the computing process. In most cases, an ANN is a robust framework that changes its structure based on outside or inner data that flows through the network during the learning phase. One of the fundamental advantages of ANN over conventional methods is its ability in capturing the complex and nonlinear interaction between prognostic markers and the outcome to be anticipated.

4) *Random forest (RF)*: Random forest (RF) algorithm is a supervised classification algorithm that creates a forest with several trees. It is a flexible, easy to utilize machine learning algorithm that mostly produces a great result. Due to its simplicity, it is also one of the most used algorithms. The more trees in the forest the more robust the forest appears in general. In the same way in the random forest classifier, the higher the number of trees in the forest indicates the high accuracy results.

5) *K-nearest Neighbors*: K-nearest Neighbors (KNN) is one of the most used algorithms in machine learning. It is a method of learning based on instances that do not require a phase of learning. The model developed is the training sample, connected to a distance function and the choice function of the class based on the classes of the nearest neighbors. Before classifying a new element, it must be compared with other elements using a similarity measure. Its k-nearest neighbors consider the class that appears most among the neighbors is assigned to the element to be classified. Besides, the appropriate functioning of the method relies on the choice of some number of a parameter such as the k parameter represents the number of neighbors chosen to assign the new element to the class and the distance used.

### III. DEEP LEARNING

Deep learning (DL) is one of the numerous strategies found within machine learning (ML) as shown in Figure 1, where ML [21] is a discipline of artificial intelligence that ensures the software estimate results with better accuracy, without the need to write explicit codes to perform the task mentioned. DL methods are utilized in ML in terms of quick learning and implementation of large and complex data. DL is widely utilized in numerous software disciplines for example computer vision, speech and sound processing, bioinformatics, computer games, search engines, manufacturing, online advertising, and financing, etc. It is realized that DL provides highly successful results in processes of estimation and classification.

DL describes a bunch of computational models composed of many layers of data processing, which make it conceivable to learn by representing these data through several levels of abstraction [22] from a large amount of training data, these models discover recurrent structures by automatically refining their interior parameters via a backpropagation algorithm as shown in Figure 2. Each layer of the network transforms the signal nonlinearly to increase the selectivity and invariance of the representation. With a sufficient number of layers, the network can generate a hierarchy of representations that will make the model both sensitive to very small details and

insensitive to large variations. The classification issue is an important component in the field of deep learning since it is focused on judging a new sample that belongs to which predefined sample category, according to a train set containing a certain number of known samples. The classification problem is also called supervised classification, since all samples in the train set are labeled, and all categories are predefined.

The output is defined by the following formula in (2):

$$Y = f(\sum_j w_j x_j + b) \quad (2)$$

Where  $w_j$  is the network weights,  $b$  is a bias term, and  $f$  is a specified activation function. Figure 3 shows a natural extension of this simple model is attained by combining multiple neurons to form a so-called hidden layer.

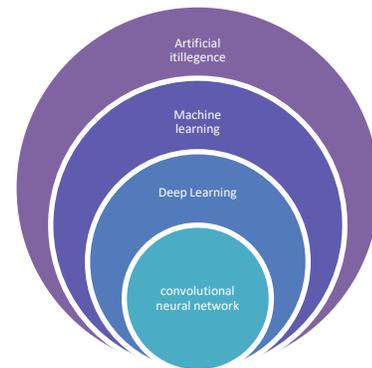


Fig. 1. The Relationship between Artificial Intelligence, Machine Learning, Deep Learning, and Artificial Neural Networks.

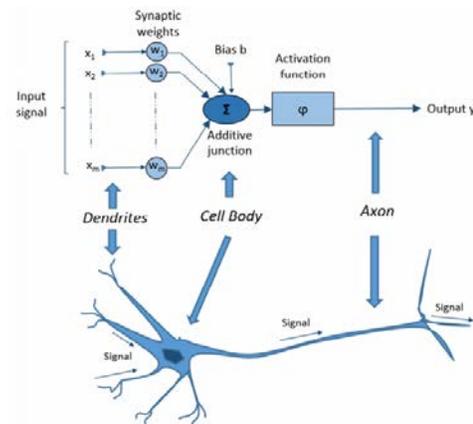


Fig. 2. The Analogy between an Artificial Neuron and a Biological Neuron. X Represents the Inputs, the Bias b, the Activation Function  $\phi$ , and Weights w are Adjusted Automatically by the Network.

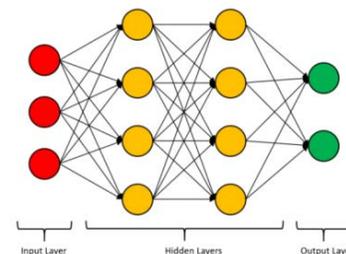


Fig. 3. Representation of Layers of Deep Learning.

#### IV. FEATURE SELECTION

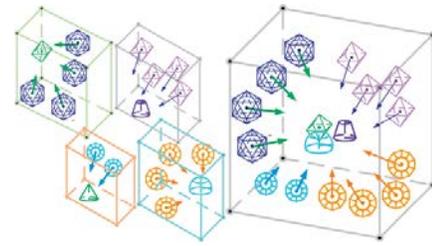
Feature selection (FS) is a pre-processing method that has been demonstrated to significantly affect the performance of the data mining techniques [23] (e.g. classification) in terms of either the quality of the extracted patterns or the running time required to analyze the complete dataset. It reduces the number of features, removes irrelevant, redundant, or noisy features, and brings about palpable effects for applications: speeding up a data mining algorithm, improving learning accuracy, and leading to better model comprehensibility's methods are arranged into filters and wrappers [24]. While a learning algorithm (e.g. classification) is approached by the wrapper in the evaluation of the feature subset, filters rely on the data itself to evaluate the feature subset using designated methods (e.g. information gain) [25].

Searching for an ideal subset of features is a major challenge when solving feature selection problems. The primary target when selecting a feature is to find a set of  $M$  features from an original set of  $N$  where  $M < N$  without information lose. Therefore, an impractical approach to this problem is to create all possible subsets. If the dataset includes  $N$  features, then there will be  $2^N$  subsets to be generated and evaluated, which are considered computationally expensive tasks [23]. This paper introduces Dragonfly as a feature selection and studies its effect on accuracy.

##### A. Dragonfly Algorithm (DA)

Dragonfly is an open-source python library for scalable Bayesian optimization. Bayesian optimization is utilized for optimizing black-box functions whose evaluations are usually expensive. Beyond vanilla optimization techniques, DA provides an array of tools to scale up Bayesian optimization to expensive large-scale problems. These include features that are especially suited for high dimensional optimization, parallel evaluations in synchronous or asynchronous settings which means conducting multiple evaluations in parallel, multi-fidelity optimization which using cheap approximations to speed up the optimization process, and multi-objective optimization which optimizing multiple functions simultaneously. It is compatible with Python2 ( $\geq 2.7$ ) and Python3 ( $\geq 3.5$ ) and has been tested on Linux, Mac OS, and Windows platforms.

DA is a recently well-established population-based optimizer proposed by Mirjalili in 2016 [26]. The hunting and migration strategies of dragonflies are the base of the DA algorithm. The hunting method is known as a static swarm (feeding), in which all members of a swarm can fly in small clusters over a limited space for discovering food sources. Dynamic swarming is considered the migration strategy of dragonflies (migratory). In this phase, the dragonflies are eager to take off in bigger clusters, and as a result, the swarm can migrate. Dynamic and static groups are shown in Figure 4. Moreover, in other swarm-based methods, the operators of DA perform two main concepts: intensification, encouraged by the dynamic swarming activities, and diversification, motivated by the static swarming activities.



(a) Static Swarm. (b) Dynamic Swarm.  
Fig. 4. Dynamic and Static Dragonflies.

Five behaviors characterize DA, where  $X$  is the position vector,  $X_j$  is the  $j$ -th neighbor of the  $X$ , and  $N$  denotes the neighborhood size:

Separation: dragonflies use this strategy to separate themselves from other agents. This procedure is formulated as (3):

$$S_i = \sum_{j=1}^N X - X_i \quad (3)$$

Alignment: shows how an agent will set its velocity to the velocity vector of other adjacent dragonflies. This concept is modeled based on (4) Where  $V_j$  indicates the velocity vector of the  $j$ -th neighbor:

$$A_i = \frac{\sum_{j=1}^N V_j}{N} \quad (4)$$

Cohesion: shows members' inclination to move in the direction of the nearest mass center. This step is formulated as in (5):

$$C_i = \frac{\sum_{j=1}^N X_j}{N} - X \quad (5)$$

Attraction: illustrates the propensity of members to step towards the food source. The attraction tendency among the food source and the  $i$ -th agent is performed based on (6) Where  $F_{loc}$  is the food source's location:

$$F_i = F_{loc} - X \quad (6)$$

Distraction: illustrates the proclivity of dragonflies to keep themselves away from a conflicting enemy. The distraction among the enemy and the  $i$ -th dragonfly is performed according to (7) Where  $E_{loc}$  is the enemy's location:

$$E_i = E_{loc} + X \quad (7)$$

In DA, the fitness of food source and position vectors are updated based on the fittest agent found so far. Moreover, the fitness values and positions of the enemy are calculated based on the worst dragonfly. This fact will help DA converge in the solution space towards more promising regions and in turn, avoid non-promising areas. The position vectors of dragonflies are updated based upon two rules: the position vector and the step vector ( $X$ ). The step vector indicates the dragonflies' direction of motion and it is calculated as in (8):

$$X_{t+1} = (sS_i + aA_i + cC_i + fF_i + eE_i) + wX_t \quad (8)$$

Where  $s$ ,  $w$ ,  $a$ ,  $c$ ,  $f$ , and  $e$  show the weighting vectors of different components. The location vector of members is calculated as in Eq. (9), where  $t$  is iteration:

$$X_{t+1} = X_t + X_{t+1} \quad (9)$$

The pseudo-code of the DA algorithm is given in Algorithm 1 as follows:

```

Initialize the population  $X_i$  ( $i = 1, 2, \dots, n$ )
Initialize  $\Delta X_i$  ( $i = 1, 2, \dots, n$ )
while ( $t < \text{Max\_Iteration}$ )
    Evaluate each dragonfly
    Update (F) and (E)
    Update the main coefficients(i.e.,  $w$ ,  $s$ ,  $a$ ,  $c$ ,  $f$ , and  $e$ )
    Calculate  $S$ ,  $A$ ,  $C$ ,  $F$ , and  $E$ (using Eqs. (3) to (7))
    Update step vectors using Eq. (8)
    Calculate  $T(\Delta X)$  using Eq. (9)
    Update  $X_{t+1}$  using Eq. (8)
    Return the best agent
End while
    
```

## V. EXPERIMENTAL DISCUSSION

The data is split into a training set (80%), testing set (10%), and validation sets (10%) several times, and a Cross-Validation (CV) approach was utilized to evaluate the accuracy, sensitivity, and specificity of each of the classifiers with five folds.

### A. Model

The proposed model in this study is represented in a block diagram as shown in Figure 5 explaining the process conducted within the model. It is planned with three phases first of them utilizing traditional classifiers for example SVM, NB, RF, and KNN, secondly applying deep learning for enhancing the accuracy of the detection of breast cancer, finally applying the principle of feature selection using DA with deep learning classification to improve the performance.

### B. Missing Dataset Technique

The training of a model with a dataset containing missing values may significantly influence the quality of the deep learning model. For this reason, the utilization of WBCD in training was ensured by the correction of 16 incorrect data found with statistical missing value analysis. There are two techniques in handling the missing data: The mean Imputation technique and Missing Data Ignoring Technique. Mean Imputation technique works by calculating the mean value of readily available values in a column and then substituting the missing values in each column independently from each other [27]. Missing Data Ignoring Technique simply deletes the cases that contain missing data.

### C. Normalization of Dataset

A normalization process between the ranges of 0-1 was applied in the data set for eliminating the long learning time caused by the size of the data set. The MinMaxScaler method was used in this process as shown in (1).

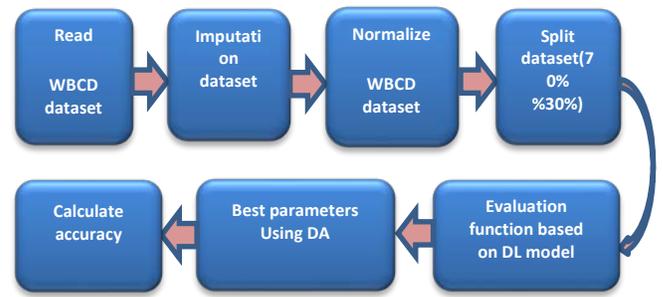


Fig. 5. Block Diagram of the Model.

### D. Splitting the Dataset

The data used in experiments are separated into two groups as training and testing using (train\_test\_split) library in python. The allocation of available data among these three data sets is vital for the objectivity of success. Because of different tests, the data set in the suggested model was allocated as 80% (559 data) for training, 20% (140 data) for testing and validating. The process of allocation is shown in Figure 6. The cross-validation method was utilized in the implementation of this process [28].

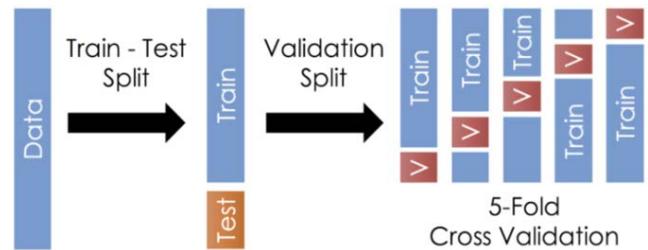


Fig. 6. Splitting Dataset using Cross-validation.

### E. Neural Network Model

Any neural network (NN) model has multiple parameters that control its performance for example number of hidden layers, number of nodes in each layer, the type of activation function, number of epochs, and batch size.

### F. Epoch

The NN learns the patterns of input data by reading the input dataset and applying various calculations to it. However, it does not make that only once, it learns, over and over, utilizing the input dataset and learning outcomes from the previous trials. An epoch is a process of learning from the input dataset in each trial. Expanding the number of epochs doesn't generally imply that the network will give better results, it may cause overfitting. Using the trial-and-error method, several epochs were chosen until the outcomes still the same after a very few cycles.

### G. Activation Functions of the Neural Network

The activation functions used in the layers of the created neural network are described as follows:

1) *Rectified Linear Unit (ReLU)*: ReLU activation function is utilized in the input layer and hidden layers of the neural network. ReLU as seen in Figure 7 is an activation

function that recently gained popularity for its practicality in deep learning. It enables the neural network to learn faster [21]. The numerical expression of the function is provided in (10).

$$f(x) = \max(0, x) \tag{10}$$

2) *Sigmoid activation function*: The sigmoid activation function is used in the output layer of the neural network. It is a function that gets a value between the ranges of (0, 1) as seen in Figure 8. The numerical expression of the function is given in (11).

$$\sigma(x) = \frac{1}{1 + \exp(-x)} \tag{11}$$

3) *Softmax activation function*: The Softmax is a function that turns a vector of K real values into a vector of K real values that sum to 1. The input values can be positive, negative, zero, or greater than one, but the Softmax transforms them into values somewhere in the range 0 and 1 as shown in Figure 9, so that they can be interpreted as probabilities. Large multi-layer neural networks end in a penultimate layer that outputs real-valued scores that are not efficiently scaled and which makes working with them complicated. In the current study, the Softmax is very helpful as it turns the scores into a normalized probability distribution. Consequently, it is normal to append a Softmax function as the final layer of the neural network.

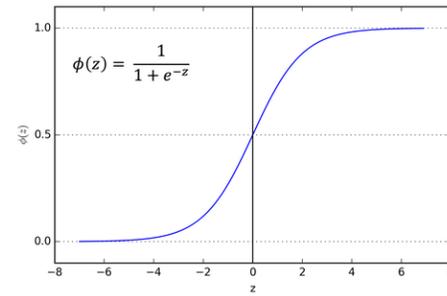


Fig. 9. Softmax Activation Function.

### H. Dropout

Dropout is one of the methods that are utilized to prevent memorization. In each iteration, it randomly removes some neurons from a layer at a specified rate. The process of dropout is shown in Figure 10. They dropped the crossed units out of the network.

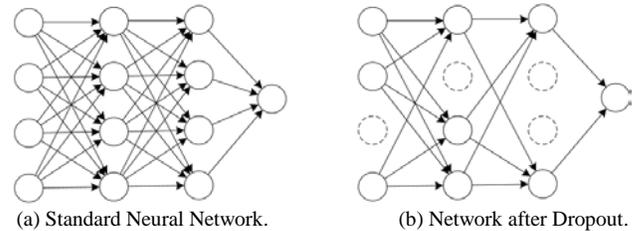


Fig. 10. Dropout Neural Network Model. (a) A Standard Neural Network. (b) After the Dropout is Applied, the Same Network. Dotted Lines Indicate a Node that has been Dropped.

### I. Optimization

Optimization is a basic issue in the learning process in deep learning applications. Its techniques are utilized to find the optimum value in solving non-linear problems. RMSprop, adagrad, adadelta, adam, adamax. Moreover, there are differences between each of these algorithms in terms of performance and speed. In this study, the optimization algorithm of Adaptive Moment Optimization (Adam) was applied.

### J. Loss Function

The loss function is a type of function that measures both the error rate and performance of a designed model. In DL, the last layer of a NN is the layer where the loss of function is defined. In DL applications, the function calculates the dissimilarity between the estimation of the designed model and the required real value. In case that a model with good estimation capability is designed, the difference between the real value and estimated value will be lower. An output of a higher loss value indicates that the designed model contains defects. In the literature, there are various loss functions such as mean squared error, mean absolute percentage error, mean squared logarithmic error, hinge, logcosh, sparse categorical cross-entropy, binary cross-entropy, kullback, poisson, and many others. In this study, the meager straight out cross-entropy misfortune work was utilized.

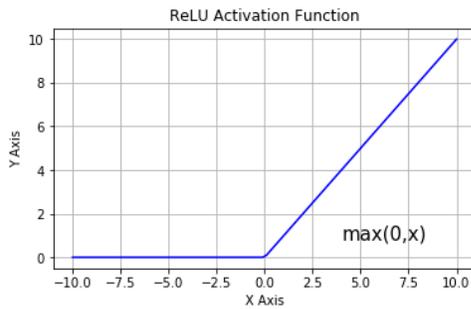


Fig. 7. Relu Activation Function.

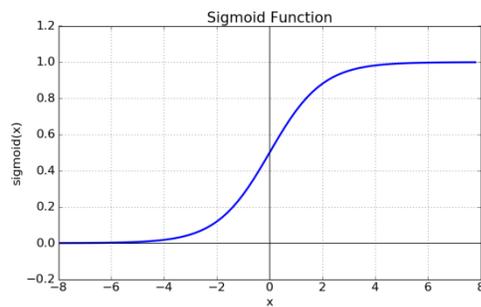


Fig. 8. Sigmoid Function Activation.

### K. Early Stopping

In the models where training is made by iteration with data, the duration of learning must be terminated at the right time. Otherwise, if training is not stopped, all of the samples in the data set for training will be memorized by the system. These outcomes in a decrease in the capability of estimation of unknown samples. In case of early termination, the performance of the system will decline in that it could not fully analyze the data. The same outcome will also arise in the case of over-training. In case of an overfitting possibility for the program, a parameter of early stopping was defined; the training will be stopped regardless of the number of iterations.

## VI. RESULTS AND DISCUSSION

In this section, performance evaluation is discussed using accuracy which is used as the percentage of correct predictions. Table 1 shows the comparative study of different classifiers which easily analyses KNN, RBF, SVM, and NB. Some experiments handled missing data by Mean Imputation technique and others by Missing Data Ignoring Technique. It declares that RF gives a better result when using 10 trees, and KNN with 3 neighbors which reduces the complexity of the model and consumes less processing time. PCA+SVM with RBF kernel when using missing data ignoring technique considered as a better classifier as compared to others which achieved 99%.

### A. Deep Learning Usage with the Dataset

The proposed model utilizes two layers at the start, then eventually experiments with more layers which have been observed that the convergence time is larger for deeper networks. Many parameters control the deep learning model. One of them is the number of hidden layers, if data is less complex and is having fewer features then neural networks with 1 to 2 hidden layers will work, but if data is having large features, so to get an optimum solution, 3 to 5 hidden layers can be used. It should be noticed that increasing hidden layers will also increase the complexity of the model which may sometimes lead to overfitting. Another one is the number of hidden neurons; it should be between the size of the input layer and the size of the output layer. It may be 2/3 the size of the input layer, plus the size of the output layer and it should be less than twice the size of the input layer [29]. The experiments are based on using batch size 16 and 9 neurons in each layer; the result is as shown in Table 2.

As shown above, in Table 2, the best accuracy achieved is 99.3% with 2 hidden layers and epochs 2000 while the accuracy reduces to 99% with 250 epochs only. More epochs mean more iteration and more consumption of time and resources. However, the difference in accuracy is not significantly considerable to endure more time consumption. Also, the same accuracy level of 99.3% is attained using 4 hidden layers and only 100 epochs. Besides, plots of the characteristic of the 4 hidden layers model are shown in Figure 11. In graph (a) the training accuracy visibly increases over time, until it reaches nearly 95%, while the validation accuracy reaches a plateau at a range of 98–99.3% after 21 epochs. Moreover, the validation loss, presented in a graph (b), reaches its minimum after 50 epochs and then halts, while the training loss keeps decreasing exponentially until it drops to nearly 0.

TABLE I. RESULTS OF TRADITIONAL CLASSIFIERS

classifier	Missing values	PCA	accuracy
RF (100)	Mean		97
RF (10)	Mean		95
RF (10)	Mean	1	<b>98</b>
RF (100)	Mean	1	98
RF (10)	Remove		98
RF (100)	remove		95
KNN (10)	Mean	1	97
KNN (3)	Mean	1	<b>98</b>
KNN (3)	Remove		96
NB	Mean	1	97
Svm (rbf)	Remove	1	<b>99</b>
Svm (rbf)	Mean		96
Svm (rbf)	Remove		97
Svm (rbf)	Mean	1	98
Svm (linear)	Mean	1	97

TABLE II. DEEP LEARNING RESULTS

Number Of layers	Epochs	Activation functions	Dropout	accuracy
2	250	Sigmoid,Softmax	0.5	<b>99</b>
2	100	Sigmoid,Softmax	0.3	98.54
2	100	Sigmoid,Softmax	0.5	97.85
2	2000	Relu,Sigmoid		<b>99.3</b>
3	150	Sigmoid,Sigmoid,Softmax	0.3	98
3	150	Relu,Relu,Softmax	0.3	97
3	250	Relu,Relu,Softmax	0.3	97.08
3	1000	Relu,Relu,Softmax	0.3	97.08
3	100	Relu,Sigmoid,Softmax	0.5	<b>98.54</b>
3	100	Relu,Sigmoid,Softmax	0.3	97.8
4	250	Sigmoid,Sigmoid,Sigmoid,Softmax	0.5	99
4	1000	Sigmoid,Sigmoid,Sigmoid,Softmax	0.3	98.5
4	100	Sigmoid,Sigmoid,Sigmoid,Softmax	0.3	<b>99.3</b>
4	150	Sigmoid,Sigmoid,Sigmoid,Softmax	0.3	97.08
4	150	Sigmoid,Softmax,Softmax,Softmax	0.3	98.54
5	15	Sigmoid,...,softmax		93.3
5	15	Softmax,...,softmax		94.3
5	20	Softmax,...,softmax		95.2
5	250	Sigmoid,...,softmax	0.25	96

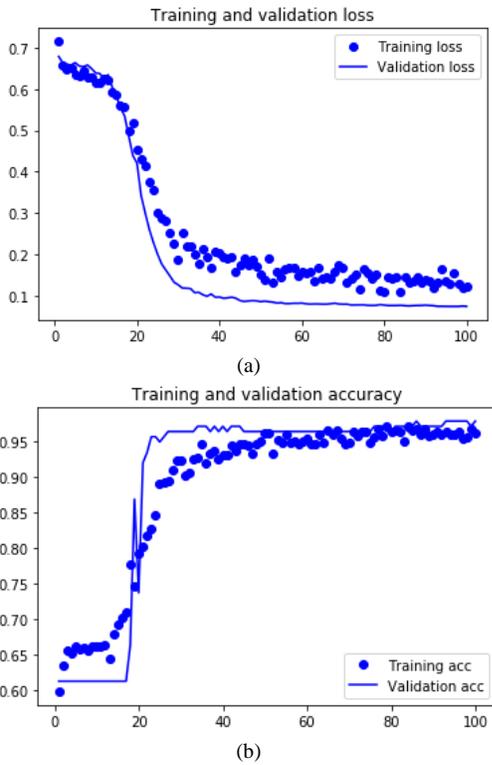


Fig. 11. (a) Training vs Validation Loss, (b) Training vs Validation Accuracy of 4 Hidden Layers Model with 100 Epochs.

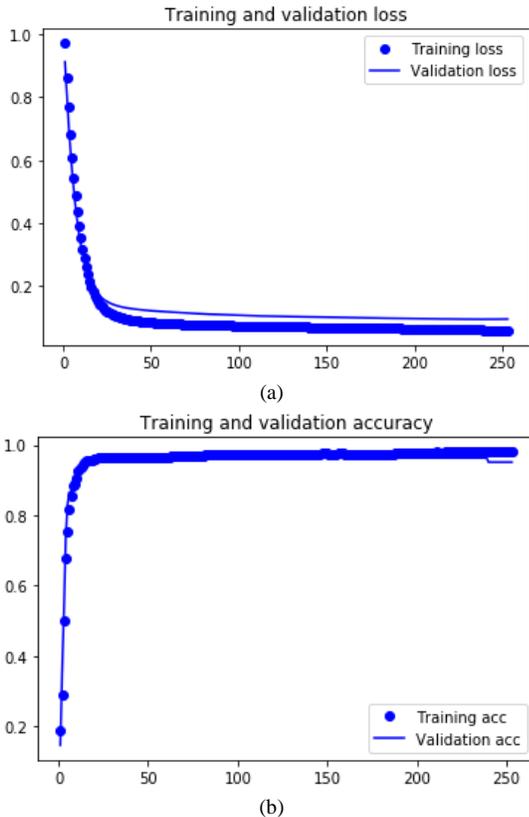


Fig. 12. Two Hidden Layers Model with 2000 Epoch, (a) Training vs Validation Loss (b) Training vs Validation Accuracy.

The characteristics of the 2 hidden layers model are shown in Figure 12, where graph (a) explains the behavior of the training and validation loss and graph (b) presents the accuracy. The validation loss clearly reaches its minimum after 200 epochs and then halts, while after 250 epochs keep decreasing exponentially and reach the minimum value for nearly 0 then it is steady-state. Also, the training and validation accuracy increases linearly until 30 epochs, and then it reaches nearly 100%.

After applying feature selection using DA with deep learning, the results are shown in Table 3. As noticed in Table 3, it gives the best result is 97.907% when choosing 20 population, 100 iteration, and 100 epochs which recommended five attributes as the most important (uniformity of cell size, uniformity of cell shape, bare nuclei, bland chromatin, and mitosis). These ML methods have been chosen because the results obtained from these methods have appeared to be more accurate than traditional classifiers. In addition to implementing these ML techniques for bigger data in the future will be at a faster rate. The main focus is to choose the most suitable classifier model for obtaining the highest accuracy and to find an improvement of similar previous works on the same database.

TABLE III. DEEP LEARNING MIXED WITH DA RESULTS

folds	population	iteration	epoch	features	Number of features	Activation function	accuracy
5	10	100	100	110011001	5	Relu,Sigmoid	96.52
5	20	100	100	011001010	4	Relu,Sigmoid	97.43
10	10	100	100	110011000	4	Relu,Sigmoid	96.69
10	20	100	100	111001000	4	Relu,Sigmoid,Softmax	97.619
10	30	150	100	111011001	6	Relu,Sigmoid	97.62
10	20	100	1000	110001001	4	Relu,Sigmoid, Sigmoid,Softmax	97.818
5	20	100	200	101001111	6	Sigmoid,Softmax,Softmax,Softmax <b>Dropout=0.25</b>	97.256
10	20	100	100	101001011	5	Softmax,Softmax,Softmax,Softmax	<b>97.907</b>
10	20	100	100	001001001	3	Sigmoid,Sigmoid,Softmax <b>Dropout=0.5</b>	96.71
10	20	100	100	110101011	6	Relu,Sigmoid	96.89
10	20	100	1000	100111011	6	Relu,Sigmoid, Sigmoid	97.49

## VII. CONCLUSION

Breast cancer prediction is very significant in the area of Medicare and Biomedical. This study aims to enhance the accuracy of the diagnosis of breast cancer with the deep learning method. Analysis of WBCD with traditional classifiers such as NB, SVM, KNN, and RF achieved high accuracy. Proposed a model that predicts breast cancer based on a deep investigation in the performance of different deep

networks on this dataset. It has been implemented by Python to be the most effective in classifying the diagnostic data set into the two classes because of the seriousness of cancer; it's found that the accuracy of the proposed model ranges between 93.5% and 99.3%. In the case of the two hidden layers model, the highest outcomes result with 250 and 2000 epochs are 99% and 99.3% respectively. The same result might be obtained with four hidden layers models and 100 epochs. It is noticed that DL hybrid with DA as a feature selection model achieved an accuracy of 97.907%. Such comparative analysis of breast cancer classification would provide insights on the efficient approaches for the detection of cancer problems.

### VIII. FUTURE WORK

The proposed model is applied to numerical data only. It would be interesting to see its behavior when it is applied to different types of data available in the medical field such as mammograms. In the future, the research may be carried out for a screening of features to diagnose breast cancer tumors.

#### REFERENCES

- [1] S. Chopra and E. L. Davies, "Breast cancer," *Med. (United Kingdom)*, vol. 48, no. 2, pp. 113–118, 2020, doi: 10.1016/j.mpmed.2019.11.009.
- [2] B. Sahu, S. Mohanty, and S. Rout, "A Hybrid Approach for Breast Cancer Classification and Diagnosis," *ICST Trans. Scalable Inf. Syst.*, vol. 0, no. 0, p. 156086, 2018, doi: 10.4108/eai.19-12-2018.156086.
- [3] M. Paredes, "Can Artificial Intelligence help reduce human medical errors? Two examples from ICUs in the US and Peru," vol. 2009, pp. 1–12, 2018, [Online]. Available: <https://techpolicyinstitute.org/wp-content/uploads/2018/02/Paredes-Can-Artificial-Intelligence-help-reduce-human-medical-errors-DRAFT.pdf>.
- [4] Dr. William H. Wolberg, "UCI Machine Learning Repository: Breast Cancer Wisconsin (Original) Data Set." <https://archive.ics.uci.edu/ml/datasets/Breast+Cancer+Wisconsin+%28Original%29> (accessed Dec. 16, 2020).
- [5] S. Aruna, S. P. Rajagopalan, and L. V. Nandakishore, "Knowledge Based Analysis of Various Statistical Tools in Detecting Breast Cancer," *Comput. Sci. Inf. Technol.*, vol. 2, pp. 37–45, 2011, doi: 10.5121/csit.2011.1205.
- [6] K. Polat and S. Güneş, "Breast cancer diagnosis using least square support vector machine," *Digit. Signal Process. A Rev. J.*, vol. 17, no. 4, pp. 694–701, Jul. 2007, doi: 10.1016/j.dsp.2006.10.008.
- [7] A. F. M. Agarap, "On breast cancer detection: An application of machine learning algorithms on the Wisconsin diagnostic dataset," *ACM Int. Conf. Proceeding Ser.*, no. 1, pp. 5–9, 2018, doi: 10.1145/3184066.3184080.
- [8] H. Asri, H. Mousannif, H. Al Moatassime, and T. Noel, "Using Machine Learning Algorithms for Breast Cancer Risk Prediction and Diagnosis," *Procedia Comput. Sci.*, vol. 83, no. Fams, pp. 1064–1069, 2016, doi: 10.1016/j.procs.2016.04.224.
- [9] P. S. Kohli and A. L. Regression, "2020 IEEE 5th International Conference on Computing Communication and Automation, ICCCA 2020," 2020 IEEE 5th Int. Conf. Commun. Autom. ICCCA 2020, pp. 1–4, 2020.
- [10] K. B. Nahato, K. N. Harichandran, and K. Arputharaj, "Knowledge mining from clinical datasets using rough sets and backpropagation neural network," *Comput. Math. Methods Med.*, vol. 2015, no. April, 2015, doi: 10.1155/2015/460189.
- [11] S. AhmedMedjahed, T. Ait Saadi, and A. Benyettou, "Breast Cancer Diagnosis by using k-Nearest Neighbor with Different Distances and Classification Rules," *Int. J. Comput. Appl.*, vol. 62, no. 1, pp. 1–5, 2013, doi: 10.5120/10041-4635.
- [12] M. M. Islam, H. Iqbal, M. R. Haque, and M. K. Hasan, "Prediction of breast cancer using support vector machine and K-Nearest neighbors," 5th IEEE Reg. 10 Humanit. Technol. Conf. 2017, R10-HTC 2017, vol. 2018-Janua, no. February 2018, pp. 226–229, 2018, doi: 10.1109/R10-HTC.2017.8288944.
- [13] H. Singh, *Practical Machine Learning with AWS*. 2021.
- [14] J. D. Hunter, "Matplotlib: A 2D graphics environment," *Comput. Sci. Eng.*, vol. 9, no. 3, pp. 90–95, 2007, doi: 10.1109/MCSE.2007.55.
- [15] S. Van Der Walt, S. C. Colbert, and G. Varoquaux, "The NumPy array: A structure for efficient numerical computation," *Comput. Sci. Eng.*, vol. 13, no. 2, pp. 22–30, 2011, doi: 10.1109/MCSE.2011.37.
- [16] H. Li and D. Phung, "Journal of Machine Learning Research: Preface," *J. Mach. Learn. Res.*, vol. 39, no. 2014, pp. i–ii, 2014.
- [17] L. Vig, "Comparative Analysis of Different Classifiers for the Wisconsin Breast Cancer Dataset," *OALib*, vol. 01, no. 06, pp. 1–7, 2014, doi: 10.4236/oalib.1100660.
- [18] Y. Qu, G. Ostrouchov, N. Samatova, and A. Geist, "Principal Component Analysis for Dimension Reduction in Massive Distributed Data Sets," *Work. High Perform. Data Min. Second SIAM Int. Conf. Data Min.*, no. June 2014, pp. 4–9, 2002.
- [19] N. Varghese, "A Survey Of Dimensionality Reduction And Classification Methods," *Int. J. Comput. Sci. Eng. Surv.*, vol. 3, no. 3, pp. 45–54, 2012, doi: 10.5121/ijcses.2012.3304.
- [20] V. Saravanan and R. Mallika, "An effective classification model for cancer diagnosis using micro array Gene expression data," *Proc. - 2009 Int. Conf. Comput. Eng. Technol. ICCET 2009*, vol. 1, pp. 137–141, 2009, doi: 10.1109/ICCET.2009.38.
- [21] İ. Yıldız and A. T. Karadeniz, "Enhancement Of Breast Cancer Diagnosis Accuracy With Deep Learning," *Eur. J. Sci. Technol.*, no. October, pp. 452–462, 2019, doi: 10.31590/ejosat.638428.
- [22] Y. Bengio, *Learning deep architectures for AI*, vol. 2, no. 1. 2009.
- [23] M. M. Mafarja, D. Eleyan, I. Jaber, A. Hammouri, and S. Mirjalili, "Binary Dragonfly Algorithm for Feature Selection," *Proc. - 2017 Int. Conf. New Trends Comput. Sci. ICTCS 2017*, vol. 2018-Janua, pp. 12–17, 2017, doi: 10.1109/ICTCS.2017.43.
- [24] H. (National U. of S. Liu, H. (Osaka U. Motoda, R. Setiono, and Z. Zhao, "Feature Selection : An Ever Evolving Frontier in Data Mining," *J. Mach. Learn. Res. Work. Conf. Proc. 10 Fourth Work. Featur. Sel. Data Min.*, pp. 4–13, 2010.
- [25] C. S. Yang, L. Y. Chuang, Y. J. Chen, and C. H. Yang, "Feature selection using memetic algorithms," *Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008*, vol. 1, pp. 416–423, 2008, doi: 10.1109/ICCIT.2008.81.
- [26] M. Mafarja, A. A. Heidari, H. Faris, S. Mirjalili, and I. Aljarah, *Dragonfly algorithm: Theory, literature review, and application in feature selection*, vol. 811. Springer International Publishing, 2020.
- [27] Q. Song and M. Shepperd, "Missing data imputation techniques," *Int. J. Bus. Intell. Data Min.*, vol. 2, no. 3, pp. 261–291, 2007, doi: 10.1504/IJBIDM.2007.015485.
- [28] D. Berrar, "Cross-validation," *Encycl. Bioinforma. Comput. Biol. ABC Bioinforma.*, vol. 1–3, no. April, pp. 542–545, 2018, doi: 10.1016/B978-0-12-809633-8.20349-X.
- [29] F. S. Panchal and M. Panchal, "International Journal of Computer Science and Mobile Computing Review on Methods of Selecting Number of Hidden Nodes in Artificial Neural Network," *Int. J. Comput. Sci. Mob. Comput.*, vol. 3, no. 11, pp. 455–464, 2014, [Online]. Available: [www.ijcsmc.com](http://www.ijcsmc.com).

# Using Machine Learning Technologies to Classify and Predict Heart Disease

Mohammed F. Alrifaie<sup>1</sup>, Zakir Hussain Ahmed<sup>2</sup>, Asaad Shakir Hameed<sup>3</sup>, Modhi Lafta Mutar<sup>4</sup>

Computer Engineering Department, Faculty of Engineering, Karabuk University, Karabuk, Turkey<sup>1</sup>

Department of Information and Communications, Basra University College of science and technology, Basrah, Iraq<sup>1</sup>

Department of Mathematics and Statistics, College of Science, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Kingdom of Saudi Arabia<sup>2</sup>

Faculty of Information and Communication Technology Universiti Teknikal Malaysia Melaka Hang Tuah Jaya Durian Tunggal, Melaka, Malaysia<sup>3</sup>

Department of Mathematics, General Directorate of Thi-Qar Education, Ministry of education, Thi-Qar, Iraq<sup>3</sup>

Faculty of Information and Communication Technology Universiti Teknikal Malaysia Melaka Hang Tuah Jaya Durian Tunggal, Melaka, Malaysia<sup>4</sup>

Department of Mathematics, General Directorate of Thi-Qar Education, Ministry of education, Thi-Qar, Iraq<sup>4</sup>

**Abstract**—The techniques of data mining are used widely in the healthcare sector to predict and diagnose various diseases. Diagnosis of heart disease is considered as one of the very important applications of these systems. Data is being collected today in a large amount where people need to rely on the device. In recent years, heart disease has increased excessively and heart disease has become one of the deadliest diseases in many countries. Most data sets often suffer from extreme values that reduce the accuracy percentage in classification. Extreme values are defined in terms of irrelevant or incorrect data, missing values, and the incorrect values of the dataset. Data conversion is another very important way to preconfigure the process of converting data into suitable mining models by acting assembly or assembly and filtering methods such as eliminating duplicate features by using the link and one of the wrap methods, and applying the repeated discrimination feature. This process is performed, dealing with lost values through the "Remove with values" methods and methods of estimating the layer. Classification methods like Naïve Bayes (NB) and Random Forest (RF) are applied to the original datasets and data sets with the feature of selection methods too. All of these operations are implemented on three various sets of heart disease data for the analysis of pre-treatment effect in terms of accuracy.

**Keywords**—Classification; Naive Bayes (NB); (Support Vector Machine SVM); Random Forest; machine learning

## I. INTRODUCTION

Nowadays one of the major causes of death is heart disease at the present time. The heart disease prediction system can support healthcare specialists in predicting heart condition based on the clinical data of patients that has been pre-entered into the system. There are several healthcare manufactures and hospitals which gather massive amounts of data for patients which are hard to deal with current systems [5]. There are a lot of tools that use prediction algorithms are available nonetheless they have several weaknesses [15,16]. Many of the tools cannot deal with large data. Actually, there are a lot of algorithms can be used to find and predict the heart disease such as the discrete differential evolution (DDE) algorithm [17]. Machine learning algorithm acts an important role in

extracting hidden knowledge and information and analyzing it from these data sets. Actually, it improves speed and accuracy. Data extraction techniques have been used in many areas, including health care. This paper aims to check whether the prediction of heart disease can be depended on data mining and machine learning [9]. By using some techniques of data mining, Prediction helps detect if a patient suffers of heart disease or not. In addition, the prediction helps specialists to get to the appropriate diagnosis more quickly, not only that, but it increases the accuracy of diagnosis leading to better results may help to reduce or reduce heart attacks at the very least. Hidden relationships can untangle and diseases are diagnosed efficiently by the help of Data mining along with soft computing techniques [7,8]. The datasets are collected and gathered from the Machine Learning Repository (UCI). It now upholds 394 datasets copies with 14 attributes those names are sex, age, chest pain type, resting blood pressure, resting electrocardiographic results, fasting blood sugar >120 mg / dl, serum cholesterol in mg/dl, exercise induced angina, maximum heart rate achieved, the slope of the peak exercise ST segment, oldpeak = ST depression caused by exercise relative to rest, number of main vessels (0-3) colored by flourosopy, thal: 7 = reversible defect; 6 = fixed defect; 3 = normal. These features are used as a service package to the MLC (community of machine learning). There are 3 data bases in the Data Set of heart disease, these data bases namely Cleveland, Hungary, Switzerland. In this paper, we analyze cardiology data based on Dataset by using the link and one of the wrap methods, and applying the repeated discrimination feature. This process is performed, dealing with lost values through the "Remove with values" methods and methods of estimating the layer. However, the outline of this paper as follows, starts from the literatures to analyze the previous studies about classification and the used algorithms in this area. Then we discuss our methodology by elaborating the procedure of the work and the application of the algorithms. In result section we illustrate the obtained results and discuss it. Finally, we summarize our work in conclusion section and future work.

## II. LITERATURE SURVEY

There are a lot of common data mining algorithms, particularly the techniques of classification, each of them is distinguished by both excellence and weakness, for example three of which are: Decision Tree, k-Nearest Neighbor (KNN), and Naïve Bayes and [10]. Naive Bayes technique is a powerful, simple and good performance of classification. Basically, it depends on Paez's theory of the probability of  $P(c|x)$  from the previous possibility of  $P(c)$ , the possibility of the given  $P(x|c)$  and the predictability probability as follows [10,11].

$$P(c|x) = \frac{P(x|c)P(c)}{P(x)} \quad (1)$$

The Bayesian Naive model is commonly used in many areas such as medical diagnosis, spam filtering, and even text classification. It gets a lot of attention among statisticians resulting in algorithm modifications. At the same time, Decision Tree algorithms (DT) can be, also it is fast in clear modeling and training. DT mechanism is by sorting the trained data in a form of tree. In the training phase, this tree is formed to determine the accuracy of the workbook for the test data. Then it will be categorized by using the tree [12].

On the other hand, we have k-nearest neighbors KNN. It is a simple technique of classification that is often used in several studies, particularly when there is little or no data distribution information. KNN is a non-deterministic algorithm, which means that it does not put assumptions about the data's distribution that is used in the analysis. KNN fits into practical environments, since data are often not followed by real theoretical statistics such as natural distribution. Lazy algorithm is also another name of KNN, or it uses only a quick training stage. It does not make circular which means that it keeps all data of training [13].

Many of researches were conducted to focus on heart diseases prediction and classification. Many data mining techniques are used for achieving and diagnosis various accuracy level of various methods [1]. The NB classifier algorithm uses conditional independence; the attribute value for a given category is believed to be independent of the values of other attributes. An example of an application of the Naïve Bayes algorithm is the proposed model for the prediction of high-risk heart disease. This application was introduced as part of the Web-based healthcare and detection package that is proposed by [2]. The data collected and prepared was considered as the training group as the work was based on two basic stages: the classification stage and the pre-processing which perform several tasks including: normalization, reduction, and cleaning of data, etc. On the other side, the second stage is the stage of prediction. In the prediction stage, the data are categorized into groups based on the type and nature of the disease, and then the establishment of a test group based on the questions of the disease. Finally send the results obtained from the prediction to the doctor.

The author in [2] proposed a Predicting heart disease model using neural network. The choice of feature is used for disease prediction. This method found a 100% accuracy of 15 features and precision of 92.5% for 13 features. There is an

improvement of 7.5% after giving up two advantages of 15 to 13.

The proposed method by [14] is used associative classification and selection of a subset of the risk of disease. They used asymmetric uncertainty, information acquisition, and genetic algorithm as measures to select the feature. Their method got 95% accuracy with the choice of hybrid feature. Heart disease data set gathered for experimental analysis with 11 features.

The author in [3] examines the performance for heart disease diabetes dataset by using several classification algorithms of machine learning like Decision Tree (J48), Naive Bayes (NB), and Support Vector Machine (SVM) with bagging technique. In order to measure the efficiency of the Classification algorithms they depend on the precision, accuracy, specificity, sensitivity, and performance. All of tests are achieved in the "WEKA TOOL", the results shown that Decision Tree (C4.5) provides a high quality of accuracy around (95.06%). [4] applied some of imputation methods for dealing with lost data. Imputation methods are algorithms designed to recover lost values of data, depending on other entered data in the data base. The choosing of the imputation effects on the performance of the machine learning's technology, for instance, it effects on the applied classification algorithm's accuracy. Thus, applying and selecting the correct calculation method is very important and commonly requires a great deal of human intervention. In this article, they suggested to using genetic programming techniques in order to seek for the correct mix of classification and imputation algorithms. They build the work based on the TPOT library of Python, and integrating a heterogeneous set of computing algorithms as part of the pipeline search of ML. They have shown that genetic programming can routinely find gradually enhanced pipelines that contain the most effective blend of feature pre-processing, classifiers, and imputation methods for a varied of classification difficulties with lost data.

The author in [6] checked various classification techniques in analysis heart disease. The classifiers like Naive Bayes, KNN, and Decision Tree are used to divide dataset. After the classification and evaluation of the performance they considered that the Decision Tree as the best classifier and the most efficient for heart disease analysis from the dataset.

## III. METHODOLOGY

Classification algorithms have been used in large data sets that are known for their study of layers and make prediction. Models store stored data sets in memory to predict. This model has the ability to predict the category label or the new data instance set [6]. So, this study used a classification algorithm under the supervision of Random Forest and Naïve Bayes to classify and predict heart disease.

In Random Forest for prediction, the accuracy is very important like healthcare fields especially when we talk about heart disease, the processing times can be used as a differentiation, while time-sensitive fields seek rapid predictions like the accuracy of the disaster prediction ratio that can also be used as a trade-off over time. This study shows the processing time and the accuracy percentage

differences between the selected variables of chosen dataset. However, the second used algorithm in this study is Naïve Bayes. It is a probability classification based on the theory of Bayes. All classifiers of Naïve Bayes suppose that the value of any given feature is an independent value of any other value, given the variable category. Bayes theory is:

$$P(C|X) = P(X|C) * P(C)/P(X) \tag{2}$$

Where X is the dataset, C refers to the class so that P(X) is a constant for all classes. Although it supposes an unrealistic condition that attributes values be conditional independent, they work amazingly well in big data sets where this condition is supposed and suspended.

The datasets are collected and gathered from the Machine Learning Repository (UCI). It now upholds 394 datasets copies with 14 attributes those names are sex, age, chest pain type, resting blood pressure, resting electrocardiographic results, fasting blood sugar >120 mg / dl, serum cholesterol in mg/dl, exercise induced angina, maximum heart rate achieved, the slope of the peak exercise ST segment, oldpeak = ST depression caused by exercise relative to rest, number of main vessels (0-3) colored by fluoroscopy, thal: 7 = reversible defect; 6 = fixed defect; 3 = normal. These features are used as a service package to the community of machine learning (MLC). There are three data bases in the Data Set of heart disease, these data bases namely Cleveland, Hungary, Switzerland.

#### IV. RESULT AND DISCUSSION

In this study, three data sets of heart diseases are first addressed to pre-processing of data to address missing values. The Heart Disease Group in Switzerland contains 123 cases with 14 features. In this data set, the chol attribute contains 99% of the lost values, while the ca attribute contains 95% of the missing values, while the fbs attribute contains 61% of the lost values, as it is shown in Table I.

In this paper, more than 60% of the lost values are subtracted to be removed. Therefore, the three attributes of the data set are removed, as it shown in Fig. 1.

Similarly, the Hungarian Heart Disease Data Collection contains 294 cases with 14 features. In this data set, the slope attribute contains 64% of the lost values, and the ca attribute contains 99% of the lost values and the thal attribute contains 90% of the lost values, as it shown in Fig. 2.

Thus, more than three attributes are exposed to removal from the data set and some of the features contain less than 60% of the lost values.

The other method of selecting the Recursion Mode provides a subset of features that produce an accurate result. The RF algorithm is used at each frequency to assess the form. The algorithm is designed to find out all of the probable subsets of attributes. It has given a set of Cleveland data set features for thal, Ca, thalach, slope, oldpeak, exang, cp and sex. Similarly, it has given oldpeak, trestbps, cp, thal, thalach, sex, exang, restecg and slope from the switzerland data set. Similarly, exang, oldpeak, cp, thalach, and sex were given from the Hungarian data collection of the classification. In pre-processing, 3 attributes are eliminated from Switzerland and also 3 attributes are removed from Hungarian datasets. In this research, two methods for selecting the feature, such as filter mode, are applied - the attributes associated with a high degree of removal and wrapping are identified. The way to remove the recurrence feature determines the best attributes for the classification. In the filtering method, a link matrix is generated from these attributes and high-linked attributes are selected to remove them. Thalach, Age, Thal, Slope, Exang, and oldpeak were identified from the Cleveland data set as greatly correlated and therefore could be removed. In general, remove and eliminate the absolute correlation attributes of 0.75 or greater, as it shown in Fig. 3. The other way of selecting the Recursion Mode provides a subset of features that produce an accurate result. The RF algorithm is used at each frequency to assess the form. The algorithm is designed to find out all of the probable subsets of attributes, as it shown in Table II. Ka, Thal, Oldbeck, CB, Thalach, Xanga, Slope and Sex have given a subset of features from the Cleveland Data Collection to the classification, as it shown in Fig. 4.

TABLE I. EVALUATION MEASURES OF RANDOM FOREST AND NAÏVE BAYES WITH ELIMINATING REDUNDANT FEATURES AND PREPROCESSING APPROACHES (BY USING FILTER METHOD)

Datasets	No of instances (NB / RF)	No of attributes (NB / RF)	Accuracy		Precision		Recall	
			NB	RF	NB	RF	NB	RF
Cleveland	296	7	98%	54%	0.9850	0.2888	0.9660	0.2766
Switzerland	123	5	84%	29%	0.7493	0.1731	0.6489	0.1923
Hungarian	294	7	95%	72%	0.9691	0.7110	0.9747	0.7146

\*(NB) Naïve Bayes\*\* (RF) Random Forest

TABLE II. EVALUATION MEASURES OF RANDOM FOREST AND NAÏVE BAYES WITH ELIMINATING REDUNDANT FEATURE AND PREPROCESSING APPROACHES (BY USING WRAPPER METHOD)

Datasets	No of instances (NB / RF)	No of attributes (NB / RF)	Accuracy		Precision		Recall	
			NB	RF	NB	RF	NB	RF
Cleveland	296	8	100%	57%	1.000	0.3452	0.9660	1.000
Switzerland	123	9	92%	44%	0.9468	0.2215	0.6489	0.8095
Hungarian	294	5	100%	82%	1.000	0.8139	0.8139	1.000

\*(NB) Naïve Bayes \*\* (RF) Random Forest

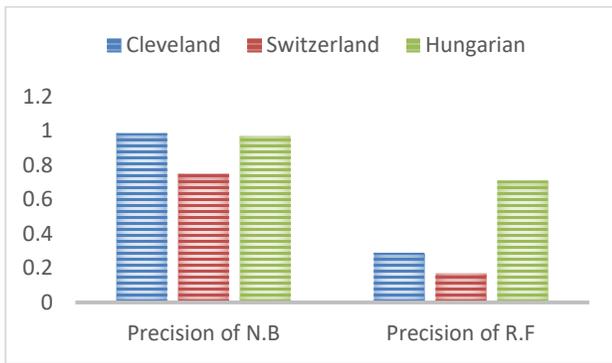


Fig. 1. Accuracy of Random Forest and Naïve Bayes with Eliminating Redundant Features and Preprocessing Approaches (by using Filter Method).

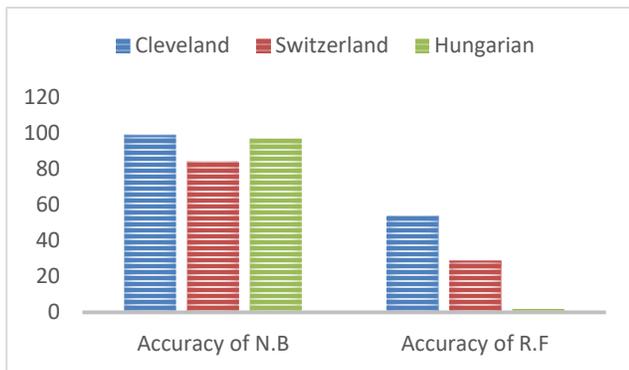


Fig. 2. Precession of Random Forest and Naïve Bayes with Eliminating Redundant Features and Preprocessing Approaches (by using Filter Method).

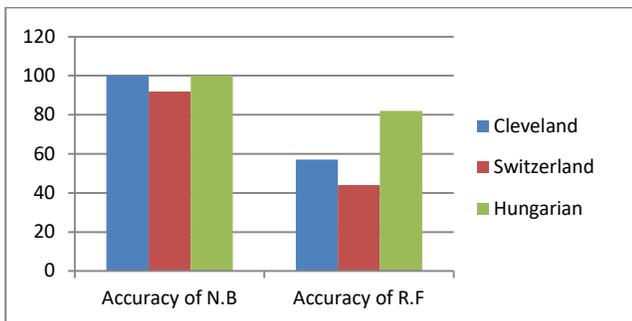


Fig. 3. Accuracy of Random Forest and Naïve Bayes with Eliminating Redundant Features and Preprocessing Approaches (by using Wrapper Method).

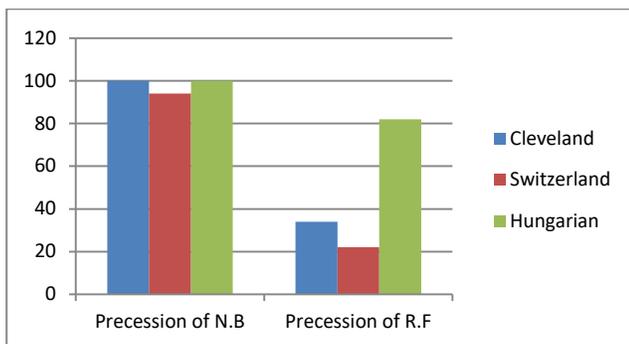


Fig. 4. Precession of Random Forest and Naïve Bayes with Eliminating Redundant Features and Preprocessing Approaches (Wrapper Method).

The following remarks are implemented between the primary data measures and post-pretreatment measures:

- For filter method when comparing Naïve Bayes with Random Forest, the obtained results indicate that Naïve Bayes gives more accurate results.
- For the feature selection wrap method, when comparing Naïve Bayes with Random Forest, the obtained results indicate that Naïve Bayes gives more accurate results.

From the observations above, we find that the Naive Bayes algorithm by using Wrapper method is appropriate for the classification of Hungarian, Switzerland, and Cleveland data sets of the Heart Disease Group.

## V. CONCLUSION

In this paper, three datasets were used (Cleveland, Hungarian, and Switzerland) Heart Disease dataset, they are used for prediction and classification of heart diseases. In the data set, some significant features may contain lost values which may give it an effect on the superiority of the data set. Filling out lost value settings and features may be one of the most important steps in pretreatment.

After parsing the data set, the lost values are determined and changed with the average of the chapter. The subsequent process is to convert the data using the Max-Min normalization technique and then various approaches are applied to select the feature to frame the subset of the important properties of the classification, Recursive Feature Correlation and Elimination. Experimental result shows that dealing with lost values and feature selection approaches significantly boosts the classification's accuracy. The performance of both feature selection processes is evaluated with Naïve Bayes and Random Forest classifiers. Naïve Bayes method of Recursive Feature Elimination gives a better advantage to the three data sets of heart disease in terms of accuracy.

## VI. FUTURE WORK

In the future work, various hybrid algorithms for optimization can be implemented as well for comparative analysis of several classification methods in addition to the possibility of using them as parameters in remote monitoring of patients by using the technology of M2M (machine-to-machine), particularly for patients those treated at remote clinics or home. M2M will be built then adding and embedding a prediction system as a new feature from one party to another.

## REFERENCES

- [1] C. S.Dangare and S. S. Apte, "Improved Study of Heart Disease Prediction System using Data Mining Classification Techniques", International Journal of Computer Applications, vol. 47, no. 10, pp. 44-48, 2012. Available: 10.5120/7228-0076.
- [2] C. S.Dangare and S. S. Apte, "A Data Mining Approach for Prediction of Heart Disease Using Neural Networks," International Journal of Computer Engineering and Technology (IJCET), vol. 3, no. 3, pp. 30-40, Oct. 2012.
- [3] T. T. Abiraami and A. Sumathi, "Analysis of Classification Algorithms for Diabetic Heart Disease," International Journal of Pure and Applied Mathematics, vol. 118, no. 20, pp. 1925-1934, 2018.

- [4] U. Garcarena, R. Santana, and A. Mendiburu, "Evolving imputation strategies for missing data in classification problems with TPOT," arXiv, vol. 2, Aug. 2017.
- [5] T. H. M. Prerana, N. C. Shivaprakash N, and N. Swetha, "Prediction of Heart Disease Using Machine Learning Algorithms- Naïve Bayes, Introduction to PAC Algorithm, Comparison of Algorithms and HDPS," International Journal of Science and Engineering, vol. 3, no. 2, pp. 90–99, 2015.
- [6] B. Bahrami and M. H. Shirvani, "Prediction and Diagnosis of Heart Disease by Data Mining Techniques," Journal of Multidisciplinary Engineering Science and Technology (JMEST), vol. 2, no. 2, Feb. 2015.
- [7] R. Cincy, E. Philipsy, C. Siji, L. P. Suresh, and S. de. E. P. A. Rajan, "A Survey on Predicting Heart Disease using Data Mining Technique," Proc. IEEE Conference on Emerging Devices and Smart Systems (ICEDSS 2018), 2018.
- [8] D. Dua and T. Karra, Archive.ics.uci.edu, 2019. [Online]. Available: <http://archive.ics.uci.edu/ml>. [Accessed: 10- May- 2019].
- [9] K. A. Enriko, M. Suryanegara, and D. Gunawan, "Heart disease prediction system using k-Nearest neighbor algorithm with simplified patient's health parameters," Journal of Telecommunication, Electric, and Computer Engineering, vol. 8, no. 8, pp. 59–65, 2016.
- [10] X. Wu, V. Kumar, J. R. Quinlan, J. Ghosh, Q. Yang, H. Motoda, and D. Steinberg, "Top 10 algorithms in data mining," Knowledge and Information Systems, vol. 14, no. 1, pp. 1–37, 2008.
- [11] I. Rish, "An empirical study of the naive Bayes classifier," IJCAI 2001 workshop on empirical, 2001.
- [12] D. Lavanya and K. U. Rani, "Ensemble decision tree classifier for breast cancer data," International Journal of Information Technology Convergence and Services (IJITCS), vol. 2, no. 1, pp. 17–24, 2012.
- [13] L. E. Peterson, "K-nearest neighbor," Scholarpedia, vol. 4, no. 2, p. 1883, 2009.
- [14] M. A. Jabbar, B. L. Deekshatulu, and C. Priti, "Prediction of risk score for heart disease using associative classification and hybrid feature Selection," IEEE ISDA 2012, pp. 628–634, 2012.
- [15] A.S. Hameed, B.M. Aboobaider, N.H. Choon, M.L. Mutar, and W. H. Bilal, "Review on the Methods to Solve Combinatorial Optimization Problems Particularly: Quadratic Assignment Model," Int. J. Eng. Technol., vol. 7, pp. 15–20, 2018.
- [16] M. L. Mutar, M. A. Burhanuddin, A. S. Hameed, N. Yusof, M. F. Alrifai, and A. A. Mohammed, "Multi-objectives ant colony system for solving multi-objectives capacitated vehicle routing problem," J. Theor. Appl. Inf. Technol., vol. 98, no. 24, pp. 4014–4027, 2020.
- [17] A.S. Hameed, B.M. Aboobaider, N.H. Choon, M.L. Mutar, 'Improved Discrete Differential Evolution Algorithm in Solving Quadratic Assignment Problem for best Solutions', International Journal of Advanced Computer Science and Applications, 9(12), pp. 434–439, 2018. doi: 10.14569/ijacsa.2018.091261.

# Towards Natural Language Processing with Figures of Speech in Hindi Poetry

Milind Kumar Audichya<sup>1</sup>

Computer Science Department  
Gujarat Technological University, Ahmedabad, India

Jatinderkumar R. Saini<sup>2\*</sup>

Symbiosis Institute of Computer Studies and Research  
Symbiosis International (Deemed University), Pune, India

**Abstract**—Poems have always been an excellent way of expressing emotions in any language. In particular, Hindi poetry is having versatile popularity among native and non-native speakers all over the world. A typical poem in Hindi is characterized by meter (“Chhand”), emotion (“Rasa”), and figure of speech (“Alankaar”). The present research work is the first of its kind in Hindi Natural Language Processing (NLP), which touches on the area of Hindi figure of speech. The authors have created a systematic hierarchical structure of Hindi “Alankaar” types and sub-types and attempted and extended the work to identify a few. A taxonomical list of 58 Hindi figures of speech is presented along with their nearest mapping to English equivalents. On the sidelines, the paper also presents the distinct rules for each type and sub-type needed for the classification task of NLP. The authors achieved 97% efficiency in reporting the first results with an average execution time of 0.002 seconds.

**Keywords**—“Alankaar”; figure of speech; Hindi; Natural Language Processing (NLP); poetry

## I. INTRODUCTION

Poetry refers to the poetic creation of a person and consists of a series of verses. Different types of poetry have been written from as early as the 25th century BCE [1]. Different types of rules and regulations are followed for writing poetry in different language scripts, yet maintaining grammar [2]. Hindi is one of the prevalent languages of the world. To some extent, Hindi is a majorly spoken language for communication in India and is written using the Devanagari script. It is used along with English as the official language of the Government of India [3].

Many well-known writers have done many poetic creations in the Hindi language, and every day many writers are writing some new poems. In Hindi poetry, “Rasa” (i.e., “emotion”), “Chhand” (i.e., verse meter), and “Alankaar” (i.e., the figure of speech) are essentials of the poetic composition [4]. Though little progress can be seen in the “Rasa” and verse-related research works, it is almost absent when it comes to the figure of speech. The figure of speech known as “Alankaar” in Hindi is capable enough to make any poem’s creation magical through its presence.

Our contribution through the present research work includes:

- Detailed exploration of Hindi “Alankaar”,
- The standardization of taxonomical classification structure for different types of “Alankaar”, and

- The specific methodology for identification of the three trendy Hindi “Alankaar”.

The former could be well exploited for Natural Language Processing (NLP) of Hindi language, particularly for the classification task.

Notably, all of these are worked upon and reported for the first time in the scientific literature. The structure of the remainder of the paper includes literature review, description of rules and creation of “Alankaar” hierarchy, “Alankaar” identification, and results. The paper ends with the conclusions derived from the work and some pointers to future work.

## II. LITERATURE REVIEW

An extensive literature review was carried out for this research, in which we tried to dig up the research items, books, blogs, and online portals for the different kinds of information retrieval and to know the current state of the research progress in this specific segment. Research works for the internationally well-known languages that can be seen concerning poetry and related nearby segments such as emotion detection, text classification, and identification in different languages such as Arabic, Chinese, English, and Persian [5-8]. Some research works related to poetry were found for Indian regional languages like Hindi, Marathi, and Punjabi [9-11].

Saini and Kaur [13] worked for Punjabi poems annotated corpus for emotion detection based on the nine different types of emotions (“Rasa”). Pal and Patel [12] introduced a model for the classification of Hindi poems. Audichya and Saini [14] worked for the unified rule-based technique for automatic metadata generation based on different meter rules in Hindi poetry. Kushwah and Joshi [15] researched the detection of a specific type of verse meter named “Rola”. Bafna and Saini [16-19] also worked using eager machine learning and concept learning algorithms to classify Hindi verses.

After founding and exploring this much, authors can powerfully convey that the figure of speech as known as “Alankaar” in Hindi is an untouched portion of the research works related to Hindi or any other Indian regional level languages. The main reason behind less work in this area is because it is tedious to deal with, and no such initial research works had been done or carried out so far. To fulfill this gap, we have presented a path to work further in Hindi NLP from the perspective of “Alankaar”. One of the goals of this research work is to organize and manage all available information related to the figure of speech in the Hindi language after

\*Corresponding Author

proper collection, verification, and validation for a better research approach so that one is not needed to deal with insufficient knowledge or contradictory information in upcoming times.

After the detailed and in-depth literature review, it was observed that there is a lack of identification mechanism which can detect and identify the different “Alankaar” in Hindi. The vast Hindi content data can be sorted in an organized manner with the generated metadata based on the detection. The metadata can help populate better search results instead of regular keywords-based searching. Apart from that, this research work can help digital libraries to manage the content based on the different types of Hindi “Alankaar”. With the perspective of computational logistics, this research work can help analyze the write-ups based on the different types of the Hindi “Alankaar”. So as authors felt, it can be a valuable and necessary novel work for current and upcoming times, which can be understood with already emphasized points, and there can be many more uses scenarios also. These all aspects were the actual motivation to carry out this research work.

### III. “ALANKAAR”: THE HINDI FIGURE OF SPEECH

The figure of speech which is scripted as “अलंकार” (“Alankaar”) in the Devanagari script of the Hindi language, is an essential part of the creation of the poem. “Alankaar” means “ornament”, and just as the beauty of a person is adorned with ornamentation, in the same way, the grace of poetry is ornamented. Something which embellishes the poem is known as the figure of speech.

To identify and detect the different types of “Alankaar” we first need standard types and rules, which are not available systematically, and where ever is available, it is either missing some information or have some fewer details [20-21]. The first and significant time-consuming task of this research work was to go through the various sources to collect, verify, and systematically structure hierarchical classes for better research.

The rules and all their relevant information collection were carried out through different places such as educational materials, websites, blogs, and portals [22-24]. After this process, we have structured everything in such a way with Hindi experts’ opinions from academia to be helpful for the upcoming research works.

#### A. Types of “Alankaar”

Mainly as per the characteristics, the types of “Alankaar” are divided into three streams which are as follows:

- 1) “Shabd Alankaar” (“शब्दालंकार”)
- 2) “Arth Alankaar” (“अर्थालंकार”)
- 3) “Ubhay Alankaar” (“उभयालंकार”)

Each has its own set of rules and further subtypes, and even sub-sub types [25]. We discuss each of them quickly in the subsequent sections.

1) “Shabd Alankaar” (“शब्दालंकार”): “Shabd Alankaar” is the first type of the Hindi figure of speech, those which embellish the poems through the words in the figure of speech, that is, by putting a particular word in a poem, the

beauty comes, and if the beauty is lost when using a synonym, are called the “Shabd Alankaar”. Although not all the “Alankaars” that come in this category are purely based on words, the primary focus in those “Alankaars” is on the words, which is why they are added into this category.

“Shabd Alankaar” have further sub and sub-sub classes as per their types mentioned as follows: Each has its own set of rules and further subtypes, and even sub-sub types [25]. We discuss each of them quickly in the subsequent sections.

#### 1.1 Alliteration (“अनुप्रास अलंकार”)

- 1.1.1 ‘Chekanupras’ (“छेकानुप्रास अलंकार”)
- 1.1.2 ‘Vrutyanupras’ (“वृत्यानप्रास अलंकार”)
- 1.1.3 ‘Latanupras’ (“लाटानुप्रास अलंकार”)
- 1.1.4 ‘Antyanpras’ (“अन्तत्यानप्रास अलंकार”)
- 1.1.5 ‘Shrtyanpras’ (“श्रत्यानप्रास अलंकार”)

#### 1.2 ‘Yamak’ (“यमक अलंकार”)

#### 1.3 ‘Punrukti’ (“पुनरुक्ति अलंकार”)

#### 1.4 ‘Vipsa’ (“विप्सा अलंकार”)

#### 1.5 ‘Vakrokti’ (“वक्रोक्ति अलंकार”)

- 1.5.1 ‘Kaku Vakrokti’ (“काकु वक्रोक्ति अलंकार”)
- 1.5.2 ‘Shelsh Vakrokti’ (“श्लेष वक्रोक्ति अलंकार”)

#### 1.6 Pun or Irony (“श्लेष अलंकार”)

- 1.6.1 ‘Abhang Shlesh’ (“अभंग श्लेष अलंकार”)
- 1.6.2 ‘Sabhang Shlesh’ (“सभंग श्लेष अलंकार”)

2) “Arth Alankaar” (“अर्थालंकार”): “Arth Alankaar” is mainly related to the meaning of the words, so those which embellish the poems through the meaning of the words in the figure of speech, That is, by putting a particular word in a poem and due to the meaning of that word the miracles occur in poetry, are called the “Arth Alankaar”. Although not all the “Alankaar” which comes in this category are purely based on the meaning of words, yet the primary focus in those “Alankaars” is on the meaning of the words that’s why they are added into this category.

“Arth Alankaar” are having further sub and sub-sub classes as per their types which are mentioned as following:

#### 1.1 Simile (“उपमा अलंकार”)

- 1.1.1 ‘Purnopama’ (“पूर्णोपमा अलंकार”)
- 1.1.2 ‘Luptopama’ (“लुप्तोपमा अलंकार”)

#### 1.2 Metaphor (“रूपक अलंकार”)

- 1.2.1 ‘Sam Rupak’ (“सम रूपक अलंकार”)
- 1.2.2 ‘Adhik Rupak’ (“अधिक रूपक अलंकार”)
- 1.2.3 ‘Nyun Rupak’ (“न्यून रूपक अलंकार”)

#### 1.3 Poetic Fancy (“उत्प्रेक्षा अलंकार”)

- 1.3.1 ‘Vastupreksha’ (“वस्तुप्रेक्षा अलंकार”)
- 1.3.2 ‘Hetupreksha’ (“हेतुप्रेक्षा अलंकार”)
- 1.3.3 ‘Falotpreksha’ (“फलोत्प्रेक्षा अलंकार”)

#### 1.4 Exemplification (“द्रष्टान्ति अलंकार/दृष्टान्त”)

#### 1.5 Doubt (“संदेह अलंकार”)

#### 1.6 Hyperbole (“अतिशयोक्ति अलंकार”)

#### 1.7 ‘Upmeyopma’ (“उपमेयोपमा अलंकार”)

- 1.8 *Converse* (“प्रतीप अलंकार”)
- 1.9 *Self Comparison* (“अनन्वय अलंकार”)
- 1.10 *Error* (“भ्रांतिमान अलंकार”)
- 1.11 *Illuminator* (“दीपक अलंकार”)
- 1.12 *Concealment* (“अपहृति अलंकार”)
- 1.13 *‘Vyatirek’* (“व्यतिरेक अलंकार”)
- 1.14 *Peculiar Causation* (“विभावना अलंकार”)
- 1.15 *Peculiar Allegation* (“विशेषोक्ति अलंकार”)
- 1.16 *Corroboration* (“अर्थान्तरन्यास अलंकार”)
- 1.17 *‘Ullek’* (“उल्लेख अलंकार”)
- 1.18 *Contradiction* (“विरोधाभास अलंकार”)
- 1.19 *Disconnection* (“असंगति अलंकार”)
- 1.20 *Personification* (“मानवीकरण अलंकार”)
- 1.21 *‘Anantyokti’* (“अन्तयोक्ति अलंकार”)
- 1.22 *Poetical Reason* (“काव्यलिंग अलंकार”)
- 1.23 *Natural Description* (“स्वभावोती अलंकार”)
- 1.24 *Typical Comparison* (“प्रतिवस्तूपमा”)
- 1.25 *Chain of Similes* (“मालोपमा”)
- 1.26 *Equal Pairing* (“तुल्योपमा”)
- 1.27 *Illustration* (“निदर्शना”)
- 1.28 *Speech of Brevity* (“समासोक्ति”)
- 1.29 *Indirect Dissection* (“अप्रस्तुतप्रर्शसा”)
- 1.30 *Special Mention* (“परिसंख्या”)

Types of ‘ALANKAAR’ - The Hindi Figure of Speech (“अलंकार के भेद”)	
1. ‘Shabd Alankaar’ (“शब्दालंकार”)	2. ‘Arth Alankaar’ (“अर्थालंकार”)
1.1 Alliteration (“अनुप्रास अलंकार”)	2.1 Simile (“उपमा अलंकार”)
1.1.1 ‘Chekanupras’ (“छेकनुप्रास अलंकार”)	2.1.1 ‘Purnopama’ (“पूर्णोपमा अलंकार”)
1.1.2 ‘Vrutyanupras’ (“वृत्तानुप्रास अलंकार”)	2.1.2 ‘Luptopama’ (“लुप्तोपमा अलंकार”)
1.1.3 ‘Latanupras’ (“लटानुप्रास अलंकार”)	2.2 Metaphor (“रूपक अलंकार”)
1.1.4 ‘Antyanpras’ (“अन्तानुप्रास अलंकार”)	2.2.1 ‘Sam Rupak’ (“सम रूपक अलंकार”)
1.1.5 ‘Shrtyanpras’ (“श्रयानुप्रास अलंकार”)	2.2.2 ‘Adhik Rupak’ (“अधिक रूपक अलंकार”)
1.2 ‘Yamak’ (“यमक अलंकार”)	2.2.3 ‘Nyun Rupak’ (“न्यून रूपक अलंकार”)
1.3 ‘Punrukti’ (“पुनरुक्ति अलंकार”)	2.3 Poetic Fancy (“उपेक्षा अलंकार”)
1.4 ‘Vipsa’ (“विप्सा अलंकार”)	2.3.1 ‘Vastupreksha’ (“वस्तुप्रेक्षा अलंकार”)
1.5 ‘Vakrokti’ (“वक्रोक्ति अलंकार”)	2.3.2 ‘Hetupreksha’ (“हेतुप्रेक्षा अलंकार”)
1.5.1 ‘Kaku Vakrokti’ (“ककु वक्रोक्ति अलंकार”)	2.3.3 ‘Falotpreksha’ (“फलतोपेक्षा अलंकार”)
1.5.2 ‘Shesh Vakrokti’ (“शेष वक्रोक्ति अलंकार”)	2.4 Exemplification (“प्रदर्शन अलंकार/दृष्टान्त”)
1.6 Pan or Irony (“श्लेष अलंकार”)	2.5 Doubt (“संशय अलंकार”)
1.6.1 ‘Abhang Shlesh’ (“अभंग श्लेष अलंकार”)	2.6 Hyperbole (“अतिशयोक्ति अलंकार”)
1.6.2 ‘Sabhang Shlesh’ (“सभंग श्लेष अलंकार”)	2.7 ‘Upmeyopma’ (“उपमेयोपमा अलंकार”)
3. ‘Ubhay Alankaar’ (“उभयालंकार”)	2.8 Converse (“प्रतीप अलंकार”)
3.1 Combination of Figures of Speech (“संयुक्ति”)	2.9 Self Comparison (“अनन्वय अलंकार”)
3.2 The fusion of Figures of Speech (“संकर”)	2.10 Error (“भ्रंतिमान अलंकार”)
	2.11 Illuminator (“दीपक अलंकार”)
	2.12 Concealment (“अपहृति अलंकार”)
	2.13 ‘Vyatirek’ (“व्यतिरेक अलंकार”)
	2.14 Peculiar Causation (“विभावना अलंकार”)
	2.15 Peculiar Allegation (“विशेषोक्ति अलंकार”)
	2.16 Corroboration (“अर्थान्तरन्यास अलंकार”)
	2.17 ‘Ullek’ (“उल्लेख अलंकार”)
	2.18 Contradiction (“विरोधाभास अलंकार”)
	2.19 Disconnection (“असंगति अलंकार”)
	2.20 Personification (“मानवीकरण अलंकार”)
	2.21 ‘Anantyokti’ (“अन्तयोक्ति अलंकार”)
	2.22 Poetical Reason (“काव्यलिंग अलंकार”)
	2.23 Natural Description (“स्वभावोती अलंकार”)
	2.24 Typical Comparison (“प्रतिवस्तूपमा”)
	2.25 Chain of Similes (“मालोपमा”)
	2.26 Equal Pairing (“तुल्योपमा”)
	2.27 Illustration (“निदर्शना”)
	2.28 Speech of Brevity (“समासोक्ति”)
	2.29 Indirect Dissection (“अप्रस्तुतप्रर्शसा”)
	2.30 Special Mention (“परिसंख्या”)

Fig. 1. Systematically Structured Graphical Representation of Hindi Alankaars.

### B. Selecting a Template

Research works are always challenging, and that’s what the beauty of research is, but when it comes to the research with the figure of speech in Hindi, it is very tedious and challenging. That’s the only reason this segment was still untouched, and no such initial research was found. While carrying out this research work, the following challenges were faced.

1) *No previous research works*: Initial level research work requires some extra efforts as we discussed already that no previous research work or articles had been found so far, so one needs to create their path or way to work to accomplish the research-related tasks and it requires massive efforts because there is no dataset, algorithms or implementation strategy is existing.

2) *Missing and conflicting information*: Information Collection, verification, and systematic arrangement are some of the initial tasks of any research work, and this is more important when dealing with a purely new segment where no such past research works or articles can be seen. The authors came across different sources in this collection and validation process where either some types were missing or having incomplete information.

3) *Context-based meaning*: To deal with Hindi words’ meanings, one can integrate with the existing Hindi wordnet or other libraries, but the context-based meaning is required, which is missing, or still, some research works are going on in the same segment and research in its own [26].

TABLE I. ALANKAARS COMPARATIVE SCENARIO AND STATS

Alankaars Comparative Scenario	Count
Total Alankaars for which English equivalent is found:	30
Total Alankaars for which English equivalent is not found:	28
Total Alankaars in Hindi:	58

4) *Homonymy and polysemy*: “Alankaars” are all about the words and their meanings, here a single word can have multiple and can be used to express different things, which are polysemy, and similar words that are either spelled similar or sound the same but have different meanings are homonymy. That is another challenge level, which is still a vast issue and essential for this research work, too [27].

5) *Multiple “Alankars” detection*: As per the nature and characteristics of “Alankaar”, there can be multiple “Alankaars” in the same poem lines or even in a part of the poem, comparatively in “Rasa” and “Chhand” usually it has been observed that mostly there will be only a single type of “Rasa” or “Chhand” will be there in a part of the poem.

6) *Unavailability of datasets for experiments*: To carry out any research work, one will always need a dataset, as there is no such research work done in this specific problem segment, and in other poem related Hindi research also works dataset is a challenge because there is no such ready dataset or open-source datasets are available. To deal with such things, one has to follow one and the only thing that makes the dataset by self, and again it requires some additional effort and time.

Despite all of the listed challenges, we followed the approach of focusing on the best optimum problem-solving methods, and the same is discussed in the following “Alankaar” Identification section.

#### IV. “ALANKAAR” IDENTIFICATION

To Identify and detect the “Alankaars” used in Hindi poetry based on the different rules of “Alankaars”, we tried to implement the viral, trendy, and three primarily used “Alankaars” out of the all mentioned 58 different types.

For example, to identify and detect these two “Alankaars”, namely “Anupras” (i.e., Alliteration) “Punrukti”, we need to know the respective appropriate rules of both types. If we consider “Anupras”, the rule says that when a specific character occurs repeatedly, there is “Anupras”. If we talk about the “Punrukti”, a word that occurs twice consecutively, then there is “Punrukti”. Let us understand with the following example which fits for both the types:

‘ढुमुकि - ढुमुकि रुनझुन धुनि - सुनि,  
कनक अजिर शिशु डोलता’

In this example, the Unicode Standard [28] Unicode Transformation Format - 8 (UTF-8) based text is accepted as input, and if we observe closely, we can see that the character ‘क’, ‘न’ and more occurs more than once, repeated and again and again so “Anupras” is here. Also, there is “ढुमुकि” word which is occurring twice consecutively it is fulfilling “Punrukti” rule. This is how one can understand this concept, but to make a computer computationally understand the same, we need to follow some systematic process so we have designed in such a way that in the case in near future we need to add some more “Alankaar” implementation we can do that very quickly.

The simplest way to understand the implementation methodology is as follows:

**Step 1:** Start.

**Step 2:** Input the data in “UTF-8” format.

**Step 3:** Cleaning and Preprocessing operations.

**Step 4:** Perform Character Count and Word Count.

**Step 5:** Send the data to check the “Alankaar”.

**Step 6:** Check “Alankaar” in “Shabd Alankaar” where it will further pass on the sub-type functions, and if any type gets detected, it will be added to the output result buffer.

**Step 7:** Check “Alankaar” in “Arth Alankaar” where it will further pass on the subtype functions and if any type gets detected, it will be added to the output result buffer.

**Step 8:** Check “Alankaar” in “Ubhay Alankaar” where it will further pass on the sub-type functions and if any type gets detected, it will be added to the output result buffer.

**Step 9:** Return appropriate output by merging all the output in the buffer.

**Step 10:** Stop.

With this methodology, many “Alankaars” can be easily covered as soon as the modeling of the specific “Alankaar” rules is done in the implementation script’s functional modules. Let’s have a look at the pseudo-code for this implementation.

```
if isshabdAlankaar():  
    outputformator(output)  
elif isarthAlankaar():  
    outputformator(output)  
elif isubhyaAlankaar():  
    outputformator(output)
```

If one need to check for specific “Alankaar” functional code goes as follow:

```
def isanupras():  
    global Input,output  
    anupras = False  
    count = character_count(Input)  
    for key, value in count.items():  
        if value >= 2:  
            anupras = True
```

The function gets called while checking “Shabd Alankaar”. As same as the “isanupras()” other alankars methods also gets executed automatically while checking different classes of “Alankaar”. Along with that, by keeping the computational perspective in mind, if required, the appropriate position of the detected “Alankaar” can also be populated along with the final metadata.

#### V. RESULTS

In this research work, we started from scratch and as a final result, we have systematically sorted and arranged standard hierarchical data of “Alankaars”. Apart from that, the authors were also able to execute binary classification for the three “Alankaars” successfully. From an implementation perspective, the authors have already implemented “Anupras”, “Punrukti” and “Yamak” “Alankaars”. The same example is used to explain the result, which was used to discuss in the

“Alankaar” Identification section. The code for the output depicted in Fig. 1 was written using Python version 3.9 and executed on MacBook Air 13-inch, 2017 system with macOS Big Sur Version 11.1 having 8 GB 1600 MHz DDR3 Memory along with 1.8 GHz Dual-Core Intel Core i5 processor.

```
कृपया इनपुट उपलब्ध करवाए (इनपुट के बाद Ctrl+D दबाए) :  
डुमुकि - डुमुकि रुनरुक्ति धुनि - सुनि ,  
कनक अजिर शिशु डोलत।  
^D  
Type : शब्दालंकार  
Sub Type : अनुप्रास अलंकार  
Type : शब्दालंकार  
Sub Type : पुनरुक्ति अलंकार  
Time Duration (In Seconds) : 0.00023818016052246094
```

Fig. 2. Output of the Automatic “Alankaar” Identification.

Fig. 2 shows that it took input and processed the same as discussed in section IV, and on completion, it returns that the input is consists of two “Alankaars” which comes under the primary type “Shabd Alankaar” and their subtypes are “Anupras” and “Punrukti”. Also, one thing to notice here is that the whole process took just 0.002 seconds, which is a rapid execution time. Apart from these two, we have also incorporated the “Yamak Alankaar” identification which works quite well, but it does not work in some scenarios as we need to make it work better using the integration of the wordnet for the meanings of the words for the comparison of different words.

Table II shows the result related stats of this research work carried out after the working model’s design and implementation integration. There is no training mechanism based on data in this research study, so whatever data inputted for the tests were genuinely on unseen data only. The test was carried out on the 78 different UTF-8 based input, and based on the results, we were finally able to achieve overall 97.00% accuracy in 0.002 second average execution time.

TABLE II. ALANKAARS IDENTIFICATION ACCURACY AND EXECUTION TIME

Alankaar	Accuracy %	Execution Time (Seconds)
“Anupras”	100.00%	0.002 Second
“Punrukti”	100.00%	0.002 Second
“Yamak”	091.00%	0.002 Second
<b>Total</b>	<b>291.00%</b>	<b>0.006 Second</b>
<b>Maximum</b>	<b>100.00%</b>	<b>0.002 Second</b>
<b>Minimum</b>	<b>091.00%</b>	<b>0.002 Second</b>
<b>Average</b>	<b>097.00%</b>	<b>0.002 Second</b>

## VI. CONCLUSION AND FUTURE WORK

This research work consists of a lot of time-consuming efforts, which concludes several things. Information related to “Alankaar” is now having some research sort of systematic arrangement which can be used to take it further. Dealing with “Alankaar” is not an easy task. “Alankaars” are itself a world

inside them, and it is not possible to cover all the “Alankaar” identification or detection in one single research work.

Nevertheless, the authors introduced how “Alankaar” identification and detection can be made automatically. Three well-known “Alankaars” are currently modeled, which are “Anupras”, “Punrukti” and “Yamak”. Wordnet integration with advanced grammatical aspects can strengthen this identification system more effectively in upcoming times. In further research works, we will be adding more types. The authors will also be looking for solutions to the challenges that were not able to overcome currently, such as the context-based meaning of Hindi words and other ambiguity-related issues.

## REFERENCES

- [1] Wikipedia Contributors, ‘Poetry,’ Wikipedia, 10-Mar-2019. [Online]. Available: <https://en.wikipedia.org/wiki/Poetry>.
- [2] ‘7 Fundamental Rules of Poetry,’ 7 Fundamental Rules of Poetry: Grammarly Blog, 06-May-2015. [Online]. Available: <https://www.grammarly.com/blog/7-fundamental-rules-of-poetry/>. [Accessed: 04-Dec-2020].
- [3] Wikipedia Contributors, ‘Hindi,’ Wikipedia, 04-May-2019. [Online]. Available: <https://en.wikipedia.org/wiki/Hindi>.
- [4] Contributors to Wikimedia projects, ‘रस,’ Wikipedia.org, 29-Nov-2006. [Online]. Available: <https://hi.wikipedia.org/s/a4j> [Accessed: 04-Dec-2020].
- [5] Z. He, W. Liang, L. Li and Y. Tian, ‘SVM-Based Classification Method for Poetry Style,’ 2007 International Conference on Machine Learning and Cybernetics, Hong Kong, 2007, pp. 2936-2940, doi: 10.1109/ICMLC.2007.4370650.
- [6] S. Hamidi, F. Razzazi and M. P. Ghaemmaghami, ‘Automatic meter classification in Persian poeties using support vector machines,’ 2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Ajman, 2009, pp. 563-567, doi: 10.1109/ISSPIT.2009.5407514.
- [7] N. Ghneim and O. Alsharif, ‘Emotion Classification in Arabic Poetry Using Machine Learning building a model for gender, dialect and age prediction from Arabic tweets View project Interactive Arabic Dictionary View project Emotion Classification in Arabic Poetry using Machine Learning,’ International Journal of Computer Applications, vol. 65, no. 16, pp. 975–8887, 2013.
- [8] A. Abbasi, H. Chen, and A. Salem, ‘Sentiment analysis in multiple languages,’ ACM Transactions on Information Systems, vol. 26, no. 3, pp. 1–34, Jun. 2008, doi: 10.1145/1361684.1361685.
- [9] J. Kaur and J.R.Saini, ‘Designing Punjabi Poetry Classifiers Using Machine Learning and Different Textual Features,’ The International Arab Journal of Information Technology, pp. 38–44, Jan. 2019, doi: 10.34028/iajit/17/1/5.
- [10] B.K. Joshi and K.K. Kushwah, ‘A Novel Approach to Automatic Detection of Chaupai Chhand in Hindi Poems,’ 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, Uttar Pradesh, India, 2018, pp. 223-228, doi: 10.1109/GUCON.2018.8675052.
- [11] P.B. Bafna and J.R.Saini, ‘An Application of Zipf’s Law for Prose and Verse Corpora Neutrality for Hindi and Marathi Languages,’ International Journal of Advanced Computer Science and Applications, vol. 11, no. 3, 2020, doi: 10.14569/ijacsa.2020.0110331.
- [12] K. Pal and B.V. Patel, ‘Model for Classification of Poems in Hindi Language Based on Rasa,’ Smart Systems and IoT: Innovations in Computing, pp. 655–661, Oct. 2019, doi: 10.1007/978-981-13-8406-6\_62.
- [13] J.R.Saini and J.Kaur, ‘Kāvi: An Annotated Corpus of Punjabi Poetry with Emotion Detection Based on ‘NavRasa’, Procedia Computer Science, vol. 167, pp. 1220–1229, 2020, doi: 10.1016/j.procs.2020.03.436.
- [14] M.K. Audichya and J.R. Saini, ‘Computational linguistic prosody rule-based unified technique for automatic metadata generation for Hindi poetry,’ 2019 1st International Conference on Advances in Information

- Technology (ICAIT), Chikmagalur, India, 2019, pp. 436-442, doi: 10.1109/ICAIT47043.2019.8987239.
- [15] K.K. Kushwah and B.K. Joshi, 'Rola: An Equi-Matrik Chhand of Hindi Poems.', International Journal of Computer Science and Information Security (IJSIS), Vol. 15, No. 3, March 2017.
- [16] P.B. Bafna and J.R. Saini, 'On Exhaustive Evaluation of Eager Machine Learning Algorithms for Classification of Hindi Verses,' International Journal of Advanced Computer Science and Applications, vol. 11, no. 2, 2020, doi: 10.14569/ijacsa.2020.0110224.
- [17] P.B. Bafna and J.R. Saini, 'Hindi Verse Class Predictor using Concept Learning Algorithms,' 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 318-322, doi: 10.1109/ICIMIA48430.2020.9074850.
- [18] P.B. Bafna and J.R. Saini, 'BaSa: A Technique to Identify Context based Common Tokens for Hindi Verses and Proses,' 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, pp. 1-4, doi: 10.1109/INCET49848.2020.9154124.
- [19] P.B. Bafna and J.R. Saini, 'Hindi Poetry Classification using Eager Supervised Machine Learning Algorithms,' 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2020, pp. 175-178, doi: 10.1109/ESCI48226.2020.9167632.
- [20] 'भारतीय काव्यशास्त्र (दिवि)/अलंकार - विकिपुस्तक,' Wikibooks.org, 2020. [Online]. Available: [https://hi.wikibooks.org/wiki/%E0%A4%AD%E0%A4%BE%E0%A4%B0%E0%A4%A4%E0%A5%80%E0%A4%AF%E0%A4%95%E0%A4%BE%E0%A4%B5%E0%A5%8D%E0%A4%B6%E0%A4%BE%E0%A4%B8%E0%A5%8D%E0%A4%A4%E0%A5%8D%E0%A4%B0\\_\(%E0%A4%A6%E0%A4%BF%E0%A4%B5%E0%A4%BF\)/%E0%A4%85%E0%A4%B2%E0%A4%82%E0%A4%95%E0%A4%BE%E0%A4%B0](https://hi.wikibooks.org/wiki/%E0%A4%AD%E0%A4%BE%E0%A4%B0%E0%A4%A4%E0%A5%80%E0%A4%AF%E0%A4%95%E0%A4%BE%E0%A4%B5%E0%A5%8D%E0%A4%B6%E0%A4%BE%E0%A4%B8%E0%A5%8D%E0%A4%A4%E0%A5%8D%E0%A4%B0_(%E0%A4%A6%E0%A4%BF%E0%A4%B5%E0%A4%BF)/%E0%A4%85%E0%A4%B2%E0%A4%82%E0%A4%95%E0%A4%BE%E0%A4%B0). [Accessed: 07-Dec-2020].
- [21] Contributors to Wikimedia projects, 'अलंकार,' Wikipedia.org, 19-Mar-2007. [Online]. Available: <https://hi.wikipedia.org/s/9ll> [Accessed: 07-Dec-2020].
- [22] 'अलंकार - अलंकार की परिभाषा, भेद, उदाहरण, Hindi Grammar.' [Online]. Available: <https://www.mycoaching.in/2018/09/Alankaar.html>. [Accessed: 07-Dec-2020].
- [23] 'अलंकार - भारतकोश, ज्ञान का हिन्दी महासागर,' Bharatdiscovery.org, 2020. [Online]. Available: <https://bharatdiscovery.org/india/%E0%A4%85%E0%A4%B2%E0%A4%82%E0%A4%95%E0%A4%BE%E0%A4%B0>.
- [24] 'अलंकार की परिभाषा, भेद, प्रकार और उदाहरण सहित पूरी जानकारी,' Hindi vibhag, 26-Aug-2017. [Online]. Available: <https://www.hindivibhag.com/%E0%A4%85%E0%A4%B2%E0%A4%82%E0%A4%95%E0%A4%BE%E0%A4%B0/>. [Accessed: 07-Dec-2020].
- [25] 'Alankaar'(Figure of speech)(अलंकार) Hindi Grammar,' hindigrammar.in. [Online]. Available: <http://hindigrammar.in/Alankaar%20.html>. [Accessed: 07-Dec-2020].
- [26] S. Rajendran and S. Arulmozi, 'Augmenting Indo-wordnet with Context' [Online]. Available: [http://www.cfilt.iitb.ac.in/wordnet/webhwn/IndoWordnetPapers/13\\_iwn\\_Augmenting%20Indo-wordnet%20with%20Context.pdf](http://www.cfilt.iitb.ac.in/wordnet/webhwn/IndoWordnetPapers/13_iwn_Augmenting%20Indo-wordnet%20with%20Context.pdf). [Accessed: 07-Dec-2020].
- [27] N. Dash, 'Polysemy and Homonymy: A Conceptual Labyrinth' [Online]. Available: [http://www.cfilt.iitb.ac.in/wordnet/webhwn/IndoWordnetPapers/08\\_iwn\\_Polysemy%20and%20Homonymy.pdf](http://www.cfilt.iitb.ac.in/wordnet/webhwn/IndoWordnetPapers/08_iwn_Polysemy%20and%20Homonymy.pdf). [Accessed: 07-Dec-2020].
- [28] 'The Unicode Standard, Version 12.0 - Devanagari.' [Online]. Available: <https://www.unicode.org/charts/PDF/U0900.pdf>.

# Formal Verification of an Efficient Architecture to Enhance the Security in IoT

Eman K. Elsayed<sup>1</sup>, L. S. Diab<sup>2</sup>, Asmaa. A. Ibrahim<sup>3</sup>  
Mathematical and Computer Science  
Al-Azhar University  
Cairo, Egypt

**Abstract**—The Internet of Things (IoT) is one of the world's newest intelligent communication technologies. There are several kinds of novels about IoT architectures, but they still suffer from security and privacy challenges. Formal verification is a vital method for detecting potential weaknesses and vulnerabilities at an early stage. During this paper, a framework in the Event-B formal method will be used to design a formal description of the secure IoT architecture to cover the security properties of the IoT architecture. As well as using various Event-B properties like formal verification, functional checks, and model checkers to design different formal spoofing attacks for the IoT environment. Additionally, the Accuracy of the IoT architecture can be obtained by executing different Event-B runs like simulations, proof obligation, and invariant checking. By applied formal verification, functional checks and model checkers verified models of IoT-EAA architecture have automatically discharged 82.35% of proof obligations through different Event-B provers. Finally, this paper will focus on introducing a well-defined IoT security infrastructure to address and reduce the security challenges.

**Keywords**—Internet of things (IoT); IoT architecture; IoT security; formal modeling and verification; Event-B

## I. INTRODUCTION

The Internet of Things (IoT) is one of the most recent research topics these days. IoT [1] allows various devices to communicate with one another over the Internet. As a result, it ensures that the device is intelligent and sends information to a central system, which will check and take necessary measures by the task at hand. To make the IoT paradigm a reality, things or objects must be identified, as well as sensing, networking, and processing capabilities.

Recent advances [2] in wireless technology, advanced communications, and intelligent systems have demonstrated a strong potential and a strong attempt to enhance human life in every way possible. Depending on the different application domains of IoT, the heterogeneity of the devices, and the ubiquitous communication, IoT is primarily composed of several sensors (wireless and automatic). It requires a deep understanding of IoT architecture. Its architecture is made up of four main layers [3, 4]; Perception, Network, Middleware, and Application layer. The interconnection of massive heterogeneous frameworks and networks of systems is referred to as IoT technology.

Because IoT devices [5] have different designs, implementations, and maintenance, they have a variety of problems and weaknesses in their software and hardware.

When all the security requirements are met successfully, a system is considered secure [6]. Confidentiality, integrity, authentication, availability, authorization, non-repudiation, and privacy are all essential requirements. For each one-off them and must ensure security in all different layers from different threats. As a result, the entire deployment architecture must be secured from attacks that could hinder IoT services or jeopardize data privacy, integrity, or confidentiality.

Since this Internet of Things is composed up of interconnected networks and heterogeneous devices, it inherits the security problems facing computer networks. Since small devices or items with sensors have limited power and memory, IoT protection is further complicated by resource constraints. Consequently, security solutions need to be adapted to the constrained architectures.

Recently, a lot of effort has gone into dealing with security issues in the IoT paradigm. Some of these approaches focus on a particular layer of security, while others aim to provide end-to-end security for IoT. According to [7], the author proposed a new efficient and secure architecture model for the Internet of things called IoT-EAA, which tends to provide end-to-end security for IoT through the top one of the IoT applications, as well as resolving various security issues that exists at various bottom layers. “Fig. 1” shows the IoT-EAA security architecture model, which contains five layers, (Hardware Layer, Network Communication Layer, Service Application Layer, Connectivity Management Layer, and Security Layer).



Fig. 1. IoT-EAA Architecture.

Event-B is a formal method for formal specification and development of systems [8] that an extension of method B. In formal Event-B methods, step-by-step models of systems can be created starting with an abstract model and enrich the abstract models with more details to form concrete models.

To ensure that a refined model conforms to abstract models [9], a series of test loads are generated to show that the refinements are correct. Event models B contain two parts called context and machine. The static part of the model, such as sets and constants, is contained in the context, while the dynamic part, such as variables and events, is contained in the machine. The main character in Event-B is refinement, which allows for the system's gradual development.

Rodin platform tool [10, 11] introduces support for Event-B modeling, automatic creation, and proving rules. Rodin is an Eclipse-based application that implements Event-B. An environment includes advanced automated provers such as PP, ML, and SMT, which generate proofs for refinements, feasibility, invariants, and well-definedness of expressions within guards, acts, and invariants. When the automatic proof discharge fails, a manual proof discharge is used. Event-B also includes an interactive proving method for manual proof. Rodin platform has a critical feature, which is the proof obligation generator. It generates proof obligations.

IoT network security [12] is divided into two categories: technological challenges and security challenges. The technological challenges are those that arise as a result of the heterogeneity and ubiquity of devices, while the security challenges are primarily related to the system's basic functions. The technological challenges mainly include [13] scalability, performance, computing, wireless technologies, and the distributed paradigm while security challenges include ensuring confidentiality, integrity, end-to-end security, and permanent availability of services.

There is a different security threat to IoT such as Denial of Service, Brute Force, Man in the middle attacks and many other attacks are visualized in the interconnected network. There are several reasons [14] for occurs these attacks like weak passwords, no encryption, personal information leakage, etc., if such security attacks are not solved to some safe level the market of IoT will be harmful because of the weak service of security. It involves not only these security issues but also have other issues of access control, authentication of different networks, and some problems of the information store. This problem requires having a well-defined security infrastructure to address these problems and reduce security Threats [15].

This paper introduces a contribution by using one of the most important formal methods called Event-B, to enhance the security of IoT technology. This involves model checking and theorem proving for IoT architecture discharge in the Rodin platform. Hence, this paper will provide structured verification for IoT architecture that focuses on security checking for each IoT architecture layer, which considers the early stages of building the IoT systems.

The rest of the paper is organized as follows. Section II discusses related works about using formal methods in the IoT area, including previous studies for the IoT and formal

methods. Section III proposed some mathematical definitions for the configurations of the IoT-EAA architecture as well as our methodology for proofing IoT-EAA architecture mathematically. Section IV discusses the verification method. Finally, the last part presents the concluding remarks and future work in Section V.

## II. RELATED WORK

Formal Verification is a promising method for ensuring security by using a variety of mathematical and logical methods to mathematically verify the accuracy of designs. Formal methods are used to implement several approaches in the IoT domain.

In [16] authors review formal methods for various protocols used in the IoT environment. They concern with the security mechanisms for communication protocols in the IoT communication layer only, but in this paper, we used formal verification methods to check the security mechanisms for each layer in the IoT architecture.

In [17] Authors improve the security and detecting various security issues at an early stage for the IoT application layer by introducing formal methods on different protocols in this layer. However, the authors concentrate on the security mechanisms for protocols in the IoT application layer only.

In [18] authors suggest a unified approach for verifying the communication protocols over a framework using machine-decomposition within Event-B. However, this approach does not introduce security properties in the IoT area.

The authors of [19] presented a comprehensive study of the most used formal verification methods and approaches for verifying and analyzing the correctness of cryptographic protocols and algorithms' security properties.

Authors in [20] introduced an automated alternative approach for supporting the early stages of the security verification process in chains. The proposed strategy analyzed the control and data planes, which included various security algorithms established in chains as security functions.

The SAT-based Model-Checker (SATMC) was suggested by the authors in [21] as a systematic verification method for verifying the correctness of critical security systems. Security protocols, business processes, and application programming interfaces for security were all included (APIs).

## III. METHODOLOGY

This section introduces the proposed method to verify the correctness of the IoT-EAA mathematically through two phases which can be classified into two sub-sections. The first subsection introduces the mathematical description of the IoT-EAA architecture model, and the second subsection will illustrate Modelling and Verifying IoT-EAA Architecture using Event-B.

### A. Mathematical Description for the IoT-EAA Architecture

This section describes the IoT-EAA architecture's mathematical description, including its composite entities and operational functions. The key physical and virtual components of the IoT-EAA architecture are also explained below.

- Definition1: (service Application layer) that is defined as a three-tuple.

$$A = [A_{id}, A_{type}, A_{sp}]$$

Where  $A_{id}$  denotes the application ID and  $A_{type}$  denotes the purpose for which the application is used (such as medicine, education, finance, entertainment, utility, and gaming).  $A_{sp}$  specifies the minimum system requirements for running the application, such as the Processor, primary memory, and secondary storage requirements, as well as the operating system version.

- Definition2: (Network communication layer) is defined as a six-tuple.

$$NC = [ND, S, T, T_s, R, D]$$

Where ND is Network devices that called routers are used to direct packets between networks. Also, S denotes the Source, which generates data to be transmitted (sensors or actuators), and T is the Transmitter that Converts data into transmittable signals through  $T_s$ , which the Transmission System that Carries data to the R Receiver to Convert the received signal into data and received it to the D the Destination that Takes the incoming data.

- Definition3: hardware layer denoted by HW and defined as a three-tuple.

$$HW = [HW_{id}, HW_{st}, HW_{type}]$$

where,  $HW_{id}$  is an integer that represents the hardware's unique ID.

$HW_{st}$  represents whether the hardware is in an active or inactive state, and is represented as a Boolean,  $HW_{st} = \{0, 1\}$ , where the values 0 and 1 symbolize the inactive and active states, respectively.

- Definition4: The specifications of the Hardware denoted by (HWtype) are represented as a six-tuple.

$$HW_{type} = [P, M, B, S, c, f]$$

where, P stands for the hardware processor specifications, which include information such as processor core speed, bus specifications, and internal register (cache memory) size. The memory size, memory clock, and data rate requirements for primary memory (RAM) are stored in M.

Tuple B contains information about the battery, such as voltage, size (AA or AAA), type (Ni or C electrodes), and the number of batteries needed is the symbolic representation of the various kinds of sensors that make up the node's sub-modules. The hardware used for wireless communication for the node, such as Bluetooth and ZigBee, is represented by the tuple c. f denotes the frequency range in which the HW runs.

- Definition5: connectivity management layer is defined as a two-tuple.

$$CM = [HM, NM]$$

Where the HM denoted the management of IoT hardware and NM denoted the management of Network communication.

Property1: The function of connectivity management, which manage the connection between HW and NC as represented in Equation (1).

$$F(CM): HM \longleftrightarrow NM \quad (1)$$

The operator  $\longleftrightarrow$  denoted the management of the connectivity between HW and NC layers.

Now all components of the IoT architecture will define in Equation (2).

$$IoT\ AR = \sum ((HW \succ NC) / CM) \succ A \quad (2)$$

The operator  $\succ$  denotes the existence of a successor relationship between two operands. For example,  $X \succ Y$  denotes that Y is a successor of X.

To satisfy the security in wholly the IoT architecture as represented in Equation (3).

$$IoT\ AR = \sum ((HW \succ NC) / CM) \succ A \Leftrightarrow S \quad (3)$$

The proposed theory for IoT security: the IoT application service satisfies a high degree of security if and only if secure the connection of hardware devices and network by managing the connection between them.

### B. Modeling and Verifying IoT-EAA Architecture using Event-B

Formal methods consider an important tool for providing quantitative statements about safety and security properties for the digital systems [22]. These methods are usually used to formally verify a model. Therefore, Model checkers and Theorem provers are two different types of Formal Method tools. In model checkers, a system's model verifies its state space exhaustively and automatically according to a given specification. Human expertise is often required by theorem provers to guide the proof of correctness by providing design and specification characteristics as algebraic constraints or theorem [23].

Some tools, such as AVISPA [24], Scyther [25], and Tamarin, concentrate on security protocols, while others, such as UPPAAL [26], PRISM [27], and Rodin platform [11], focus on Event-B modeling for statistical and probabilistic verification. When it comes to security design verification, the primary objective is usually to verify or falsify security properties such as secrecy and authentication.

Table I shows the various tools for verifying IoT protocols as well as the architecture for probabilistic/statistical model checkers.

According to Table I, the Event-B formal method will be used, which has the simulations and proof obligations that include both model checker the theorem prover that tends to verify the correction of the IoT-EAA architecture model.

TABLE I. PROBABILISTIC / STATISTICAL MODEL CHECKER

	UPPAAL	PRISM	Rodin
<b>Input language</b>	XTA and XML	PRISM language	Event-B language
<b>typical applications</b>	real-time controllers and communication protocols with critical timing aspects	verification of probabilistic real-time systems	Validation and verification of probabilistic real-time systems
<b>statistical model checking</b>	√	√	√
<b>probabilistic model checking</b>	✗	√	√
<b>Model Checker</b>	√	√	√
<b>Theorem Prover</b>	✗	✗	√
<b>Simulator</b>	√	√	√
<b>GUI</b>	√	√	√
<b>Case Studies</b>	√	√	√

The IoT-EAA is established in Event-B. To get a better overview of the IoT-EAA architecture, the Event-B refinement technique will be used to build the IoT-EAA Event-B model gradually and follow, down – top layers, at the initial model the down layer called the Hardware layer that defines the properties for different devices, which are used for data collection. Then go to the top layer in the contract model through two refinements called machine for network communication layer, which refines the machine for the hardware layer and sees the context for the network communication layer. As well as a machine for the service application layer that refines the machine for the network communication layer and sees the context for the service application layer.

To present the IoT-EAA architecture, additionally, introduce three incremental refinements of the IoT-EAA architecture model. These refinements implemented by Event-B modeling language to formalize the given architecture refinements implemented by Event-B modeling language to formalize the given architecture.

As shown in Fig. 2 the relationship between context and machine for IoT-EAA architecture is described. Machines and Event-B contexts are included in the model. The contexts contain all the required data structures and axioms to set up a machine.

The IoT architecture layer is implemented as events on the machine, and the properties that must be verified are written as invariants.

The Initial Model (Hardware layer): it contains several devices, practically; by using the Rodin platform in the preparation phase consisted of the device state on/off, An Event-B context declares a device state-defined using axiom3 for device state. An abstract model declares a list of variables defined by invariants (inv3 – inv8); as well as different events for the network communication layer and security as shown in Fig. 3.

Three events were introduced to one event to specify the desired functional behavior for the hardware layer of an IoT-EAA, As well as an event for the connectivity management layer and the security layer of an IoT-EAA. These events include guard(s) for enabling the given action(s) and the actions that define the changes to the states of the hardware layer. Here, we provide all events related to the hardware layer

(data collection, manage the connection, and security), the hardware layer machine component will be described.

The first refinement (Network Communication layer): this refinement refined the initial model behavior into two phases; one focus on the network communication and the other phase refined the connectivity management layer and security layer into several sub-events. Practically, in this refinement, which includes (manage connection and security) events.

As well as Two new events to specifying the desired functional behavior (send data and receive data) are introduced in the network communication layer. In this refinement, we define an enumerated set and a list of variables to formalize the network communication operations defined by invariants (inv1 – inv11) that will be described in Fig. 4.

The second refinement (Service Application layer): this refinement can refine the Network Communication layer by introducing detailed events for the Service Application layer such as an interface with end-users that able to be linked for the major gap between users and applications; as well as security events for the security layer. In this refinement, an enumerated set and a list of variables were defined to formalize the service application operations by invariants (inv1 – inv5) context and machine for these refinements will be described in Fig. 5.

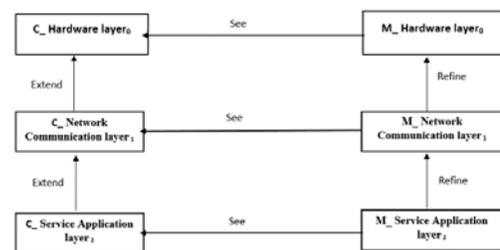


Fig. 2. Machine and Context Relationships for IoT- EAA Architecture.



Fig. 3. Variables and Invariants for the Hardware Layer.

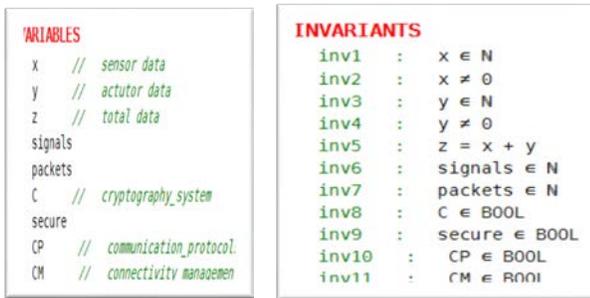


Fig. 4. Machine for Network Communication Layer.

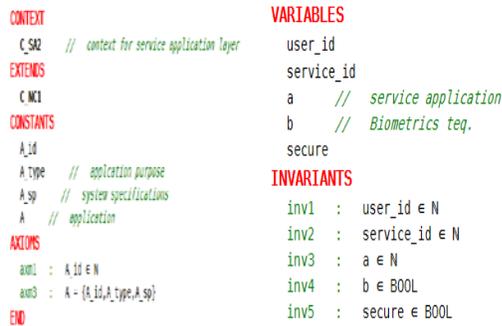


Fig. 5. Context and Machine for the Service Application Layer.

#### IV. VERIFICATION METHODS

In this section, we present the backbone of Event-B called a proof obligation generator [10]. This step runs after the static checker that checks the texts of the contexts and machines.

The validated models of IoT-EAA have together discharged 140 proof obligations, of which 82.35% proof obligations were automatically discharged through different Event-B provers. Well-definedness of predicates and expressions in invariants, guards, actions, variants, and witnesses for all events, feasibility checks, variable reuse check, guard reinforcing, and witness feasibility in refinements are all part of the proof obligations.

Variant checks for natural numbers and decreasing variants for convergent and predicted occurrences, theorems in axioms and invariant preservation for refinements and invariants used for verification of required security properties, theorems in axioms and invariant preservation for refinements and invariants used for verification of required security properties.

- Detecting some IoT security attacks using Event-B formal method.

IoT vision has been suffered from unprecedented attacks, which have resulted in the loss of privacy, organized crime, mental anguish, and the potential for human life to be jeopardized [28]. IoT has different attacks that occur in different IoT layers, one of these attacks called spoofing attack [29] is introduced, which considers a more dangerous attack for IoT applications.

Spoofing is the act of misrepresenting a communication from an unknown source as coming from a reliable source. Spoofing attacks can target a variety of domains, including emails, phone calls, and websites, or they can be more technical, like a computer spoofing an IP address; spoofing an email, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

On IoT nodes, a dynamic IP address attachment can be expanded from IPV4 to IPV6 when IPV4 addresses are insufficient for future requirements. Simple changes such as the IP stack are updated to support message exchange and avoid the use of complex cryptographic schemes for authentication.

To verify that the proposed method is useful for securing the IoT applications, various types of spoofing attacks are detected using the Rodin platform. We applied two types of spoofing attacks called “ip\_address\_spoofing” and “ARP\_spoofing.” Executing various runs and observing the sequence of events and variable values in each of these events will provide accuracy in securing the model.

By establishing a new event in the machine of the hardware layer for IoT\_EAA architecture detected the security error because the secure action must be “FALSE” (if the IP address for the hardware layer does not equal the IP address for the attacker device this considers conflict as well as event guard that is (if the security protocol sp is true then the security must be false) as illustrated in Fig. 6 with representing the mechanism of Event-B for detecting different types of spoofing attacks.



Fig. 6. Different Types of Spoofing Attack effect in Security.

#### V. CONCLUSION AND FUTURE WORKS

This paper looks at a vital application for the Formal Verification of IoT Architectures, focusing on security mechanisms. That is, different Event-B properties such as simulations, proof obligation, and invariant checking are used to verify the accuracy of the IoT-EAA architecture, which are then discharged in the Rodin platform to enhance security and detect security concerns at an early stage. Also, each IoT-EAA architecture layer's security issues will be discussed. Using the proposed method, various types of spoofing attacks were introduced in the Rodin platform. We verified that various security properties are discovered, as well as the proposed IoT Architecture (IoT-EAA) in general.

In future work, IoT-EAA architecture will be enhanced to cover all semantic IoT security properties. As well as using different verification methods to verify various types of IoT protocols.

#### REFERENCES

- [1] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi and T. Kamal, "A Review on Internet of Things (IoT)", International Journal of Computer Applications 113(1):1-7, 2015.
- [2] O. Mariya, and A. Rhattoy. "A secure model for machine to machine device domain based group in a smart city architecture." International Journal of Intelligent Engineering and Systems 12.1, 151-164, 2019.
- [3] M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi and T. Kamal "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications (0975 8887) Volume 111-No. 7, 2015.
- [4] S. Vashi; J. Ram; J. Modi; S. Verma; C. Prakash "Internet of Things (IoT): A vision, architectural elements, and security issues", In 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (pp. 492-496). IEEE, 2017.
- [5] Soumyalatha, S. G. Hegde, "Study of IoT: understanding IoT architecture, applications, issues and challenges", In 1st International Conference on Innovations in Computing & Net-working (ICICN16), CSE, RRCE. International Journal of Advanced Networking & Applications, May 2016.
- [6] M. Imdad, D. W. Jacob, H. Mahdin, Z. Baharum, S. M. Shaharudin, & M. S. Azmi, "Internet of things (IoT); security requirements, attacks and counter measures". Indonesian Journal of Electrical Engineering and Computer Science, 18(3), 1520-1530, 2020.
- [7] A. A. Elngar, E. K. Elsayed, & A. A. Ibrahim, "A New Efficient and Secure Architecture Model for Internet of Things". In International Conference on Innovative Computing and Communications (pp. 401-416). Springer, Singapore, 2020.
- [8] J.-R. Abrial, Modeling in Event-B: System and Software Engineering. Cambridge, U.K.: Cambridge Univ. Press, 2010.
- [9] A. S. A. Hadad, Ma, C., & A. A. O. Ahmed, "Formal Verification of AADL Models by Event-B". IEEE Access, 8, 72814-72834, 2020.
- [10] J. R. Abrial, M. Butler, S. Hallerstede, T. S. Hoang, F. Mehta, & L. Voisin, "Rodin: an open toolset for modelling and reasoning in Event-B", International journal on software tools for technology transfer, 12(6), 447-466, 2010.
- [11] Rodin: "A Tool for Event-B formal method". [Online]. Available: <http://wiki.Event-B.org/index.php/Rodin> Platform.
- [12] R. Mahmoud, T. Yousuf, F. Aloul, & I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE, 2015.
- [13] Khan, M. A., & Salah, K. "IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411, 2018.
- [14] A. W. Ahmed, M. M. Ahmed, O. A. Khan, & M. A. Shah, "A comprehensive analysis on the security threats and their countermeasures of IoT. International Journal of Advanced Computer Science and Applications, 8(7), 489-501, 2017.
- [15] I. Andrea, C. Chrysostomou, & G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges". In 2015 IEEE symposium on computers and communication (ISCC) (pp. 180-187). IEEE, 2015.
- [16] K. Hofer-Schmitz, & B. Stojanović, "Towards formal verification of IoT protocols: A review". Computer Networks, 174, 107233, 2020.
- [17] K. Hofer-Schmitz, & B. Stojanović, "Towards formal methods of IoT application layer protocols". In 2019 12th CMI Conference on Cybersecurity and Privacy (CMD) (pp. 1-6). IEEE, 2019.
- [18] M. Diwan, & M. D'Souza, "A framework for modeling and verifying IoT communication protocols", In International Symposium on Dependable Software Engineering: Theories, Tools, and Applications (pp. 266-280). Springer, Cham, 2017.
- [19] M. A. Al-humaikani, L. B. A. Rahim, A Review on the Verification Approaches and Tools used to Verify the Correctness of Security Algorithms and Protocols, International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 10, No. 6, pages 146-152, 2019.
- [20] N. Schnepf, R. Badonnel, A. Lahmadi, S. Merz, "Automated verification of security chains in software-defined networks with synaptic", Proc. IEEE Conference on Network Softwarization (NetSoft), 2017.
- [21] A. Armando, R. Carbone, L. Compagna, "SATMC: a SAT-based model checker for security protocols, business processes, and security APIs", Int. J. Softw. Tools Technol. Transf., Vol. 18, No. 2, 2016.
- [22] K. Keerthi, I. Roy, A. Hazra, and C. Rebeiro, "Formal verification for security in iot devices," in Security and Fault Tolerance in Internet of Things. Springer, pp. 179-200, 2019.
- [23] R. C. Armstrong, R. J. Punnoose, M. H. Wong, & J. R. Mayo, "Survey of existing tools for formal verification". SANDIA REPORT SAND2014-20533, 2014.
- [24] AVISPA. "A tool for Validation of Internet Security Protocols." [Online]. Available: <http://www.avispa-project.org/>.
- [25] Scyther: "A tool for the automatic verification of security protocols." [Online]. Available: <https://people.cispa.io/cas.cremers/scyther/>.
- [26] UPAAL: "A toolbox for modeling, simulation and verification of real time systems." [Online]. Available: <https://uppaal.org/>.
- [27] PRISM: "A tool for formal modelling and analysis." [Online]. Available: <https://www.prismmodelchecker.org/>.
- [28] H. A. Abdul-Ghani, D. Konstantas, & M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model", International Journal of Advanced Computer Science and Applications, 9(3), 355-373, 2018.
- [29] N. Wang, L. Jiao, P. Wang, M. Dabaghchian, & K. Zeng, "Efficient identity spoofing attack detection for iot in mm-wave and massive mimo 5g communication", In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE, 2018.

# Conceptual Model with Built-in Process Mining

Sabah Al-Fedaghi  
Computer Engineering Department  
Kuwait University  
Kuwait

**Abstract**—Process mining involves discovering, monitoring, and improving real processes by extracting knowledge from event logs in information systems. Process mining has become an important topic in recent years, as evidenced by a growing number of case studies and commercial tools. Current studies in this area assume that event records are created separately from a conceptual model (CM). Techniques are then used to discover missing processes and conformance with the CM, as well as for checks and enhancements. By contrast, in this paper we focus on modeling events as part of a tight multilevel CM that includes a static description, dynamics, events-log scheme, and monitoring and control system. If there is an out-of-model event log, it is treated as a requirement needed to build or enrich the CM. The motivation for such a unified system is our thesis that process mining is an essential component of a CM with built-in mining capabilities to perform self-process mining and attain completeness. Accordingly, our proposed conceptual model facilitates collecting data generated about itself. The resultant framework emphasizes an integrated representation of systems to include process-mining functionalities. Case studies that start with event logs are recast to evolve around a model-first approach that is not limited to the initial event log. The result presents a framework that achieves the aims of process mining in a more comprehensive way.

**Keywords**—Process-mining techniques; event log; conceptual modeling; static model; events model; behavioral model

## I. INTRODUCTION

Process mining [1] is a branch of data science concerned with the handling of event records produced during the execution of organization processes. It involves discovering, monitoring, and improving real processes by extracting knowledge from event logs in information systems [2]. Process mining has become an important topic in recent years, as evidenced by a growing number of case studies and commercial tools, such as the site maintained by the IEEE Task Force on Process Mining [3][4].

Event logs that characterize behavior have been used in such areas as program visualization and concurrent-system analysis to infer an approximation model (see Fig. 1) that can be relied upon for creating a more complete CM. In this paper, *events* refer to “*activities* executed by resources at particular times and for a particular case” [5] (*italics added*). A model is a description that provides a reasonably rigorous specification (in this paper, a diagrammatic one) of the static structure and behavior of a system. The model is a depiction of what a system should be doing and what it is actually doing. Here, an explicit separation exists between description and execution. However, we mix the *models* used to enforce the *process*

*execution* because they are necessarily synchronized. The execution is the activation of the model, and the model is a specification of the execution. We herein refer to processes occurring on a computer under the watchful eye of the system’s monitoring component. Fig. 1 shows our vision of the place of the CM in a system.

Current process-mining studies assume that event records appear *separately* from model events (Fig. 2). The process-mining technique then tries to discover missing processes and conformance with the model, as well as for checks and enhancements. An independent log system (e.g., manual) collects the events data. By contrast, in the approach presented in this paper, we construct a *thinging machine* (TM) model by analyzing requirements, including possible non-model logs. The model automatically generates data about its events (see Fig. 3) as part of a tightly integrated model (see Fig. 4).

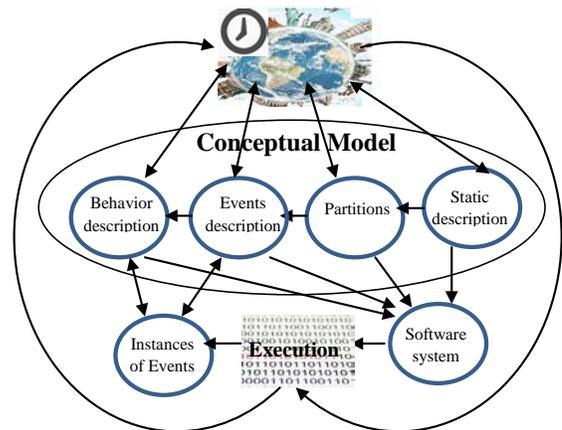


Fig. 1. General View of the Conceptual Model Position between Reality and Software System.

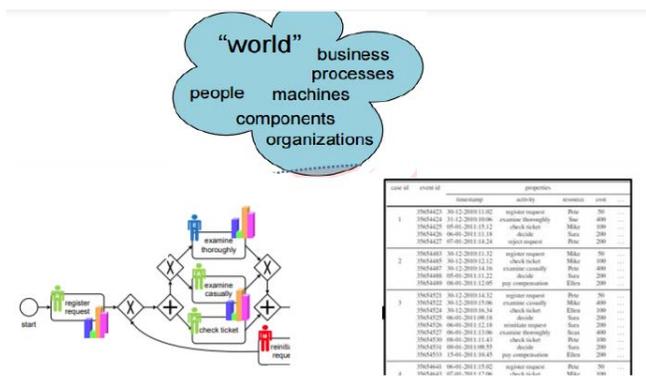


Fig. 2. Current Visualization of Process Mining.

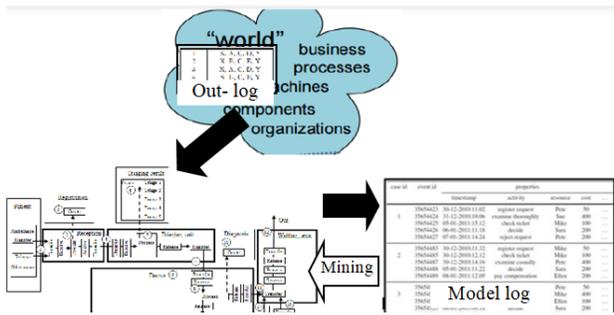


Fig. 3. TM Visualization of Event-Log System.

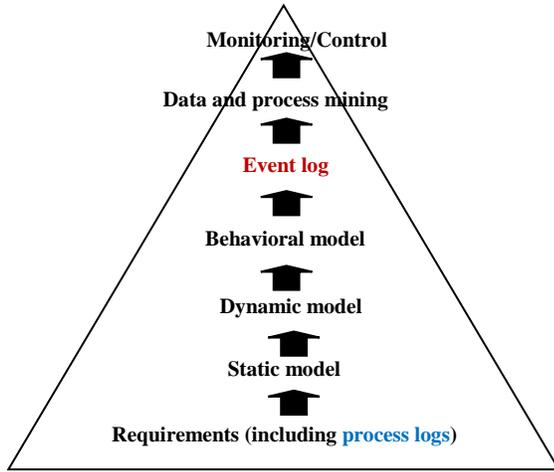


Fig. 4. The Position of Events in the System-Development Stages.

The TM model involves a static model of the relationships between *things* (to be defined later) through *machines* (to be defined later), a dynamic model of decompositions that embed behavior, event types, behavior in terms of chronology of events, an event log elicited from currently executed events, and a monitoring and control scheme that guides, enforces, or measures the execution. The motivation for such an integrated system is our thesis that if such an integrated model exists, it limits the need for model-less techniques for facilitating process-related problems (e.g., missing processes).

We claim that adopting an integral theoretical conceptual model takes care of tracing the process execution in the form of specifying all types of event streams (to be defined later). The events are generated by the event-log component as a part of the conceptual model function and not produced by an outside-log system. Note that the captured events in the log are already described in the *behavioral model* as some actions executed through time. The TM-based system can discover and treat issues such as a missing process.

The TM model includes only five generic actions that affect things: create, process, release, transfer, and receive. This specification contrasts with the ambiguous notion of activity (hence, the notion of event) used in current process-mining literature. If a process is missed in constructing such a model, then reexamining the model and its event logs is sufficient to make the model more complete. Such a procedure is similar to improving the dynamics of the model itself, such as changing the steps that are carried out in the model, and so

on. This approach is presented as an alternative to a “wild-goose chase” effort to discover processes using an event-log system. Suppose that one stream of behavior is  $A \rightarrow B \rightarrow C$ . Trying to run  $B \rightarrow C$  would be rejected because it is not an acceptable behavior (event stream). This is reported in the log component of the integrated model. Hence, the behavioral model may be modified to accept starting with B in addition to starting with A. Accordingly, the execution of the behavioral model would accept  $B \rightarrow C$  as an acceptable stream of events. In this case, a missing process is discoverable through its rejection as reported in the log component of the system.

In Section 2, we will briefly describe our main tool—that is, the TM model. The TM model has been applied in several diverse fields such as security [6] and privacy [7]. We provide a TM modeling example in Section 2 to clarify our notion of a conceptual model with built-in process mining. Section 3 applies our approach to a case study that is more complicated. Section 4 reviews related works.

## II. TM MODELING

The TM model articulates the ontology of the world in terms of an entity that is simultaneously a *thing* and a *machine*, called a *thimac* [8-11]. A thimac is like a double-sided coin. One side of the coin exhibits the characterizations assumed by the thimac, whereas, on the other side, operational processes emerge that provide dynamics. A thing is subjected to doing, and a machine does. The simplest type of machine is shown in Fig. 5. The actions in the machine (also called stages) can be described as follows:

**Arrive:** A thing moves to a machine.

**Accept:** A thing enters the machine. For simplification, we assume that all arriving things are accepted; hence, we can combine the arrival and accept stages into one stage: the **receive** stage.

**Release:** A thing is ready for transfer outside the machine.

**Process:** A thing is changed, but no new thing results.

**Create:** A new thing is born in the machine.

**Transfer:** A thing is input into or output from a machine.

Additionally, the TM model includes storage and triggering (denoted by a dashed arrow in this study’s figures), which initiates a flow from one machine to another. Multiple machines can interact with each other through movement of things or triggering. Triggering is a transformation from one series of movements to another.

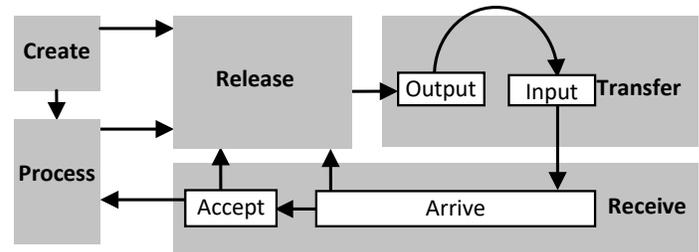


Fig. 5. The Thinging Machine.

**Example:** According to Weijters and Van der Aalst [12], “The models mined by process mining tools can be used as an objective starting point during the deployment of systems that support the execution of processes and/or as a feedback mechanism to check the prescribed process model against the enacted one.” Weijters and Van der Aalst [12] illustrate how process-mining techniques work using an example of the event log shown in Fig. 6. This log shows the events involved in applying for a license to ride motorbikes or drive cars as follows:

- X = Apply for license
- A = Attend classes on how to ride motorbikes
- B = Attend classes on how to drive cars
- C = Do theoretical exam
- D = Do practical exam to ride a motorbike
- E = Do practical exam to drive a car
- Y = Obtain result

Then, Weijters and Van der Aalst [12] construct a Petri net model that corresponds to the table in Fig. 7.

Instead, in TM, we consider the table in Fig. 6 to be collected data, along with other requirements gathered to develop the model of a license system. Thus, we minimally add new processes that make sense to achieve a reasonably complete model. Fig. 8 shows the resultant TM static model.

ID	Process instance
1	X, A, C, D, Y
2	X, B, C, E, Y
3	X, A, C, D, Y
4	X, B, C, E, Y
5	X, B, C, E, Y
6	X, A, C, D, Y

Fig. 6. Event Log (Adopted from [12]).

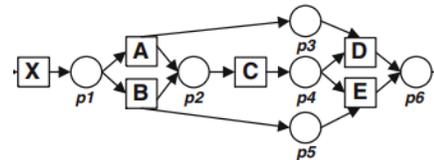


Fig. 7. Petri Net Model (Partial Adapted from [12]).

First, a person (circle 1) creates and sends an application to obtain a license (2). The application is received and is processed (3), and acknowledgement is sent to the applicant (4 and 5). The applicant (6) then attends classes on how to ride a motorbike (7) or how to drive a car (8).

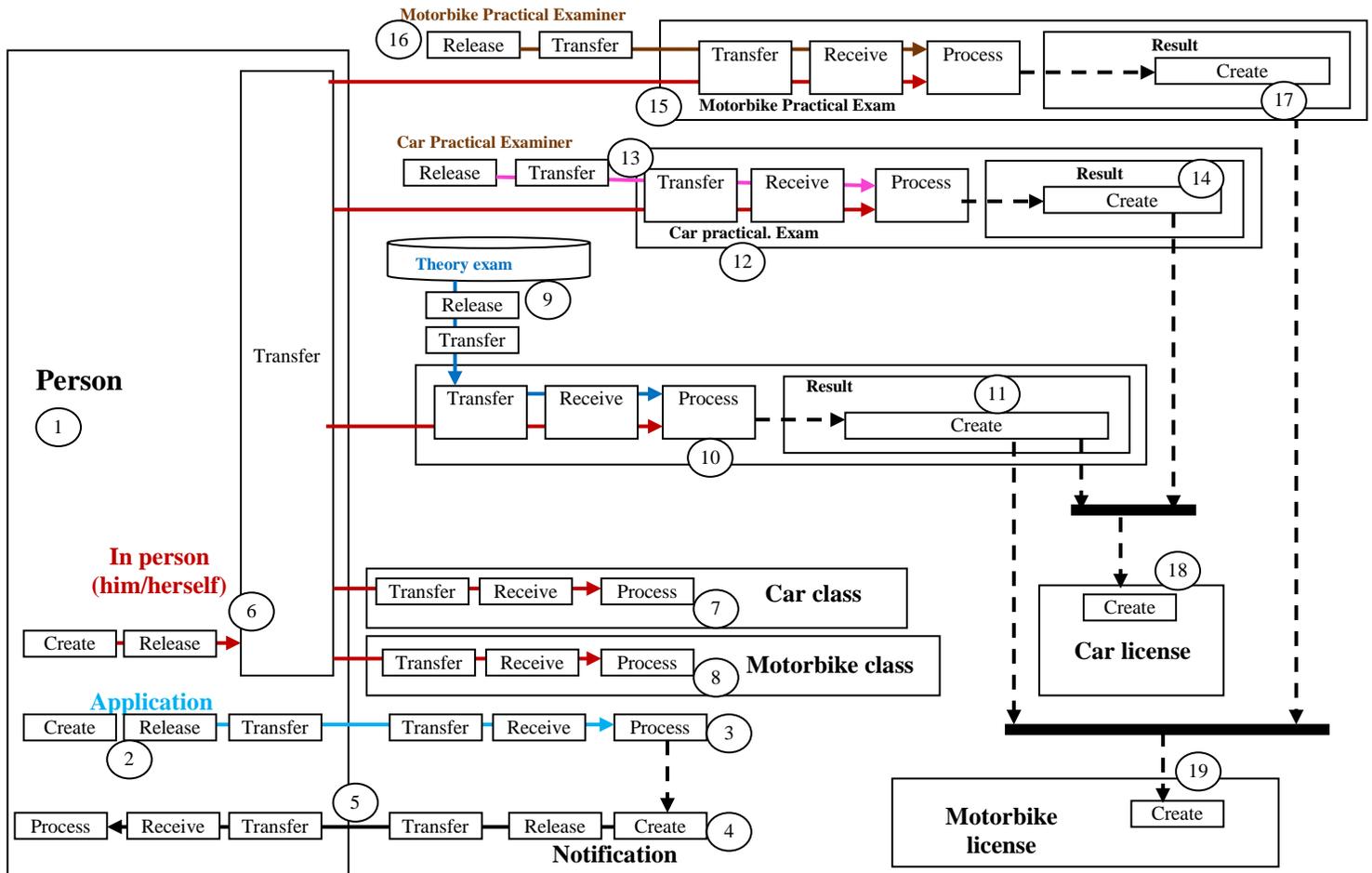


Fig. 8. The Static TM Model of the Licensing System.

Next, the applicant takes the theoretical exam (9 and 10) that generates a result (11). Assuming the applicant passes the theoretical exam, he or she goes on to the practical driving exam (12) performed by an examiner (13), which produces a result (14). Alternatively, the applicant goes on to the practical riding exam (15) performed by an examiner (16), which produces a result (17). The results of the theoretical exam (11) and the practical driving exam (14) lead to a driver's license (18). The results of the theoretical exam (11) and the practical riding exam (17) lead to a motorcycle rider's license (19).

Such an approach is different from the process mining of Weijters and Van der Aalst [12] because it builds a complete

model of the licensing system, which may use other typical requirement-collection methods. The next step in the TM approach is building the event-log scheme by finding all events in the static model of Fig. 8. This starts with identifying a set of events that are meaningful to the modeler. A TM event is defined based on (a) the region of an event, (b) the time of an event, and other attributes of events. Fig. 9 shows the representation of the event *A person applies for a license*. Accordingly, the static model is partitioned as shown in Fig. 10, where we assume that each partition (region) represents an event as follows.

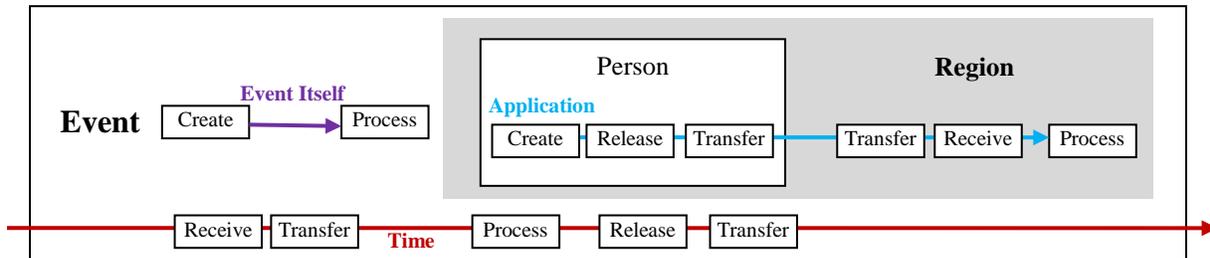


Fig. 9. The Event *A Person Applies for a License*.

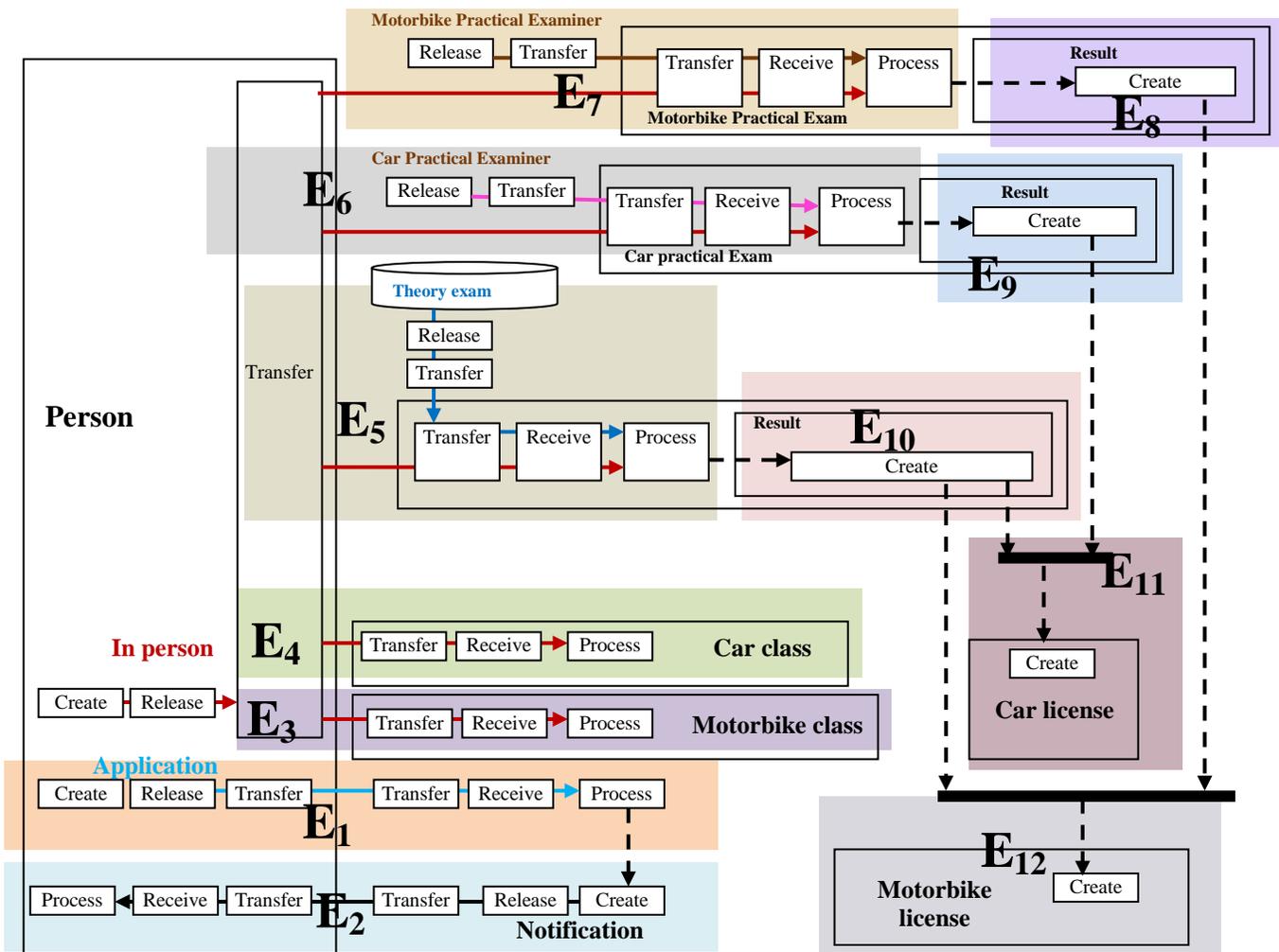


Fig. 10. The Static TM Model of the Licensing System.

- Event 1 ( $E_1$ ): A person applies for a license.
- Event 2 ( $E_2$ ): An acknowledgement is sent to the applicant.
- Event 3 ( $E_3$ ): The applicant attends classes on how to ride motorbikes.
- Event 4 ( $E_4$ ): The applicant attends classes on how to drive a car.
- Event 5 ( $E_5$ ): The applicant takes the theoretical exam.
- Event 6 ( $E_6$ ): The applicant takes the practical driving exam.
- Event 7 ( $E_7$ ): The applicant takes the practical riding exam.
- Event 8 ( $E_8$ ): The result of the practical riding exam appears.
- Event 9 ( $E_9$ ): The result of the practical driving exam appears.
- Event 10 ( $E_{10}$ ): The result of the theoretical exam appears.
- Event 11 ( $E_{11}$ ): The applicant obtains a motorbike license.
- Event 12 ( $E_{12}$ ): The applicant obtains a car license.

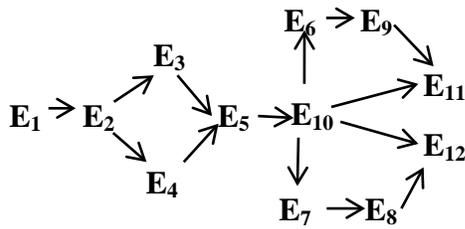


Fig. 11. The Behavioral TM Model of the Licensing System.

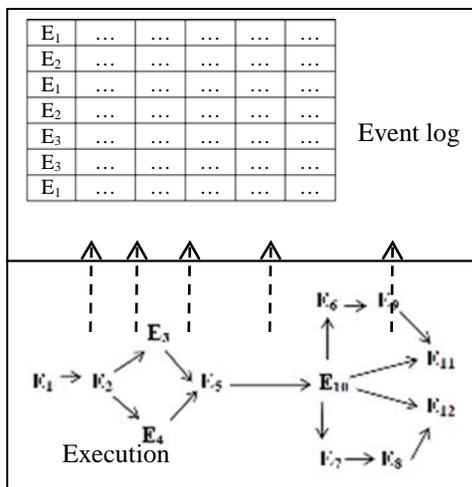


Fig. 12. The Execution of the System Generates Meta Events according to the Behavioral Model.

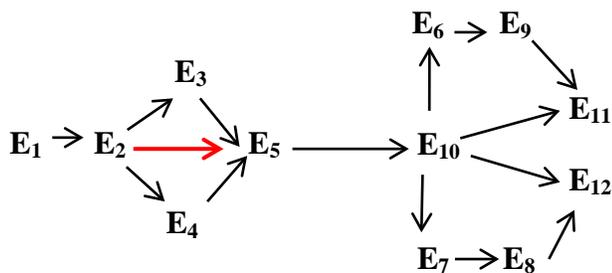


Fig. 13. The Behavioral TM Model of the Licensing System Such that a Person can take the Theoretical Exam without taking Classes.

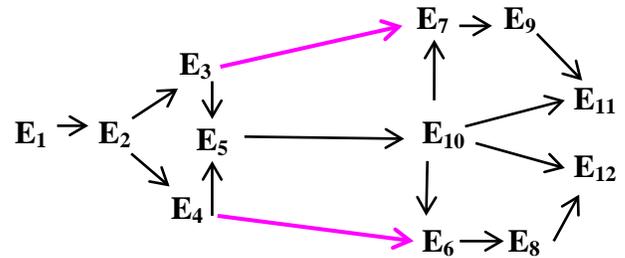


Fig. 14. The Behavioral TM Model of the Licensing System where the Theoretical Exam and Practical Exams are not in Any Particular Order.

Fig. 11 shows the behavioral model according to the chronology of events. At this stage, an event-log scheme can be developed to record each event. We call such a record a meta event as shown in Fig. 12. The set of meta events can be mined for various reasons, including process discovery. For example, suppose we have the event stream ( $E_1, E_2, E_5$ )—that is, an applicant applies for a license but then takes the theoretical exam without taking any classes. The monitoring system can easily recognize such a new behavior and reports it to the control system. Accordingly, a new process can be added to the behavioral model either automatically or manually (see Fig. 13). As another example, suppose that it is discovered from the event log that the theoretical exam and practical exam do not necessarily have to be in a particular order (e.g., a person can take the practical exam before the theoretical exam). Again, this can be discovered by mining the event log, and the behavioral model can be modified as shown in Fig. 14.

### III. HEALTH SYSTEM

In this section, we apply the TM approach introduced in the previous section to a large and real problem that involves health systems in four hospitals. According to Suriadi et al. [13] (see also Partington et al. [14]), variations in the treatment of patients across various hospitals substantially affect the quality and costs. The main research question is to identify the extent to which cross-hospital variations exist and why they exist. Suriadi et al. [13] used health care datasets to discover the pathways that patients traversed within hospitals. They compared process models and logs between various hospitals to identify subgroups (i.e., cluster of cases) that can explain the variations in patient flows.

In Suriadi et al.'s [13] case study, each hospital maintains an information system for managing operating theaters and tracking patient transfers between physical wards. The data extracted from these systems capture activities related to emergency department (ED) care. Suriadi et al. [13] excluded several cases (e.g., patient transfers and insufficiently documented cases).

A conceptual model is presented in terms of the UML class diagram (see partial view in Fig. 15). Despite the impressive work of Suriadi et al. [13] as a whole integration effort, we can see the typical assumption in many UML modeling projects in Fig. 15. Simply, the elementary conceptual notions are not in the right order. *Events*, an upper level notion, are mixed with static notions such as *patient* and

doctor. As demonstrated in the previous section on the licensing system, time is a global feature that lifts the whole model from staticity to dynamicity. In the class diagram of Fig. 15, events are treated as a mere class.

In our recasting of this health system, the TM model includes all processes in every hospital as a holistic virtual description of the union of all ED processes. Each hospital schema reflects a partial view of this encompassing model. Thus, there are partial event logs in various hospitals. If there is a difference among various EDs, it is a subsystem variation (e.g., some hospitals do not provide some services in the ED). If an emergency process (say, p1) exists in Hospital A but not in Hospital B, then p1 can be discovered from comparing the (static) processes in the global conceptual model.

A. Static Model

As shown partially in Fig. 16, Partington et al. [14] used BPMN. Fig. 17 shows the holistic TM static model of the EDs as described in Partington et al. [14]. This model is supposed to be built upon inspection of each hospital’s ED. Some details have been added to make the example more meaningful. In Fig. 17, a patient comes to the emergency unit by either an ambulance or other means (circle 1). In the reception, he or she is processed (2) to register the patient (3), and then he or she moves (4) to the triage unit where he or she is processed (5) to determine the degree of urgency (6). Accordingly, the patient then moves (7) to be processed (8) by a doctor (9) who writes a diagnosis (10). If some hospitals have additional processes (e.g., nurse processing), it is possible to add them to create a union for emergency operations that are not performed by Hospital 1.

Depending on the doctor’s diagnosis, the patient moves to

- a waiting area (11) before leaving the hospital (12) or
- the cardiac, medical, A&E or other unit (13–16).

The patient either goes to the waiting area (17) before leaving the hospital or goes to a ward, and then he or she goes to the waiting area to leave (18–19).

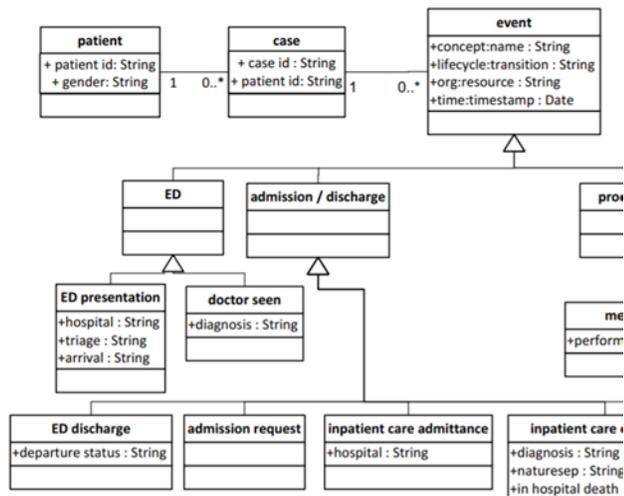


Fig. 15. Conceptual Model of the Event Log used in Suriadi et al. [13] case Study.

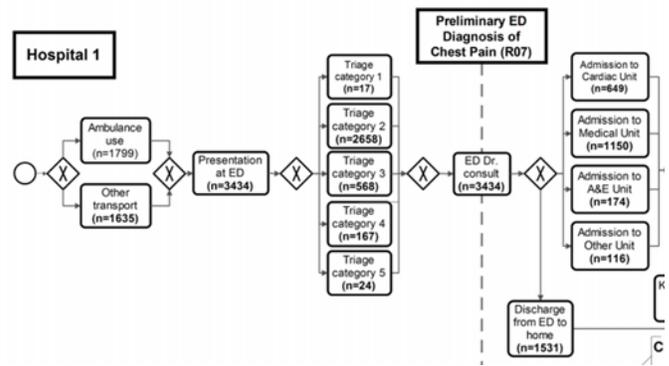


Fig. 16. Partial BPMN Model of Hospital 1 (partial, from [14]).

B. Dynamic Model

At this stage, the modeling reaches a critical point that leads to defining what an event is. As mentioned in the licensing system in Section 2, an event in TM is a region in the static model that involves time and possibly other properties (not discussed in this ED description). Fig. 18 shows the event *The patient moves from the triage unit to be processed by a doctor*. Accordingly, the static model of Fig. 17 is divided into the decompositions shown in Fig. 19, where we represent each event by its region as follows:

- Event 1 (E<sub>1</sub>): A patient arrives at the ED by ambulance.
- Event 2 (E<sub>2</sub>): A patient arrives at the ED by other means.
- Event 3 (E<sub>3</sub>): The patient is received and is registered.
- Event 4 (E<sub>4</sub>): The patient moves to the triage unit.
- Event 5 (E<sub>5</sub>): The patient is processed in the triage unit.
- Event 6 (E<sub>6</sub>): The patient moves from the triage unit to a doctor.
- Event 7 (E<sub>7</sub>): A doctor examines the patient.
- Event 8 (E<sub>8</sub>): The patient leaves the doctor after being processed (i.e., diagnosed).
- Event 9 (E<sub>9</sub>): The patient goes to the waiting area and then leaves the ED.
- Event 10 (E<sub>10</sub>): The patient goes to the cardiac unit.
- Event 11 (E<sub>11</sub>): The patient leaves the cardiac unit.
- Event 12 (E<sub>12</sub>): The patient goes to the medical unit.
- Event 13 (E<sub>13</sub>): The patient leaves the medical unit.
- Event 14 (E<sub>14</sub>): The patient goes to the A&E unit.
- Event 15 (E<sub>15</sub>): The patient leaves the A&E unit.
- Event 16 (E<sub>16</sub>): The patient goes to another unit.
- Event 17 (E<sub>17</sub>): The patient leaves the other unit.
- Event 18 (E<sub>18</sub>): The patient goes to the ward.
- Event 19 (E<sub>19</sub>): The patient dies in the ward.
- Event 20 (E<sub>20</sub>): The patient leaves the ward.

C. Behavioral Model

Fig. 20 shows the behavioral model in terms of the chronology of events. Each *stream* of events (the sequence of events for a single type of patient; e.g., E<sub>1</sub>, E<sub>3</sub>, E<sub>4</sub>, E<sub>5</sub>, E<sub>6</sub>, E<sub>7</sub>, E<sub>8</sub>, and E<sub>9</sub>) can be examined to see the process that a patient goes through. There are 40 types of event streams in Fig. 20. There are many *instances* of these types of streams. Any deviation from these streams results in alerts from the monitoring system. Note that each hospital has a sub-behavior of the global behavior. From such representation of events, we can discover a different or new ED behavior in one hospital,

as shown in Fig. 21 (red arrows). In this case, the indicated hospital does not have an ambulance service. Additionally, a physician immediately examines the received patient; thus, an arrow that bypasses triaging is added. The point here is that with such a TM representation of the behavioral model, it is easier to discover missing processes. This development of a

model is an alternative approach to chasing missing processes through the non-model-based event log. Thus, we expect that if all systems in the hospitals were remodeled using the TM model, the resultant behavioral representations would contrast with an overall model in the holistic system.

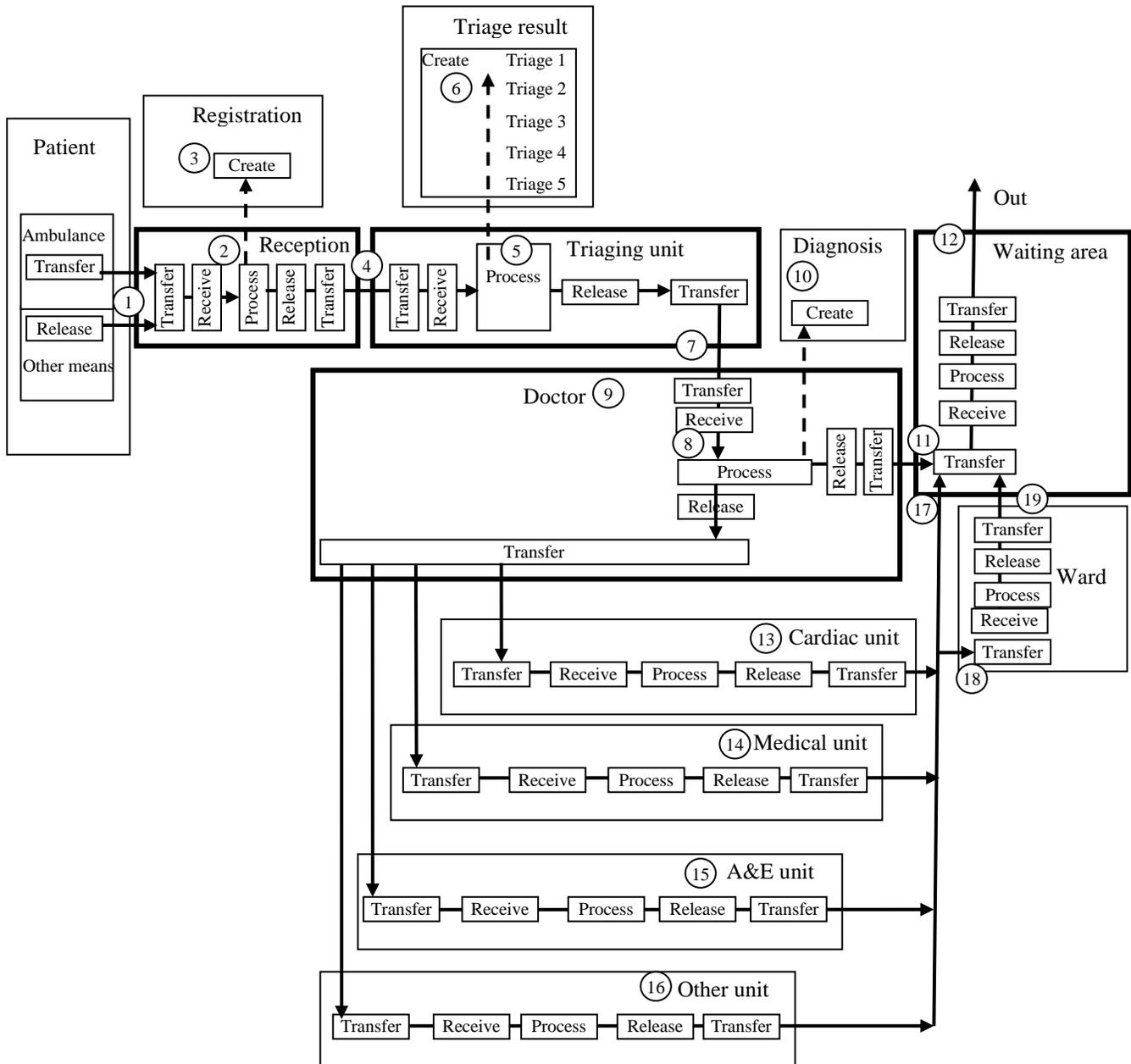


Fig. 17. The Static Model of the Emergency Department in a Hospital.

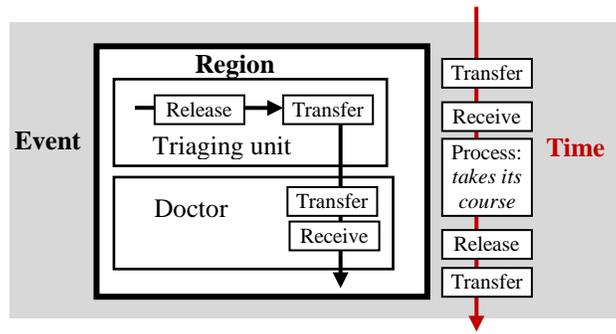


Fig. 18. The event the Patient Moves from the Triage Unit to be processed by a Doctor.

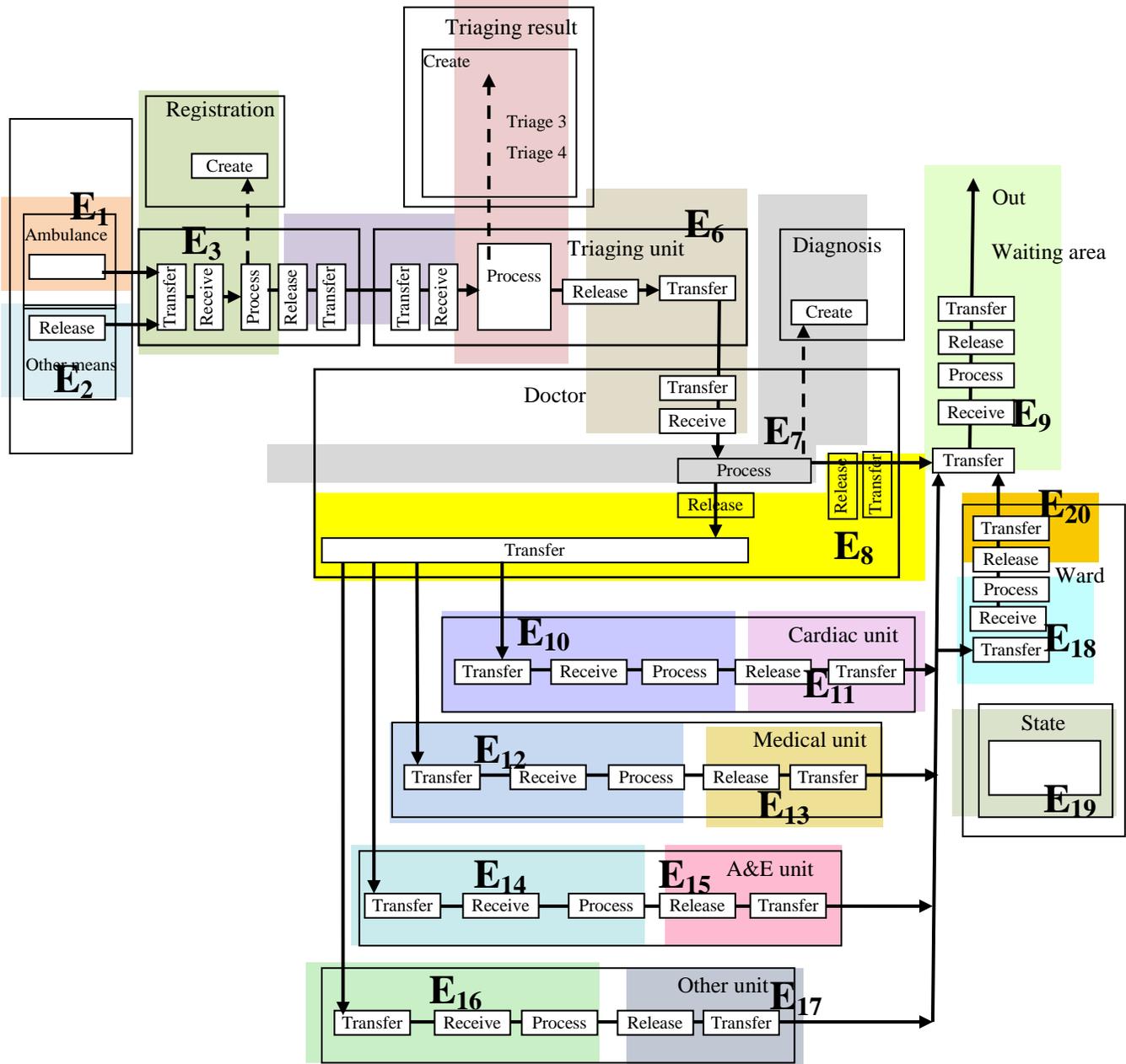


Fig. 19. The Dynamic Model of the Emergency Department in a Hospital.

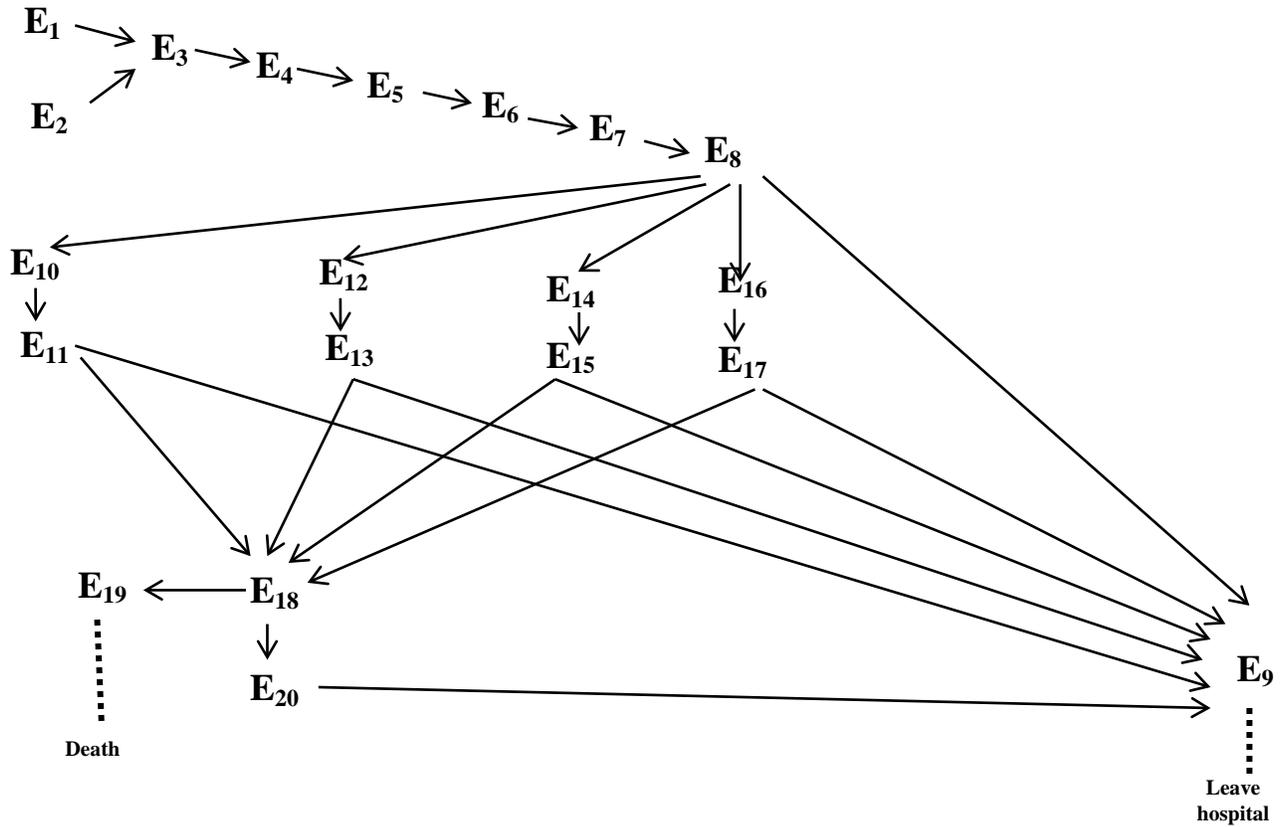


Fig. 20. The Behavioral Model of the Emergency Department in a Hospital.

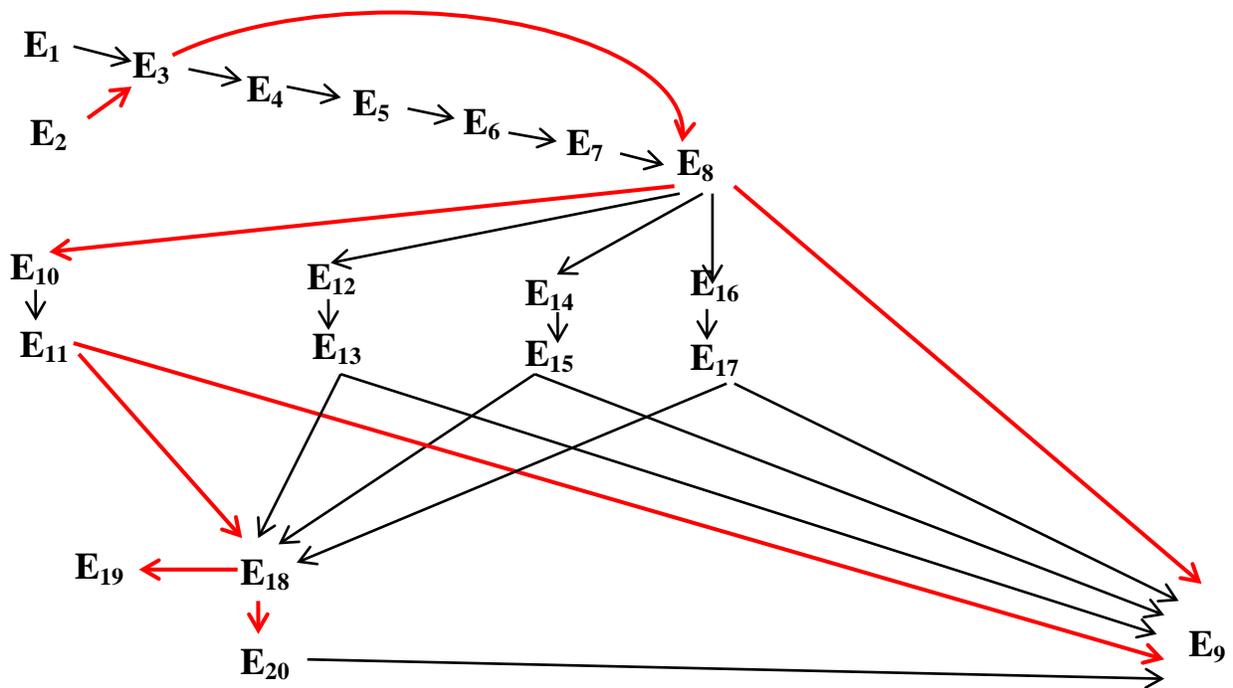


Fig. 21. Different Behavioral Model of the Emergency Department in a Hospital.

#### IV. RELATED MATERIALS

Most of the information systems used by organizations do not record the execution data in a process-centric way so that the data are not ready for process mining. Techniques for event-log preparation can be categorized into methods for event data extraction, correlation, and abstraction. Techniques in this area assign semantics to data elements by defining how they can jointly be interpreted as the execution of a business process activity [15][16].

Process mining provides a set of techniques and algorithms for process discovery, conformance checking, and enhancement [1][17].

- Process discovery aims at the creation of a process model automatically from the data recorded during process execution [4].
- Conformance checking processes the recorded data based on a process model and provides diagnostic results [18].
- Process enhancement enriches a given process model based on the recorded data [19][20], thereby providing a more complete process representation.

According to van der Aalst [1], despite the maturity of the individual process-mining techniques, considerable resources have to be allocated in process-mining projects for the extraction and preparation of event data before the actual analysis can even start. Process-mining techniques use different representations and make different assumptions, and users often need to resort to trying different methods in an ad hoc manner [5]. Finding, merging, and cleaning event data remain a challenge for the application of process-mining techniques [2].

#### V. CONCLUSION

In this paper, we have examined the notion of process mining. We proposed the conceptual TM model as a unifying description at the static, dynamic, and behavioral levels of the system with its own events-log component. Process mining takes place based on this event log of the system. A pre-model or out-of-model event log can be utilized in building the TM model. Once the model with its multilevel stages is built, then the model through its event-log component can mine its processes to discover new or missing processes that can be added, manually or automatically, to the specification of accepted behavior.

In this paper, we presented TM as a new model to be applied to process mining. Future research will elaborate on using TM in the process mining area with more complex examples. Specifically, TM needs to be related to such notions as process enhancement and conformance.

#### REFERENCES

- [1] W. M. Van der Aalst, "Data science in action," in *Process Mining*, 2nd ed., Berlin: Springer, 2016, pp. 3–23. . DOI 10.1007/978-3-662-49851-4\_1
- [2] W. Van der Aalst, A. Adriansyah, A. K. A. de Medeiros, and F. Arcieri, T. Baier, T. Blickle, et al. (78 co-authors). "Process mining manifesto," in *Business Process Management Workshops*, F. Daniel, K. Barkaoui, and S. Dustdar, Eds. Berlin: Springer, 2012, pp. 169–194.
- [3] M. Dumas and L. García-Bañuelos, "Process mining reloaded: Event structures as a unified representation of process models and event logs," in *Application and Theory of Petri Nets and Concurrency*, vol. 9115, R. Devillers and A. Valmari, Eds. Springer, 2015, pp. 33–48. . DOI 10.1007/978-3-319-19488-2\_2
- [4] A. Augusto, R. Conforti, M. Dumas, M. L. Rosa, F. M Maggi, A. Marrella, et al. (8 co-authors), "Automated discovery of process models from event logs: Review and benchmark," *IEEE Trans. Knowl. Data Eng.*, vol. 31, pp. 686–705, 2019. . DOI org/10.1109/TKDE.2018.2841877
- [5] W. M. P. van der Aalst, "Process discovery from event data: Relating models and logs through abstractions," *Data Min. Knowl. Discov.*, vol. 8, no. 3, February 2018. . DOI 10.1002/widm.1244
- [6] S. Al-Fedaghi, and A. Alrashed, "Threat risk modeling," 2010 Second International Conference on Communication Software and Networks, 26-28 Feb. 2010, Singapore, 405-411. DOI 10.1109/ICCSN.2010.29
- [7] S. Al-Fedaghi, G Fiedler, B Thalheim, "Privacy enhanced information systems," The 15th European-Japanese Conference on Information Modeling and Knowledge, In *Frontiers in Artificial Intelligence and Applications*, Volume 136: Information Modeling and Knowledge Bases XVII, 94-111. Y. Kiyoki, et al. (Eds), 94-111, IOS Press, 2006.
- [8] S. Al-Fedaghi, "Conceptual temporal modeling applied to databases," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, pp. 524–534, 2021. DOI 10.14569/IJACSA.2021.0120161
- [9] S. Al-Fedaghi, "UML modeling to TM Modeling and back," *IJCSNS International Journal of Computer Science and Network Security*, vol. 21, no. 1, pp. 84–96, January 2021. DOI 10.22937/IJCSNS.2021.21.1.13
- [10] S. Al-Fedaghi and M. AlSaraf, "High-level description of robot architecture," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 10, pp. 258–267, 2020. DOI 10.14569/IJACSA.2020.0111035
- [11] S. Al-Fedaghi, "Conceptual software engineering applied to movie scripts and stories," *J. Comput. Sci. Technol.*, vol. 16, no. 12, pp. 1718–1730, 2020. . DOI 10.3844/jcssp.2020.1718.1730
- [12] A. J. M. M. Weijters and Wil Van der Aalst, "Genetic process mining: A basic approach and its challenges," in *BPM 2005 Workshops, LNCS 3812*, C. Bussler et al., Eds. Berlin: Springer-Verlag, 2006, 203–215.
- [13] S. Suriadi, R. S. Mans, M. T. Wynn, A. Partington, and J. Karnon, "Measuring patient flow variations: A cross-organisational process mining approach," in *Asia Pacific Bus. Rev.*, C. Ouyang and J. Y. Jung, Eds. Lect. Notes Bus. Inf. Process, vol. 181. Cham: Springer, 2014, pp. 43–58. . DOI 10.1007/978-3-319-08222-6\_4
- [14] A. Partington, M. Wynn, S. Suriadi, C. Ouyang, and J. Karnon, "Process mining for clinical processes: A comparative analysis of four Australian hospitals," *ACM Trans. Inf. Syst.*, vol. 5, no. 4, 1–18, 2015.
- [15] D. Kiarash, K. Batoulis, M Weidlich, and M. Weske, "Extraction, correlation, and abstraction of event data for process mining," *WIRES Data Min. Knowl. Discov.*, vol. 10, no. 3, ay/June 2020. . DOI doi.org/10.1002/widm.1346
- [16] S. Mandal, "Events in BPMN: The racing events dilemma," in 9th Central European Workshop on Services and their Composition (ZEUS), O. Kopp, J. Lenhard, and C. Pautasso, Eds. Lugano, Switzerland, 13–14 February, 2017, 23–30.
- [17] O. Etzion and P. Niblett, *Event Processing in Action*. Stamford, CT: Manning Publications, 2011.
- [18] J. Carmona, B. F. van Dongen, A. Solti, and M. Weidlich, *Conformance Checking: Relating Processes and Models*. Switzerland: Springer Nature, 2018. . DOI 10.1007/978-3-319-99414-7
- [19] M. Leoni and F. Mannhardt, "Decision discovery in business processes," in *Encyclopedia of Big Data Technologies*, S. Sakr and A. Zomaya, Eds. Cham: Springer, 2018, . DOI 10.1007/978-3-319-63962-8\_96-1
- [20] B. Depaïre and N. Martin, "Data-driven process simulation," in *Encyclopedia of Big Data Technologies*, S. Sakr and A. Zomaya, Eds. Cham: Springer, 2018, . DOI 10.1007/978-3-319-63962-8\_102-1

# Modeling a Functional Engine for the Opinion Mining as a Service using Compounded Score Computation and Machine Learning

Rajeshwari D<sup>1</sup>

Research Scholar, ATMECE, Assistant Professor,  
Department of Information Science & Engineering,  
NIE Institute of Technology, Mysuru, India

Puttegowda.D<sup>2</sup>

Professor & Head, Department of Computer Science &  
Engineering, ATMECE, Mysuru, India

**Abstract**—The ever-growing use of the digital platform for the various walks of the applications, primarily on the collaborative platforms of e-commerce, e-learning, social media, blogging, and many more, produces a large corpus of unstructured text data. Many potential strategic solutions require an accurate and fast classification process of the Opinion's text corpus hidden patterns. In-premise applications have various real-time feasibility constraints. Therefore, offering an Opinion as a Service on the cloud platforms is a new research domain. This paper proposes a design framework of the evolution of the classification engine for opinion mining using score-based computation using a customized Vader algorithm. Another method for scalability is a machine learning model that supports a large corpus of unstructured text data classifications. The model validation is performed for the various complexes, unstructured text datasets with the different performance metrics of the cumulative score, learning rate, loss function, and specificity analysis. These metrics indicate the models' stability and scalability behaviors and their accuracy and robustness across different datasets.

**Keywords**—Text mining; opinion; sentiments; machine learning; unstructured data; cloud services

## I. INTRODUCTION

The evolution of web2.0 and Cloud has brought a complete change in the digital system's development and production [1]. Global resource constraints and economic liberalization lead to realizing a collaborative business model. A highly distributed production-distribution and consumption market require an ecosystem of technology that has high availability and scalability—Cloud computing service offerings cater to these demands [2]. The competitive environment of cloud service providers (CSP) and the enterprise demands various services apart from the Cloud's traditional offerings. The evolution of the words' representation into vectors provides an ease to process the word corpus and leads a technology, namely text analytics. Various open platforms offer a facility to express the feedback or textual expression in many contexts of the brand-building process, marketing, or product campaign. The corpus of the text contains the hidden treasure of the Opinion. It is not economically feasible for the individual organization to set up dynamically evolving methods for the opinions mining as in-premise computing infrastructure. Therefore, the CSPs are in the process of building an ecosystem to offer Opinion-Mining as a Services (OMaaS). This paper proposes an architectural

model for the Opinion-Mining design as a Service (OMaaS) offering from the CSPs. The basic workflow diagram of the 'OMaaS' is as in Fig. 1.

The framework for the OMaaS provisions a system to acquire the Cloud users (CS) text corpus (Tc) through a dedicated channel with the dashboard of the virtual layer (VL) to the cloud data store. It handles the large corpus that further gets synchronized to the cloud data text analytics Engine (TAE), where the opinion mining's effective algorithm gets executed. Finally, the respective  $CS_i \in \{CS\}$  gets the visual or statistical representation of the mined Opinion from the respective Tc. Such a model's overall success largely depends upon how effective, and in a scalable manner, the view is mined on a real-time basis.

Many ubiquitous applications are conceptualized, where text analytics plays very crucial roles. Many of such application may include: i) Dynamic info-system on the dashboard of the vehicles, ii) business strategic decision tools, iii) topic modeling, iv) summarization, v) patent data matching, vi) health care decision support system, vii) the forensic tool, viii) decision making based on feedback – sentiment analysis, ix) political campaign, x) historical literature analysis, xi) visual search. Section II describes various researches that took place in the field of text analytics in a different context. Section III provides the descriptions of the diverse dataset taken into consideration for the model variation followed by the Sections IV and V for the two respective models of cumulative score and machine learning-based classification algorithms as a proposed engine Opinion mining to be synchronous with the OMaaS. Finally, Section VI discusses the results and analysis, followed by a conclusion in Section VII.

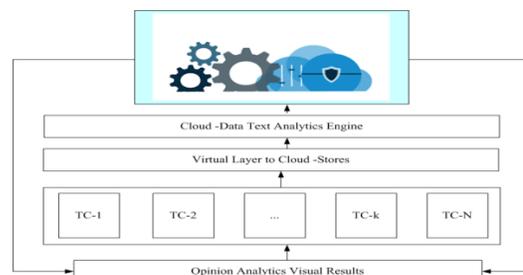


Fig. 1. Workflow Process Diagram of OMaaS.

## II. REVIEW OF LITERATURE

The use of text-data from social media like Facebook and other feeds and surveillance camera images (Neuhold et al., 2018) is found. The text analytic is exploited to display the road condition on the dashboard [3]. The big-data and the business complement's process management complement if the text generated is adequately analyzed [4]. A tree-based visual representation of text is being practiced, but this method is not scalable [5]. In research, the usual challenges to the researchers are to handle a large query result. The bag of words, along with natural language processing and visual analytics, is being studied in the work of Benito et al., (2019) [6]. Basole et al., (2019), has reviewed topic modeling on an extensive text description used in a business domain based on text analytics [7]. Summarization or building abstraction of a large document is beneficial to grab quick knowledge. Text analytics is used by Han et al., (2020) in their work [8]. Reghupathi et al., (2018), has examined the use of text analytics on patent data corpora using a concept like a word count and co-occurrence and the machine learning model [9]. Health care industries are another domain which produces a vast amount of unstructured text data (Kumar et al., 2019), has performed text analytics for decision support system [10].

The use of sequence-to-sequence learning in text analytics is becoming popular to build many text analytics-based applications with higher accuracy and lower training time (Keneshloo et al., 2019) [11]. Many giants like Facebook and Google use text analytics for their respective goals. Similar benefits can be achieved in further education, banking, and marketing sectors [12]. The forensic sector benefits if the complex text data from various communication sources are being analyzed (Koven et al., 2019), devices a tool that uses text analytics on the email data corpus [13]. Nowadays, the topic modeling algorithm is gaining popularity (El-Assady et al., 2018), proposes a decision-making technique based on relevant feedback using text analytics [14]. The study of sentiment analysis in crowdfunding is presented by (Wang et al., 2017) [15]. Media is another domain where a large corpus of text data is generated. Text analytics facilitates benefits on the topic description of an event as in the work of (Lu et al., 2018) [16]. Text analytics has also shown its benefits in the political election campaign (Gad et al., 2015), proposes an analytics tool for the visual representation of the social message trend [17].

The analysis of semantic with its content plays a vital role in content analysis [18]. Ojo et al., (2019), present patient sentiment analysis using textual data [19]. Karam et al., (2016), proposes a design of new hardware that supports the ecosystem of processor and memory for test analytics [20]. Vatrapu et al., (2016), explores set theory-based visualization to complement text analysis [21]. The sedimentation-based visualization concept of coordinated structure in text analysis has been studied by Liu et al., 2016 [22] and Sun et al., (2016) [23], respectively. Different regional history analysis is possible by text data analysis such study for Roman history is being carried out in the work of Cho et al., (2016) [24], various web-based visualization tool and fundamentals of visual text analytics are described in the work of Liu et al., (2019) by analyzing a large corpus of published papers using

concurrency relationship [25]. The basic features like parts of speech, text color, and font size make the corpus complex; an extensive survey is being conducted by Strobelt et al., (2106), different understanding highlighting, and visual search techniques [26]. In most text analytic methods, structuring the respective word with their meaning is crucial to arrive at an efficient qualitative and quantitative representation to achieve accuracy like a human [27].

## III. DATASET DESCRIPTION

The OMaaS framework proposes two core models for the classifications, which use the following datasets for evaluating the algorithms for the text analytics engine for the opinion classifications: i) Partial Complex Text and emojis, ii) fastText Facebook's AI Research (FAIR) lab[28], iii) Opinion Data from the University of Illinois, Chicago[29]

## IV. MODELLING A COMPLEX CONTENT: HYBRID OPINION USING TEXT AND SYMBOL USING CUSTOMIZED VADER ALGORITHM

### A. Vector of Text Token (TTo)

The simulation environments are controlled by initializing a Mersenne Twister generator with seed '0' [30]. The system deals with the complex heterogeneous constructs using text token and the symbols as  $Cf = \{TUS\}$ , where T= text token and S= symbols, as nowadays it is a fashion that people express their statements or Opinion with the combined format of the text sentence partially and complement it with some symbols (shown in Table I).

TABLE I. ILLUSTRATES SOME TYPICAL EXAMPLES OF THE CONSTRUCT OF SUCH A DATASET

SL.	Construct	Real meaning
1	in office 😞 wait #weekend 😞	Bored in the office waiting for the weekend
2	#weekend 😄 😄 😄	Becoming happy for the weekend

The algorithm 1 is described below:

**Algorithm 1:** Generating Vector of Text token from Complex format(unstructured)

**Input:** Cf

**Output:** TTo

**Process:**

Start

Initialize Cf  $\leftarrow$  Fn

$tCf \leftarrow f1(Cf : \forall \text{ content } \in Cf)$

Tokenization:

TTo  $\leftarrow f2(\forall (Td) \in tCf)$

End

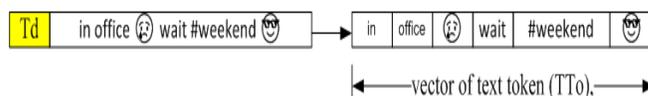


Fig. 2. TTo: Vector of Text Token  $\forall$  Text Data (Td)  $\in$  Cf.

In a start-up, the file containing the complex inputs of 'T' and 'S' as **F<sub>n</sub>** gets assigned in Cf's initialization. The 'Cf' transformation takes place into the tabular format for ease of computation, making the characteristics of  $\forall$  content  $\in$  Cf type: 'character' (**Ch**), and tCf represent the transformed format. To generate a vector of text token (TTo), the  $\forall$  text data (Td)  $\in$  tCf passes through a function of the document tokenization process (f2()), as shown in Fig. 2.

### B. Score Weightage

The score weightage (**Sw**) for  $\forall$  tokenized-Document (**tD**)  $\in$  TTo is computed using a popular "valence aware dictionary" for sentiment reasoning: "Vader" as customized Vader(**cV**) [31]. The large corpus of unstructured textual data transformation and gaining a quantitative ratio are the engine's main goals. In future applications, artificial intelligence (AI) based service are depicted as 'OaaS' models in the enterprises' CRM applications' intrinsic parts. The cV is basically a rule-oriented lexicon model (**ROLM**) based on the set of {**sL, gR, sYC**}, where, sL= 'sentiment lexicon, gR= 'grammatical rules and sYC= 'convention', such that sYC:  $\rightarrow$  {**s, P, s, I**}, such that s.P= polarity, s.I=intensity. The cV constructs a 'wordlist' with the wide-ranging list of feature-vector (Fv) such that Fv={Word(W), Phrases(P), Emo-icons (Ei), Acronyms (Ac)} with the rating of s. P and s.I in a -ve score to the +ve score, and the average is assigned as Sw. Vader's customization involves the handlers for the other parts of speech, characterization, and punctuations. The cV takes the entire tCf and their associated Fv and operates on {**s, P, s, I**} as per the specific rule sets. Finally, the summation of all the Fv scores gets normalized by scaling it in the range: **R** [-1 to 1] using equation (1) for the compounded score, Sc.

$$Sc = \frac{s}{\sqrt{s^2 + \beta}} \dots \quad (1)$$

**Algorithm 2:** Custom Vader algorithm for computing compound score Sc

**Input:** TTo

**Output:** Sc

**Process:**

*Start*

$cV \leftarrow \{sL, gR, sYC\}$

$sYC: \rightarrow \{s, P, s, I\}$

$Fv = \{(W), (P), (Ei), (Ac)\}$

$cV \leftarrow \{tCf, Fv\} : \rightarrow \{s, P, s, I\}$  as per the specific rule sets

*Normalize, Fv by scaling: R [-1 to 1]*

$\rightarrow$  using  $Sc = \frac{s}{\sqrt{s^2 + \beta}}$

*Update: Sc*

*End*

The value of  $\beta$  approximates the maximum probability of the expected cost of the score S. The algorithm is explained in algorithm 2, and the algorithm is implemented into two distinguished data set to measure the compound scores and the time computations. The results are described in Section VI of the results and discussion.

## V. MODELLING COMPLEX CONTENT: MACHINE LEARNING

### A. Auto Label Annotation for Data Model

The artificial intelligence research group (**FAIR**) by Facebook provides a model for creating a vector depiction of the equivalent word as a library. This library is popularly known as '**fast-Text**' and is used to learn text classification by different machine learning models (**MLM**). The system model takes the dataset provided by the University of Illinois, Chicago, namely: 'Opinion-Lexicon (**OL**),' which contains {6789} word list of both Class: {Negative (**Pw**), Positive (**Nw**)} as a text token (**Tt**) [32] sorted in the sequence of **a** $\rightarrow$ **z**. Further, a pre-trained model, namely, {'Word-Embedding'} provides an object named Dictionary (**Dc**) containing 9,99,994 tokens of words as string [33].

**Algorithm 3:** LabelAnnotation Data for Learning Model

**Input:** OL

**Output:** D<sub>la</sub>

*Start:*

$[Pw / Nw] \leftarrow f1(OL)$

$(W) mx 1 \leftarrow Pw \cup Nw$

$La (Undefined: La) \leftarrow f2((NaN) m, 1)$

$CLa \leftarrow La (Undefined: La): W$

$D_{la} \leftarrow W \cup CLa$

*End*

The explicit function f1() takes OL as an input argument, check the correctness of the files and convert  $\forall$  tokens (Tt)  $\in$  {Negative (Pw), Positive (Nw)} as a string and the concatenation of Pw  $\cup$  Nw, generates a list 'W' of size m x n, where n=1. Since the W  $\in$  {String Datatype}, therefore it is characterized as 'Not a Number (NaN),' a function f2() converts a list of 'NaN' of size (m x 1) into a list of Categorical variables to store the label annotation (La) for  $\forall$  Tt  $\in$  W. Further, the corresponding elements of the W are mapped:  $\rightarrow$  La as a categorical Labels (CLa) annotation. The pair of (W and CLa) provides Labelled Annotated data (**D<sub>la</sub>**) used for the Learning models.

### B. Token-based Filtering

The token-based filtering takes the Labeled Annotated data table (**D<sub>la</sub>**) from the previous procedure of Auto Label Annotation for Data Model. The explicit function f3() takes the **D<sub>la</sub>** as an input argument to return the tokenized documents (**D<sub>toc</sub>**), which is a set of {T1, T2, Tk, Tn}, where possible as per the text dataset T1 to Tn could be  $\in$  {#, , www.address.com,}. The process of the function f3() removes the stop words (SW) and also executes the process of stemming [34] or lemmatization [35]. Further, an additional argument passed to the f3() provides the BoW, which can be extended to multi-lingual analysis. Additionally, all the Unicode punctuations or symbols get eliminated after passing the D<sub>toc</sub> into the function designed to remove it. The English language has approximately 225 stop words eliminated from the updated D<sub>toc</sub> after passing a function that handles these stop words as a noise before further processing the text analytics. Finally, the noise processed D<sub>toc</sub> transforms into lower cases for further processing.

**Algorithm 4: Token-based filtering**

**Input:**  $D_{la}$   
**Output:**  $D_t$   
 Start  
 $D_{toc} \leftarrow f_3(D_{la})$   
 Update:  
 $D_{toc} \leftarrow$  punctuation removal ( $D_{toc}$ )  
 $D_{toc} \leftarrow$  Eliminate stop words ( $D_{toc}$ )  
 $D_{toc} \leftarrow$  Capitalized lower ( $D_{toc}$ )  
 Update:  $D_{toc}$   
 end

**C. SMO based Support Vector Machine Classifier**

The SMO based support vector machine classifier (SVMC) creates a dictionary(D) object from the pretrained fastText[28] word model(ftW). The ftW is a training model-1 which has already taken T1 time, and whenever a new dataset needs to be trained so if the transfer learning model[36] is used, then for a new training model as training model-2 takes T2 time, which is lesser time as  $T_2 < T$  as  $T = T_1 + T_2$  as in Fig. 3.

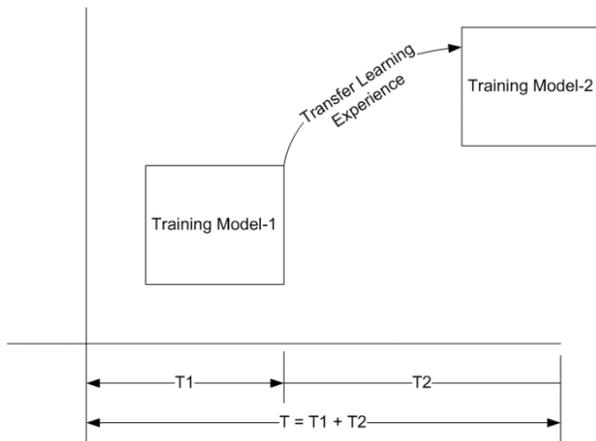


Fig. 3. Time Minimization for Training using a Transfer Learning Approach.

Algorithm 4 describes the process of the SMO-based support vector machine classifier building steps.

**Algorithm 5 : Text Classifier Learning Model**

**Input:** D,  
**Output:** tModel  
 Process:  
 $D \leftarrow$  ftW  
 Call Algorithm-3  
 $D_{la}(W, CLa) \leftarrow$  OL  
 Check:  
 $Idx \leftarrow$  not [ $d_{la}(W) \in D$ ]  
 $D_s \leftarrow$  num of W  
 Random Partition: Cross Validation  
 $[D\text{-train}, D\text{-test}] \leftarrow f(D_s, \text{num}W)$   
 $D\text{-train} \leftarrow$  Word2vector[D-train]  
 $Td \leftarrow [D\text{-train} \cup CLa]$   
 Train SVM- 1-Class-Binary Classifier  
 $tModel \leftarrow F(Td)$

The algorithm 3 LabelAnnotation Data for Learning Model provides  $D_{la} = \{W, CLa\}$ , further the indexes of all the words  $D_{la}(W)$ , which does not belong to the D created as  $Idx$ . The total data size  $D_s$  is the total number of word count  $\text{num}W$ . The  $D_s$  partitioning occurs for cross-validation as a random partition on  $D_s$  to define the partition for a statistical model ( $\{D\text{-Train}, D\text{-Test}\}$ ). The mapping processing of the words to the vector is an essential technique in NLP, which uses ANN to learn a large corpus of the text data, where every word is represented as a list of numbers as a vectorizing simple mathematical function that maps to a semantic similarity as  $D\text{-train} \leftarrow \text{Word2vector}[D\text{-train}]$  and finally the training input to the SVM classifier is obtained as  $[D\text{-train} \cup CLa] \rightarrow Td$ . With the Td, the support vector machine (SVM) classifier for one-class and binary classification is trained to get the text classifier model as  $tModel \leftarrow F(Td)$ . Fig. 4 and Fig. 5 show the hyper-parameter optimization results status.

The model t is trained on the low-dimension(Low-D) predictors by mapping the independent variables as predictors using a kernel() and support sequential -minimal optimizer(SMO) using an iterative-Single data kernel function or L1- softmargin minimization whose adjustments with every cycle is shown in Fig. 4 and 5. The confusion matrix for a different dataset for the test performance is described in the results section.

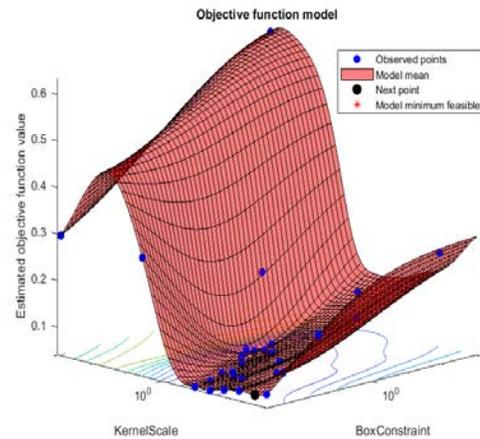


Fig. 4. Objective Function Model.

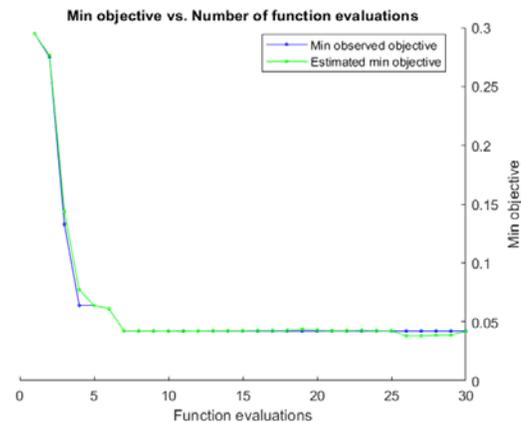


Fig. 5. Minimum Objective vs. Number of Functions Eval.

VI. RESULTS AND DISCUSSION

Fig. 6 and Fig. 7 represents the normalized compound scores for TTo with the number of token N= 60 and 1,60,0000, respectively.

The time of processing, including all the process of tokenization, score computation, and visual presentation, is tabulated in Table II below:

It is seen that when the dataset with 50 statements, each average statement time has taken is 3.8 seconds. In contrast, when evaluated on the complex text corpus of 160,0000 views, then the average time taken is 991 sec. Therefore, the consistency y is not maintained as the method is entirely rule-based, and the complexities of the text corpus also vary. For the scalability test, when the same dataset of 50 statements is made multiple copies of 50x, then the time to process is shown in the Table III and its variance as in Fig. 8.

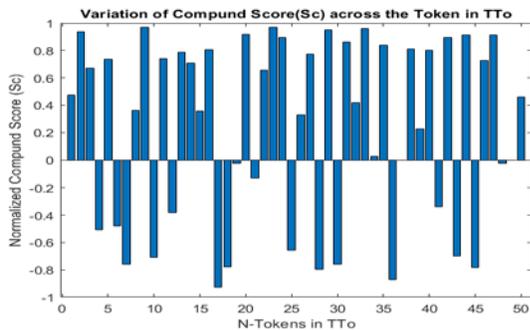


Fig. 6. Variation of Normalized Compound Score Sc across N-Token in TTo, N= 50.

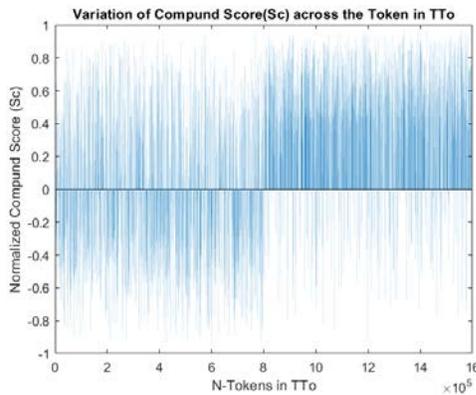


Fig. 7. Variation of Normalized Compound Score Sc across N-token in TTo, N= 160, 0000.

TABLE II. PROCESSING TIME FOR A SMALL AND LARGE COMPLEX DATASET

Sl. No	Size of the Token	Time to Process (in Sec)
1	50	13
2	1600000	1614

TABLE III. PROCESSING TIME FOR THE SCALABILITY TEST OF A UNIFORM DATASET

Sl. No	Size of the Token	Processing (in Sec)
1	50	0.33

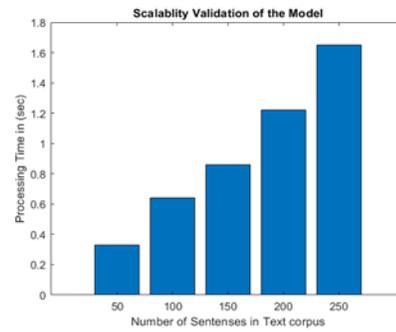


Fig. 8. Variance of Time to Process.

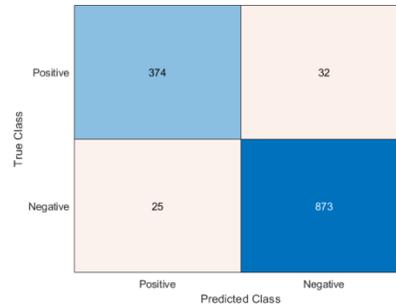


Fig. 9. Confusion Matrix between the Predicted Class and the True Class.

The SMO-based SVM model provides the following confusion matrix on Opinion Data's test data from the University of Illinois, Chicago [29]. The confusion matrix among the predicted class and true class is given in Fig. 9.

VII. CONCLUSION

The increasing corpus of text data brings challenges to the data storage and the text analytics' computational effort. These papers propose a framework for offering the Opinion Mining design process as a Cloud Services. The subscribers can avail themselves of fast and cost-effective services for the opinion analysis on their text corpus data. The paper proposes two distinguished methods as a Vedar based score computation and another as an SVM-based learning model as an opinion analytics engine. The score-based algorithm performs well on the small dataset, whereas the learning-based model is computationally effective on the large corpus.

The proposed algorithm for futuristic research can be considered with different datasets. Further, the given algorithm can be incorporated in other cloud services where opinion mining is necessary. Also, the security parameter can be incorporated in the ongoing and future researches in opinion mining.

REFERENCES

- [1] Duroao, Frederico, Jose Fernando S. Carvalho, Anderson Fonseca, and Vinicius Cardoso Garcia. "A systematic review on cloud computing." The Journal of Supercomputing 68, no. 3 (2014): 1321-1346.
- [2] Y. Hung, "Investigating How the Cloud Computing Transforms the Development of Industries," in IEEE Access, vol. 7, pp. 181505-181517, 2019, doi: 10.1109/ACCESS.2019.2958973.
- [3] R. Neuhold, H. Gursch, R. Kern and M. Cik, "Driver's dashboard – using social media data as additional information for motorway operators," in IET Intelligent Transport Systems, vol. 12, no. 9, pp.

- 1116-1122, doi: 10.1049/iet-its.2018.5337
- [4] S. Sakr, Z. Maamar, A. Awad, B. Benatallah, and W. M. P. Van Der Aalst, "Business Process Analytics and Big Data Systems: A Roadmap to Bridge the Gap," in IEEE Access, vol. 6, pp. 77308-77320, 2018. doi: 10.1109/ACCESS.2018.2881759
- [5] S. Liu, Y. Chen, H. Wei, J. Yang, K. Zhou, and S. M. Drucker, "Exploring Topical Lead-Lag across Corpora," in IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 1, pp. 115-129, 1 Jan. 2015. doi: 10.1109/TKDE.2014.2324581
- [6] A. Benito-Santos and R. Therón Sánchez, "Cross-Domain Visual Exploration of Academic Corpora via the Latent Meaning of User-Authored Keywords," IEEE Access, vol. 7, pp. 98144-98160, 2019. doi: 10.1109/ACCESS.2019.2929754
- [7] R. C. Basole, H. Park and R. O. Chao, "Visual Analysis of Venture Similarity in Entrepreneurial Ecosystems," in IEEE Transactions on Engineering Management, vol. 66, no. 4, pp. 568-582, Nov. 2019. doi: 10.1109/TEM.2018.2855435
- [8] Q. Han, D. Thom, M. John, S. Koch, F. Heimerl, and T. Ertl, "Visual Quality Guidance for Document Exploration with Focus+Context Techniques," in IEEE Transactions on Visualization and Computer Graphics, vol. 26, no. 8, pp. 2715-2731, 1 Aug. 2020.
- [9] V. Raghupathi, Y. Zhou, and W. Raghupathi, "Legal Decision Support: Exploring Big Data Analytics Approach to Modeling Pharma Patent Validity Cases," in IEEE Access, vol. 6, pp. 41518-41528, 2018. doi: 10.1109/ACCESS.2018.2859052
- [10] S. Kumar and M. Singh, "Big data analytics for the healthcare industry: impact, applications, and tools," in Big Data Mining and Analytics, vol. 2, no. 1, pp. 48-57, March 2019. doi: 10.26599/BDMA.2018.9020031
- [11] Y. Keneshloo, T. Shi, N. Ramakrishnan, and C. K. Reddy, "Deep Reinforcement Learning for Sequence-to-Sequence Models," in IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 7, pp. 2469-2489, July 2020. doi: 10.1109/TNNLS.2019.2929141
- [12] F. Amalina et al., "Blending Big Data Analytics: Review on Challenges and a Recent Study," in IEEE Access, vol. 8, pp. 3629-3645, 2020. doi: 10.1109/ACCESS.2019.2923270
- [13] J. Koven, C. Felix, H. Siadati, M. Jakobsson and E. Bertini, "Lessons Learned Developing a Visual Analytics Solution for Investigative Analysis of Scamming Activities," in IEEE Transactions on Visualization and Computer Graphics, vol. 25, no. 1, pp. 225-234, Jan. 2019. doi: 10.1109/TVCG.2018.2865023
- [14] M. El-Assady, R. Sevastjanova, F. Sperrle, D. Keim, and C. Collins, "Progressive Learning of Topic Modeling Parameters: A Visual Analytics Framework," in IEEE Transactions on Visualization and Computer Graphics, vol. 24, no. 1, pp. 382-391, Jan. 2018. doi: 10.1109/TVCG.2017.2745080
- [15] W. Wang, K. Zhu, H. Wang, and Y. J. Wu, "The Impact of Sentiment Orientations on Successful Crowdfunding Campaigns through Text Analytics," in IET Software, vol. 11, no. 5, pp. 229-238, 10 2017. doi: 10.1049/iet-sen.2016.0295
- [16] Y. Lu, H. Wang, S. Landis, and R. Maciejewski, "A Visual Analytics Framework for Identifying Topic Drivers in Media Events," in IEEE Transactions on Visualization and Computer Graphics, vol. 24, no. 9, pp. 2501-2515, 1 Sept. 2018. doi: 10.1109/TVCG.2017.2752166
- [17] S. Gad et al., "ThemeDelta: Dynamic Segmentations over Temporal Topic Models," in IEEE Transactions on Visualization and Computer Graphics, vol. 21, no. 5, pp. 672-685, 1 May 2015. doi: 10.1109/TVCG.2014.2388208
- [18] K. Kurzhals, M. John, F. Heimerl, P. Kuznecov and D. Weiskopf, "Visual Movie Analytics," in IEEE Transactions on Multimedia, vol. 18, no. 11, pp. 2149-2160, Nov. 2016. doi: 10.1109/TMM.2016.2614184
- [19] A. Ojo and N. Rizun, "Enabling Deeper Linguistic-Based Text Analytics—Construct Development for the Criticality of Negative Service Experience," in IEEE Access, vol. 7, pp. 169217-169256, 2019. doi: 10.1109/ACCESS.2019.2947593
- [20] R. Karam, R. Puri, and S. Bhunia, "Energy-Efficient Adaptive Hardware Accelerator for Text Mining Application Kernels," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 24, no. 12, pp. 3526-3537, Dec. 2016. doi: 10.1109/TVLSI.2016.2555984
- [21] R. Vatrapu, R. R. Mukkamala, A. Hussain and B. Fleisch, "Social Set Analysis: A Set Theoretical Approach to Big Data Analytics," in IEEE Access, vol. 4, pp. 2542-2571, 2016. doi: 10.1109/ACCESS.2016.2559584
- [22] S. Liu, J. Yin, X. Wang, W. Cui, K. Cao, and J. Pei, "Online Visual Analytics of Text Streams," in IEEE Transactions on Visualization and Computer Graphics, vol. 22, no. 11, pp. 2451-2466, 1 Nov. 2016. doi: 10.1109/TVCG.2015.2509990
- [23] M. Sun, P. Mi, C. North, and N. Ramakrishnan, "BiSet: Semantic Edge Bundling with Biclusters for Sensemaking," in IEEE Transactions on Visualization and Computer Graphics, vol. 22, no. 1, pp. 310-319, 31 Jan. 2016. doi: 10.1109/TVCG.2015.2467813
- [24] I. Cho, W. Dou, D. X. Wang, E. Sauda, and W. Ribarsky, "VAiRoma: A Visual Analytics System for Making Sense of Places, Times, and Events in Roman History," in IEEE Transactions on Visualization and Computer Graphics, vol. 22, no. 1, pp. 210-219, 31 Jan. 2016. doi: 10.1109/TVCG.2015.2467971
- [25] S. Liu et al., "Bridging Text Visualization and Mining: A Task-Driven Survey," in IEEE Transactions on Visualization and Computer Graphics, vol. 25, no. 7, pp. 2482-2504, 1 July 2019. doi: 10.1109/TVCG.2018.2834341
- [26] H. Strobel, D. Oelke, B. C. Kwon, T. Schreck, and H. Pfister, "Guidelines for Effective Usage of Text Highlighting Techniques," in IEEE Transactions on Visualization and Computer Graphics, vol. 22, no. 1, pp. 489-498, 31 Jan. 2016. doi: 10.1109/TVCG.2015.2467759
- [27] D. Park, S. Kim, J. Lee, J. Choo, N. Diakopoulos and N. Elmqvist, "ConceptVector: Text Visual Analytics via Interactive Lexicon Building Using Word Embedding," in IEEE Transactions on Visualization and Computer Graphics, vol. 24, no. 1, pp. 361-370, Jan. 2018. doi: 10.1109/TVCG.2017.2744478
- [28] "Fasttext", <https://fasttext.cc/docs/en/english-vectors.html>, Retrieved on 26-02-2021
- [29] "CS" <https://www.cs.uic.edu/~liub/FBS/sentiment-analysis.html>, Retrieved on 26-02-2021
- [30] X. Tian and K. Benkrid, "Mersenne Twister Random Number Generation on FPGA, CPU, and GPU," 2009 NASA/ESA Conference on Adaptive Hardware and Systems, San Francisco, CA, 2009, pp. 460-464, doi: 10.1109/AHS.2009.11.
- [31] Gilbert CH, Hutto E. Vader: A parsimonious rule-based model for sentiment analysis of social media text. In Eighth International Conference on Weblogs and Social Media (ICWSM-14). Available at (20/04/16) <http://comp. Social. gatech. edu/papers/icwsml4. vader. hutto. pdf> 2014 Jun (Vol. 81, p. 82).
- [32] Hu, M., and Liu, B., 2004, July. Mining opinion features in customer reviews. In AAAI (Vol. 4, No. 4, pp. 755-760).
- [33] Mikolov T, Grave E, Bojanowski P, Puhresch C, Joulin A. Advances in pre-training distributed word representations. arXiv preprint arXiv:1712.09405. 2017 Dec 26.
- [34] F. Heimerl, S. Lohmann, S. Lange, and T. Ertl, "Word Cloud Explorer: Text Analytics Based on Word Clouds," 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, 2014, pp. 1833-1842, doi: 10.1109/HICSS.2014.231.
- [35] Risch J, Kao A, Poteet SR, Wu YJ. Text visualization for visual text analytics. In Visual data mining, 2008 (pp. 154-171). Springer, Berlin, Heidelberg.
- [36] Zixuan Ke, Bing Liu, Hao Wang, and Lei Shu. Continual Learning with Knowledge Transfer for Sentiment Classification. to appear Proceedings of European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD-2020), Ghent, Belgium, 14-18, September 2020.

# Model for Predicting Customer Desertion of Telephony Service using Machine Learning

Carlos Acero-Charaña<sup>1</sup>, Erbert Osco-Mamani<sup>2</sup>  
Universidad Nacional Jorge Basadre Grohmann  
E.P. Informatica y Sistemas, Tacna-Peru

Tito Ale-Nieto<sup>3</sup>  
Universidad Privada de Tacna  
E.P. de Sistemas, Tacna-Peru

**Abstract**—In the present study, it is observed that many people are affected by the services provided by telephony, who leave the service for different reasons, for which the use of a model based on decision trees is proposed, which allows predicting potential dropouts from Customers of a telecommunications company for telephone service. To verify the results, several algorithms were used such as neural networks, support vector machine and decision trees, for the design of the predictive models the KNIME software was used, and the quality was evaluated as the percentage of correct answers in the predicted variable. The results of the model will allow acting proactively in the retention of clients and improves the services provided. A data set with 21 predictor variables that influence customer churn was used. A dependent variable (churn) was used, which is an identifier that determines if the customer left = 1, did not leave = 0 the company's service. The results with a test data set reach a precision of 91.7%, which indicates that decision trees turn out to be an attractive alternative to develop prediction models of customer attrition in this type of data, due to the simplicity of interpretation of the results.

**Keywords**—Software KNIME; Support Vector Machine (SVM); neural networks; decision trees

## I. INTRODUCTION

The study of churn or customer drop-out is an area in which large resources are invested year after year. Always, with the intention of being able to discover in advance, whether a customer will decide to switch from a company to their competition.

In particular, in the area of telecommunications, it has become increasingly necessary to study customer flight, given the high competitiveness that is developing globally. In the telecommunications industry from 2008 to 2010, customer leakage became 30% annual [13, 15] (pre-numerical portability studies). The objective of this article is to build mathematical models based on data to estimate the probability of customer desertion from telephone companies conditioned on the value of their individual and/or network attributes and/or since it has survived a given time in the company.

From the above, it follows that customer loss is an industry problem and where it becomes necessary to apply advanced tools that allows predicting and describe in some way, which customers have the greatest risk potential to change companies.

A classification tree allows you to visually set the conditions that a client must have to enter a dropout condition, while a neural network only eventually reports the result of the

prediction. Such differences are crucial when implementing preventive actions to prevent leakage [2]. In other words, the predictive model must not only perform well in classification, but also be interpretable to identify actions for customer tenure in the organization.

The mining technique selected for the design of the proposed predictive model is the classification type decision tree, because it is a predictive technique and the data available for model development correspond to categorical and discrete variables, which conform to the characteristics of a decision tree, in addition to the feasibility of interpreting the information obtained graphically [8].

The result of the application of the algorithm, allows build a decision tree which has the advantage of being easy to interpret and allows quickly and easily to the user, determine if a client, given a set of attributes that defines their historical behavior, is at risk of leaving the service [3].

On the other hand, data mining delivers promising results, we test models based on algorithms such as Neural Networks (ANN), Support Vector Machines (SVM) and Decision Tree, which our based model is expected to improve the limitations of traditional models.

## II. THEORETICAL FRAMEWORK

### A. Basics and Types of Customer Leakage

Customer flight, within telecommunications, occurs when a customer cancels the service provided by the company [10]. In such cancellation, the client can decide to resign from the company (voluntary), or the company can expel him (involuntary).

In particular, the connotation of churn refers to customer flight, so for the purposes of this study, churn is counted based on the customer's decision to leave the company by canceling a service. Also, churn can be understood as that term used to collectively describe the termination of services of a customer's subscription, where the customer is someone who has joined the company for at least a period of time ... a churner or fugitive is a customer who has left the company [6]. The main types of fugue according to [6, 12] are:

- Absolute: subscribers who have unlinked on the total database in a period.
- From line or service: This type of churn the number of discontinued services on the total database.

- Primary: Regarding the number of failures Secondary: Decrease in traffic volume.
- Package leak: This leak is characterized by the fact that plans and / or products change within the company [6].
- Company flight: Undoubtedly the most expensive, in this case the client escapes towards the competition, therefore, not only is the income not received, but also the company's prestige expressed in the participation of competing market.

### B. Predictive Models

Predictive analysis model is a name given to a collection of mathematical techniques with the common goal of finding a mathematical relationship between an objective, response or dependent variable and various predictive factors and independent variables, with the objective of measuring future values of these predictor factors and inserting them into the mathematical relationship to predict future values of the target variable. Since these relationships are never perfect in practice, it is desirable to give a measure of uncertainty in predictions [4].

To identify those factors that intervene in the prediction, they can be grouped into three categories: those that have little possibility of affecting the result, those with some certainty to affect the results and must be considered in the model and those that are in the middle, which may or may not influence the final result, being necessary to identify through a series of techniques whether they should be included in the model [4].

1) *Tree decision model*: Decision trees are defined as a recursive procedure, in which an 'N' number of instances are progressively divided into groups, according to a division rule that maximizes the homogeneity or purity of the response variable or class variable [6]. An advantage of decision trees is their easy interpretation, due to the graphic model that can be rescued from the result of the recursive partition.

When passing through each node of the tree the leaves are finally reached, which represent the final result of the fulfillment of all the conditions and which classify an instance in any of the states of the class variable as shown in Fig. 1. The only condition that partitions should be required to separate examples into different children, so that the cardinality of the nodes decreases as one descends the tree [8]. The construction of the decision tree is carried out through the partition algorithm that is explained in Fig. 2.

Based on the idea of looking for partitions that discriminate or achieve more pure nodes, numerous partition criteria have been presented, such as: Expected error criterion, Gini criterion and Entropy (Witten & Frank, 2005). These partition criteria look for the partition S that minimizes the function I (s) defined as follows [8]:

$$I(s) = \sum_{j=1..n} P_j * (P_j^1, P_j^2, \dots, P_j^c) \quad (1)$$

In Equation (1) (General Impurity Equation), n is the number of child nodes of the partition (number of partition conditions), P<sub>j</sub> is the probability of "falling" at node j, P<sub>j</sub><sup>1</sup> is the proportion of elements of class 1 at node j, P<sub>j</sub><sup>2</sup> is the

proportion of elements of class 2 at node j, and so on for the c classes. Under this general formula, each partition criterion implements a different function f, as shown in Table I [8].

The functions in Table I are called impurity functions and the function I (s), calculates the weighted average (depending on the cardinality of each child) of the impurity of the children of a partition.

The partition criterion used in this research corresponds to the Gini Index, since it is incorporated by default in the algorithm of the Decision Tree node of the KNIME software, the program used to design the predictive model of this study. This criterion compares the heterogeneity or impurity of the parent node with the sum of the impurities of the child nodes (Ramírez et al., 2009).

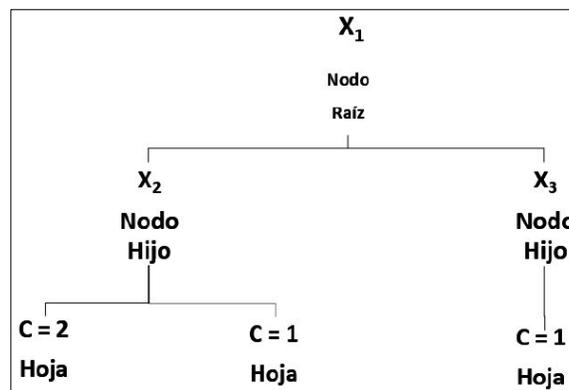


Fig. 1. Decision Tree Example, The Root Node is above the Tree. Internal Nodes (Decision Nodes) Correspond to Partitions on Particular Attributes. p.10, By Hernández et al., 2004, [8].

**ALGORITMO** Partición

**Input:** D conjunto de N ejemplos etiquetados, cada uno de los cuales está caracterizado por n variables predictoras X<sub>1</sub>,..., X<sub>n</sub> y la variable clase C.

**Output:** Árbol de clasificación.

**SI** todos los ejemplos de D son de la misma clase c => Asignar la clase c al nodo N.

**SALIR:** # Esta rama es pura, ya no hay que seguir partiendo. N es hoja.

**SINO:** -

Particiones: = generar posibles particiones.

Mejor partición: = seleccionar la mejor partición según el criterio de partición.

1. Seleccionar la variable que se adecúa mejor al criterio de partición X<sub>i</sub> con valores x<sub>i</sub><sup>1</sup>,..., x<sub>i</sub><sup>m</sup>.
2. Particionar D de acorde con los n<sub>i</sub> valores de x<sub>i</sub> en D<sub>1</sub>,..., D<sub>n<sub>i</sub></sub>
3. Construir n<sub>i</sub> subárboles T<sub>1</sub>,..., T<sub>n<sub>i</sub></sub> con los valores x<sub>i</sub><sup>1</sup>,..., x<sub>i</sub><sup>m</sup>

**FIN**

**FIN SI**

**FIN ALGORITMO**

Fig. 2. Decision Tree Learning Algorithm by "Partition" (Divide and Conquer), The Two Important Points for the above Algorithm to Work Correctly are the Partitions to Consider and the Partition Selection Criteria. p. 11, by Hernández et al., 2004. [8].

TABLE I. IMPURITY FUNCTION FOR EACH PARTITION CRITERION

Criterion	$f(P^1, P^2, \dots, P^c)$
expected error	$\min(P^1, P^2, \dots, P^c)$
GINI	$1 - \sum (P_j)^2$
Entropy	$\sum P_j * \log(P_j)$

Note: Impurity criteria functions for the Decision Tree search algorithm. by Ramirez et al., 2009 [8].

Partitions are a set of exhaustive and exclusive conditions. The more partitions that are allowed, the more expressive and precise the decision trees are. However, the more partitions the complexity of the algorithm is greater. [8].

2) *Artificial Neural Network-ANN model*: This data mining model is one of the most popular strategies for supervised learning and classification. However, due to its complexity, it is not possible to know exactly the origin of its results, which is a difficulty when explaining its operation. In a direct sense, an artificial neural network (or simply called neural network, or ANN) “consists of processing elements (called neurons) and the connections between them with coefficients (weights) linked to the connections, which constitute a neural structure, and a training and reminder algorithms attached to the structure” [14], which in simple words can be described as “a pool of simple processing units that communicate by sending signals between them over a large number of weighted connections” [1]. The following is a general diagram of this model in Fig. 3.

In neural networks, the multilayer Perceptron is one of the most used architectures for problem solving, due to its capacity as a fundamental approximation and its ease of use and applicability. This does not mean that it is a perfect implementation since it also has different problems and limitations, such as the learning process for complex problems with a large number of variables.

As an example of this we have the problem of classifying the binary function XOR. If we represent this function in space and carry out the projection of the points as shown in Fig. 4, we can verify that we achieve that these input data are linearly separable, and therefore with it an adequate classification of their patterns.

a) *Multilayer neural network function*: The computation performed in this type of neural network to extract the output  $y_i$  assuming a network with a single hidden layer would be as follows:

$$Y_i = g_1\left(\sum_{j=1}^L W_{ij} S_j\right) = g_1\left(\sum_{j=1}^L W_{ij} \left(g_2\left(\sum_{r=1}^N T_{jr} X_r\right)\right)\right) \quad (2)$$

Here we have that  $w_{ij}$  is the synaptic weight of the connection between the output unit  $i$  and the hidden processing unit  $j$ .  $L$  would be the number of processing units in the hidden layer;  $g_1$  would be the transfer function for the process units of the output layer, which can be the identity function, the hyperbolic tangent or a logistic function;  $t_{jr}$  is the synaptic weight connecting process unit  $j$  of the hidden layer with input  $r$ . Finally, we have the function  $g_2$  which is the transfer function of the processing units of the hidden layer,

which can also be of the type previously mentioned for the processing units of the output layer.

b) *Delta rule or backpropagation algorithm*: The aim of this algorithm is to achieve the smallest error made for each desired output, in this way we want the expected outputs to be as similar to the desired output. What it intends is the determination of the synaptic weights so that the total error committed is the minimum:

$$E = \frac{1}{2} \sum_{k=1}^p \sum_{i=1}^M (z_i(k) - y_i(k))^2 \quad (3)$$

The backpropagation algorithm uses the descending gradient method and that makes use of the gradient vector, being one of the most used for this type of algorithm.

3) *Model Support Vector Machine (SVM)*: These methods are properly related to classification and regression problems. Given a set of training examples (of samples) we can label the classes and train an SVM to build a model that predicts the class of a new sample. Intuitively, an SVM is a model that represents the sample points in space, separating the classes to 2 spaces as wide as possible by means of a separation hyperplane defined as the vector between the 2 points, of the 2 classes, closest to the which is called a support vector. When the new samples are put into correspondence with said model, depending on the spaces to which they belong, they can be classified into one or the other class [18].

$$F = \{\varphi(x) \parallel x \in X\}$$

$$x = \{x_1, x_2, \dots, x_n\} \rightarrow \varphi(x) = \{\varphi_1(x), \varphi_2(x), \dots, \varphi_1(x)\} \quad (4)$$

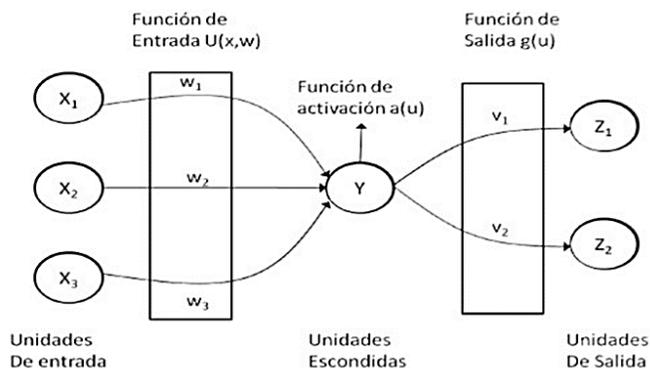


Fig. 3. Structural Model of a Neural Network, por Hernández et al., 2004 [8].

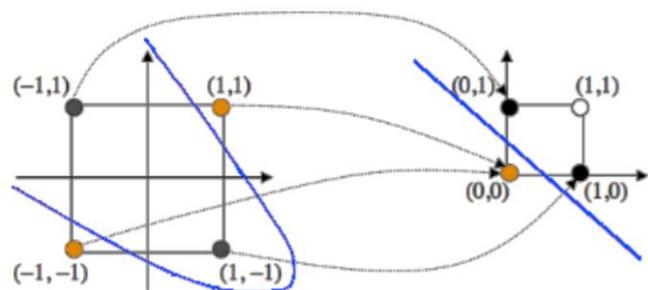


Fig. 4. Projecting the Input Patterns, por Hernández et al., 2004 [8].

Types of Kernel functions

a) *Polynomial-homogeneous*:  $K(x_i, x_j) = (x_i * x_j)^n$  function interpreted graphically as shown in Fig. 5.

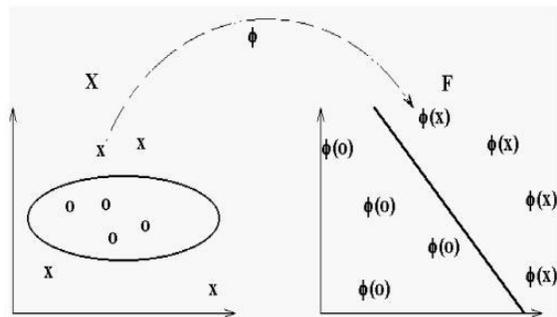


Fig. 5. Polynomial Function – Homogeneous, B. Kröse and P. van der Smagt., 1996 [1].

b) *Perceptron*:  $K(x_i, x_j) = ||x_i - x_j||$  function interpreted graphically as shown in Fig. 6.

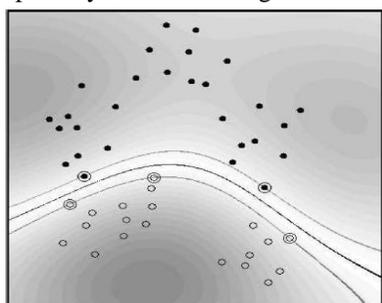


Fig. 6. Perceptron Function, B. Kröse and P. Van Der Smagt., 1996. [1].

c) *Gaussian radial basis function*: separated by a hyperplane in the transformed space as shown in Fig. 7.  $K = (x_i, x_j) = \exp(-(x_i - x_j)^2 / 2(\sigma)^2)$

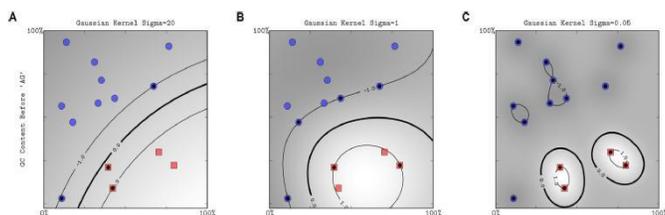


Fig. 7. Gaussian Radial basis Function, B. Kröse and P. Van Der Smagt., 1996. [1].

C. Evaluation Metrics

The technical evaluation measures that are generally used are based on a contingency Table II that describes the predicted hit and miss instances. This contingency table is called a confusion matrix that "contains information about current and predicted classifications, carried out by a classification system" [7]. The scheme of this for a case of binary classification is:

Based on this table, the following metrics of the following equations (5), (6), (7), (8) and (9) of a technical nature [9] are defined:

TABLE II. BINARY CASE CONFUSION TABLE SCHEMA

Categories		Current Class	
		0	1
Hypothetical Class	0	TN	FN
	1	FP	TP
Total Columns		N=FP+TN	P=TP+FN

Note: Impurity criteria functions for the Decision Tree search algorithm. by Ramirez et al., 2009 [8].

Precision

With the precision metric we can measure the quality of the machine learning model in classification tasks (5).

$$Precision = \frac{TP}{TP+FP} \tag{5}$$

Recall

The completeness metric will inform us about the amount that the machine learning model is able to identify.

$$Recall = \frac{TP}{P} \tag{6}$$

Accuracy

Accuracy measures the frequency with which the classifier makes a correct prediction. It is the relationship between the number of correct predictions and the total number of predictions (7). Its general formula is the following [9]:

$$Accuracy = \frac{TP+TN}{P+N} \tag{7}$$

f-measure

It is the measure of precision that a test has and is usually used in the testing phase of search algorithms and information retrieval and document classification (8) and (9) [9].

$$F - Measure = \frac{2}{\frac{1}{Recall} + \frac{1}{Precision}} \tag{8}$$

$$Lift = \frac{Precision}{\frac{P}{P+N}} \tag{9}$$

a) *Roc curves*: They are curves that show the ability of the classifier to position the true instances with respect to the false ones [9]. In a more accurate definition, it can be said that the ROC Curves are those that measure the ratio of the rate of true positives (correct predictions) versus the rate of false positives (wrong predictions). The positive being the one referring to the leakage class when it comes to a binary classification problem. These curves do not have an associated formula. However, they do have a metric, which is called "Area Under the curve" (AUC), which is defined as the area under the ROC Curve, in addition, it has the following statistical property: "The AUC of a classifier is equivalent to the probability that the classifier will position a positive random instance better than a negative random instance" [16, 17].

### III. RELATED JOBS

Customer churn is a critical problem and one of the most important concerns for large telcos, various approaches were applied to predict customer churn, using data mining and machine learning approaches. Most of the related work focused on applying just one data mining method to extract knowledge, and the others focused on comparing various strategies to predict attrition.

J. Wang and Gavril et al. [11, 19] presented an advanced data mining methodology to predict the loss of prepaid customers using a data set for the call details of 3,333 customers with 21 functions and a dependent loss parameter with two values: Yes / No. Some Features include information on the number of incoming and outgoing messages and voicemail for each customer. The author applied the "PCA" principal component analysis algorithm to reduce the dimensions of the data. Three machine learning algorithms were used: Neural Networks, Support Vector Machine, and Bayes Networks to predict the churn factor. The author used AUC to measure the performance of the algorithms. The AUC values were 99.10%, 99.55%, and 99.70% for Bayes Networks, Neural networks, and support vector machine, respectively. The data set used in this study is small and there were no missing values.

Huang et al. [20] studied the problem of customer loss on the big data platform. The researchers' goal was to show that big data greatly improves the rotation prediction process based on the volume, variety and speed of the data. Dealing with the data from the operational support department and the business support department of the largest telecommunications

company in China needed a big data platform to design the fractures. The Random Forest algorithm was used and evaluated using AUC.

Makhtar et al. [21] proposed a model for the prediction of abandonment using the approximate set theory in telecommunications. As mentioned in this article, the Rough Set classification algorithm outperformed other algorithms such as Linear Regression, Decision Tree, and Voted Perception Neural Network.

### IV. EXPERIMENTATION

Different prediction models were proposed for the data set, the most accurate was chosen using the precision evaluation metric generated by each model. The model for predicting the abandonment of telephone service customers is shown below in Fig. 8.

#### A. Modelo Decisión Tree

For the proposed model, the blocks for data reading flow, processing, partitioning for data input and testing and the evaluation stage are implemented, using the knime data mining software. Fig. 9 shows the nodes of the flow of the decision tree prediction model.

#### B. Artificial Neural Network Model – ANN

For the neural network prediction model, we proceed with data processing (normalization, training partition and data testing); Neural network data analytics nodes are used for processing; For the evaluation stage, the model evaluation score nodes are used, using the knime data mining software. Fig. 10 shows the nodes of the flow of the artificial neural network prediction model.

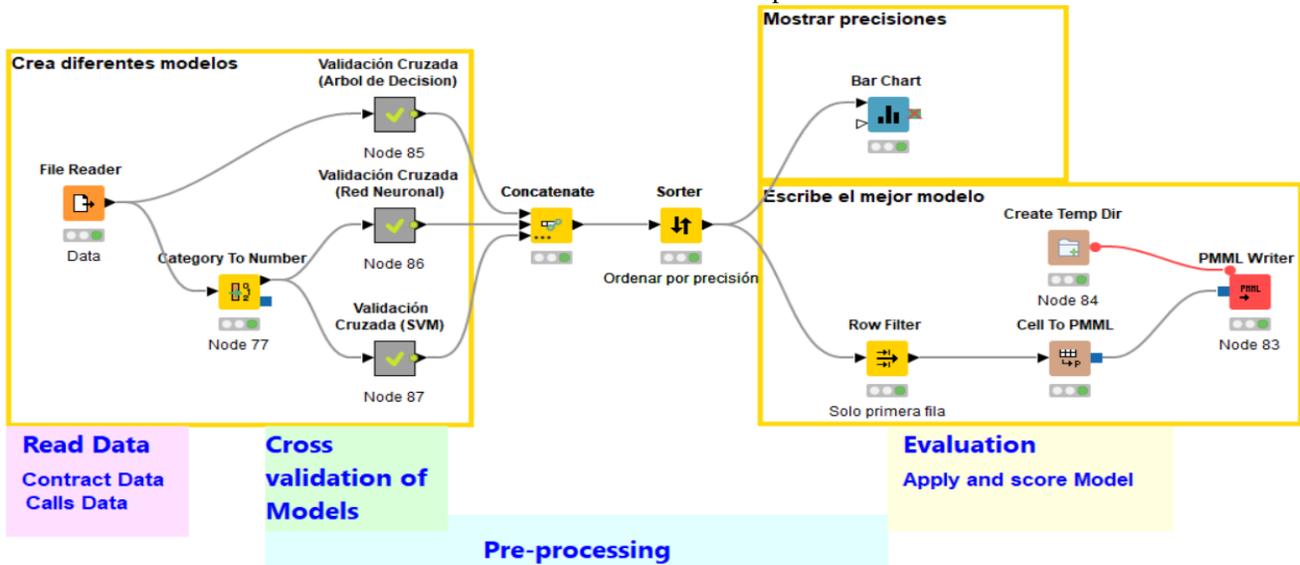


Fig. 8. General Churn Prediction Model with KNIME Software, (Note: Own elaboration)

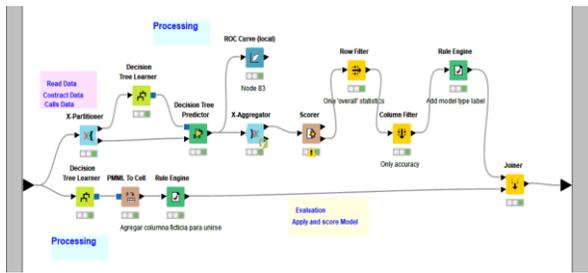


Fig. 9. Churn Prediction Model - Decision Tree with KNIME Software, (Note: Own Elaboration).

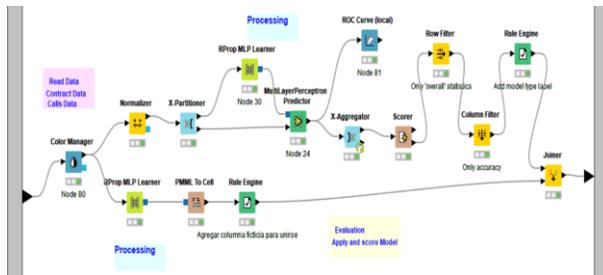


Fig. 10. Churn Prediction Model - ANN Artificial Neural Network with KNIME Software, (Note: Own Elaboration).

### C. Support Vector Machine Model (SVM)

For the support vector machine prediction model -SVM proposed in Fig. 11, the blocks for data reading flow, processing, partitioning for data input and testing and the evaluation stage are implemented, using the software of knime data mining.

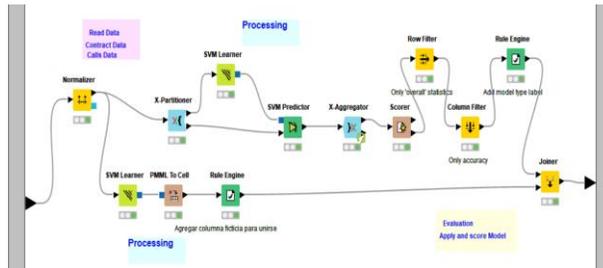


Fig. 11. Churn Prediction Model - SVM with KNIME Software, (Note: Own Elaboration).

### D. Data

For the predictive analysis model, a study test data set has been worked with, which has 3,333 customer data from a telephone service company. This database gathers a set of variables that offer information related to the company about the account, calls, plans, claims, etc. that has been used for the construction of predictive models.

The list and explanation of these attributes that are used in this study is shown in Table III.

This is a prediction problem. Starting with a small set of historical data, where we can see who has left and who has not in the past of service of the telephone company, we want to predict which customer will abandon (churn = 1) and which customer will not abandon (churn = 0).

attr 1, attr 2, ..., attr n => churn (0/1)

TABLE III. PREPROCESSED CHURN-RELATED VARIABLES

Attribute	Data type	Description
Account Length	Integer	Account length
VMail Message	Integer	Sending voice messages
Day Mins	Double	Minutes in the day
Eve Mins	Double	Minutes in the afternoon
Night Mins	Double	Minutes at night
Intl Mins	Double	International minutes
CustServ Calls	Integer	Consumer Service Calls
Churn	String	Churn-0 I don't give up Churn-1 Abandonment
Int'l Plan	Integer	International Plan
VMail Plan	Integer	Voice Message Plan
Day Calls	Integer	Calls per day
Day Charge	Double	Charge per day
Eve Calls	Integer	Afternoon calls
Eve Charge	Double	Charge for the call in the afternoon
Night Calls	Integer	Calls at night
Night Charge	Double	Call charge at night
Intl Calls	Integer	International Calls
Intl Charge	Double	International call charge
State	String	Status, Place
Area Code	Integer	Area Code
Phone	Integer	Phone No.

Note: Own elaboration

## V. TESTING

For the tests used of the dataset as real data, there are 3,333 customers affiliated with the telephone service, of which 2,850 customers did not abandon the telephone services (Churn = 0) and 483 customers that did abandon the telephone service (Churn = 1). For the verification and corroboration of these data, three machine learning prediction models were carried out, such as Decision Trees, Artificial Neural Networks-ANN and Support Vector Machine-SVM.

For the verification of the prediction models, the matrix of confusion, precision, accuracy and F-Value shown by the KNIME modeling software is analyzed and interpreted.

### A. Confusion Matrix of the Decision Tree Model

Table IV does not show the confusion matrix for the Decision Trees predictive model, which shows a success of 2706 clients who did not abandon the telephone service and in 98 they were wrong. And it hit 278 customers who left the service and 171 were wrong.

In Fig. 12 shows the graph of the ROC curve for the decision tree algorithm, it presents an AUC of 0.837, which validates the model as good, the level of certainty is 91.7% for churn = 0.

TABLE IV. CONFUSION MATRIX DECISION TREE

Real values	Prediction Values		
		Churn=0	Churn=1
	Churn=0	2706	98
Churn=1	171	278	

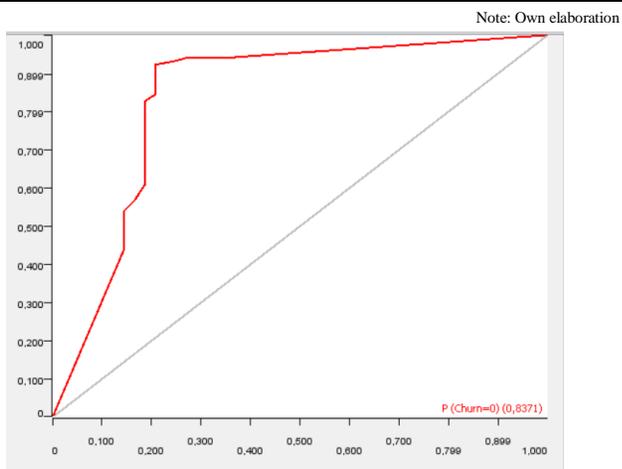


Fig. 12. ROC Curve Model Decision Tree P (Churn = 0), with KNIME Software (Note: Own Elaboration).

In Fig. 13 shows the graph of the ROC curve for the decision tree algorithm, it presents an AUC of 0.805, which validates the model as good, the level of certainty is 91.7% for churn = 1.

Table V shows the percentage of precision of the Decision Trees predictive model, it shows us the precision of certainty for each evaluation metric in churn = 0 and churn = 1, which are the percentages of certainty of the dataset; obtaining a general precision of 91.7% of certainty in the prediction model.

B. Confusion Matrix of the Artificial Neural Network-ANN Model

Table VI shows the confusion matrix for the predictive model of artificial Neural Networks, which shows a success of 2787 clients who did not abandon the telephone service and in 63 they were wrong. And 187 customers who left the service were right and 296 were wrong.

In Fig. 14 shows the graph of the ROC curve for the decision tree algorithm, it presents an AUC of 0.9242, which validates the model as good, the level of certainty is 89.1% for churn = 0.

In Fig. 15 shows the graph of the ROC curve for the decision trees algorithm, it presents an AUC of 0.9296, which validates the model as good, the level of certainty is 89.1% for churn = 1.

Table VII shows the percentage of precision of the predictive model of Artificial Neural Networks, it shows us the precision of certainty for each evaluation metric in churn = 0 and churn = 1, which are the certainty percentages of the dataset; obtaining a general precision of 89.1% of certainty in the prediction model.

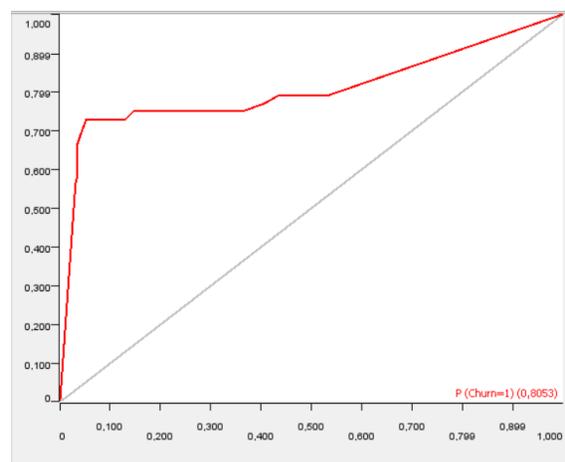


Fig. 13. ROC Curve Model Decision Tree P (churn = 1), with KNIME Software (Note: Own Elaboration).

TABLE V. DECISION TREE MODEL PRECISION MATRIX WITH KNIME

Evaluation metrics	ROW ID		Overall
	Churn=0	Churn=1	
Recall	0.965	0.619	---
Precision	0.941	0.739	---
Sensitivity	0.965	0.619	---
Specificity	0.619	0.965	---
F-measure	0.953	0.674	
Accuracy	---	---	0.917

Note: Own elaboration

TABLE VI. CONFUSION MATRIX ARTIFICIAL NEURAL NETWORK

Real values	Prediction Values		
		Churn=0	Churn=1
	Churn=0	2787	63
Churn=1	296	187	

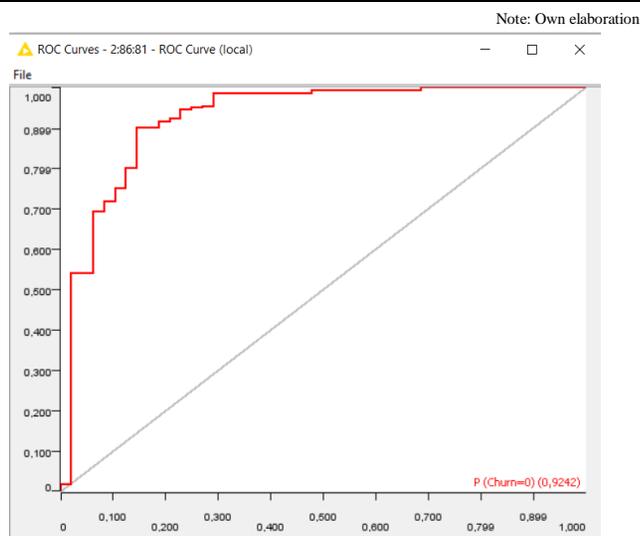


Fig. 14. ROC Curve Model Artificial Neural Network-ANN P (Churn = 0), with KNIME Software (Note: Own Elaboration).

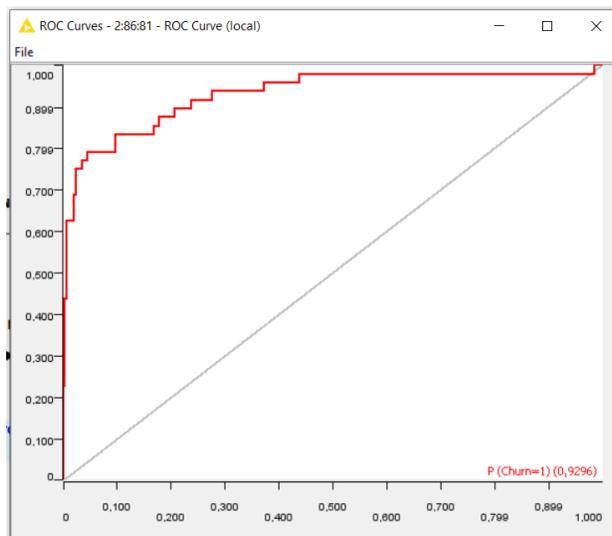


Fig. 15. ROC Curve Model Artificial Neural Network-ANN P (Churn = 1), with KNIME Software (Note: Own Elaboration).

TABLE VII. PRECISION MATRIX OF THE NEURONAL NETWORK MODEL WITH KNIME

Evaluation metrics	ROW ID		
	Churn=0	Churn=1	Overall
Recall	0.977	0.383	---
Precision	0.903	0.74	---
Sensitivity	0.977	0.383	---
Specificity	0.383	0.977	---
F-measure	0.939	0.505	
Accuracy	----	---	0.891

Note: Own elaboration

### C. Support Vector Machine Model-SVM Confusion Matrix

Table VIII shows the confusion matrix for the predictive model of Support Vector Machines-SVM, which does not present reliability in the prediction of the data since it predicted that 2850 did not leave the service and a null value of the customers who left the service.

Table IX shows the percentage of precision of the predictive model of the Support Vector Machine-SVM, which does not show reliable data to predict the certainty of abandonment or not of the clients in the telephone service.

TABLE VIII. CONFUSION MATRIX ARTIFICIAL NEURAL NETWORK

Real values	Prediction Values		
		Churn=0	Churn=1
	Churn=0	2850	0
Churn=1	483	0	

Note: Own elaboration

TABLE IX. SUPPORT VECTOR MACHINE MODEL PRECISION MATRIX-SVM WITH KNIME

Evaluation metrics	ROW ID		
	Churn=0	Churn=1	Overall
Recall	1	0	---
Precision	0.855	---	---
Sensitivity	1	0	---
Specificity	0	1	---
F-measure	0.922	---	---
Accuracy	----	---	0.855

Note: Own elaboration

## VI. RESULTS EVALUATION

In Fig. 16 and 17 the 3 predictive models were analyzed giving a precision of 91.7% for the Decision Trees model, 89.1% precision for the Neural Networks model and 85.5% for the Support Vector Machine model.

Row ID	Accuracy	Method	PMML
Overall_Row0	0.917	Decision Tree	<?xml version="1...<PMML version="4...<Header copy...<Applica...</Applic...</Header>
Overall_Row0...	0.891	Neural Netw...	<?xml version="1...<PMML version="4...<Header copy...<Applica...</Applic...</Header>
Overall_Row0...	0.855	SVM	<?xml version="1...<PMML version="4...<Header copy...<Applica...</Applic...</Header>

Fig. 16. Comparison of the Proposed Model, with KNIME Software (Note: Own Elaboration).

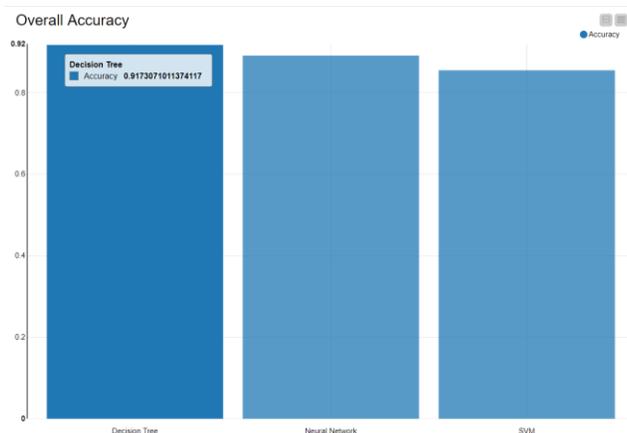


Fig. 17. Churn General Prediction Model, with KNIME Software (Note: Own Elaboration).

## VII. CONCLUSIONS

In this paper, he presents an experiment to compare three data mining prediction models, applied to a data set of abandonment or loss of service from a telephone company.

After evaluating these data mining models using KNIME software, such as Decision Tree, Artificial Neural Networks-ANN, Support Vector Machine-SVM, it was found that the precision for the Decision Tree model is 91.7% correct, the ANN model is 89.1% correct and the SVM model is 85.5% correct. Therefore, the decision tree model is the most accurate for this customer service leak prediction problem.

Specifically, it has been possible to successfully design a classification model based on a decision tree that allows classifying a subscriber as a customer in possible abandonment of telephony services.

For the validation of the models according to the ROC curve, the predictive models of decision trees and neural networks can be used since they result in a good acceptance test since the AUC (area under the curve) is 0.8 - 0.9 of acceptance.

## REFERENCES

- [1] B. Kröse and P. van der Smagt. An introduction to Neural Networks. None, 1996. 135 P.
- [2] B. Q. Huang, T. M. Kechadi, B. Buckley, G. Kiernan, E. Keogh, and T. Rashid. A new feature set with new window techniques for customer churn prediction in land-line telecommunications. *Expert Syst. Appl.*, 37: 3657-3665, May 2010.
- [3] CIMPOERU, C and ANDREESCU, A. Predicting Customers Churn in a Relational Database. *Informatica Economica* [Online] 2014, 18 (3), 5-16. [cit. February 12, 2016]. Available at: <https://search.proquest.com/openview/2b1c7bbe95f3543cd613111094959dce/1?Pqorigsite=gscholar&cbl=55108>.
- [4] Dickey. (2012). Introduction to Predictive Modeling with Examples. Obtained from SAS Global.
- [5] FAWCETT, T. An introduction to ROC Analysis. *Pattern Recognition* [Online]. 2006. 27 (8), 861-874. [cit. February 12, 2016]. DOI: <https://doi.org/10.1016/j.patrec.2005.10.010> Available at: <http://www.sciencedirect.com/science/article/pii/S016786550500303X>.
- [6] GIUDICI, P AND FIGNI, S. *Applied Data Mining for Business and Industry*. s.l. : Wiley, DOI: <https://doi.org/10.1002/9780470745830.index>, 2009.
- [7] G. Huerta. Balancing data for galaxy image classification. Technical report, Polytechnic University of Puebla, 2010.
- [8] HERNÁNDEZ O, J., RAMIREZ QUINTANA, MJ., FERRI RAMIREZ, C. *Introduction to Data Mining*. Madrid: Pearson Prentice Hall, 2004. Forum 2012: <http://support.sas.com/resources/papers/proceedings12/337-2012.pdf>.
- [9] J. Burez and D. Van den Poel. Handling class imbalance in customer churn prediction. *Expert Syst. Appl.*, 36: 46264636, April 2009.
- [10] J. Lu. Predicting customer churn in the telecommunications industry an application of survival analysis modeling using sas. Technical report, Sprint Communications Company, 2001.
- [11] J. Wang, editor. *Data mining: opportunities and challenges*. IGI Publishing, Hershey, PA, USA, 2003.
- [12] M. Richeldi and A. Perrucci. Analyzing churn of customers.
- [13] M. A. P. M. Lejeune. Measuring the impact of data mining on churn management. *Internet Research*, 11 (5): 375387, 2001.
- [14] N. K. Kasabov. *Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering*. MIT Press, Cambridge, MA, USA, 1st edition, 1996. 550 P.
- [15] S. Molina. Application of data mining techniques to predict customer churn in a telecommunications company. Master's thesis, School of Engineering of the Ponticia Universidad Católica de Chile, 2009. 114 P.
- [16] U. Fayyad, G. Piatetsky-shapiro, and P. Smyth. From data mining to knowledge discovery in databases. *AI Magazine*, 17: 3754, 1996.
- [17] Urias, H. Q., & Salvador, B. R. P. (2014). *Statistics for engineering and science*. Grupo Editorial Patria.
- [18] YU, Wei, et al. Application of support vector machine modeling for prediction of commiseases: the case of diabetes and pre-diabetes. *BMC medical informatics and decision making*, 2010, vol. 10, no 1, p. 16.
- [19] Brandusoiu I, Todorean G, Ha B. Métodos para la predicción del abandono en la industria de las telecomunicaciones móviles prepagas. En: Congreso internacional de comunicaciones. 2016. p. 97-100.
- [20] Huang F, Zhu M, Yuan K, Deng EO. Predicción de abandono de empresas de telecomunicaciones con big data. En: Conferencia internacional ACM SIGMOD sobre gestión de datos. 2015. p .607-18.
- [21] Makhtar M, Nafis S, Mohamed M, Awang M, Rahman M, Deris M. Churn modelo de clasificación para una empresa de telecomunicaciones local basado en la teoría de conjuntos aproximada. *J Fundam Appl Sci*. 2017; 9 (6): 854-68.

# Evaluating Software Quality Attributes using Analytic Hierarchy Process (AHP)

Botchway Ivy Belinda<sup>1</sup>, Akinwonmi Akintoba Emmanuel<sup>2</sup>, Nunoo Solomon<sup>3</sup>, Alese Boniface Kayode<sup>4</sup>

Department of Computer Science and Engineering, University of Mines and Technology, UMaT, Tarkwa, Ghana<sup>1</sup>

Department of Cybersecurity, Federal University of Technology, Akure, FUTA, Akure, Nigeria<sup>2,4</sup>

Department of Electrical and Electronic Engineering, University of Mines and Technology, UMaT, Tarkwa, Ghana<sup>3</sup>

**Abstract**—The use of quality software is of importance to stakeholders and its demand is on the increase. This work focuses on meeting software quality from the user and developer's perspective. After a review of some existing software-quality models, twenty-four software quality attributes addressed by ten models such as the McCall's, Boehm's, ISO/IEC, FURPS, Dromey's, Kitchenham's, Ghezzi's, Georgiadou's, Jamwal's and Glibb's models were identified. We further categorized the twenty-four attributes into a group of eleven (11) main attributes and another group of thirteen (13) sub-attributes. Thereafter, questionnaires were administered to twenty experts from fields including Cybersecurity, Programming, Software Development and Software Engineering. Analytic Hierarchy Process (AHP) was applied to perform a multi-criteria decision-making assessment on the responses from the questionnaires to select the suitable software quality attribute for the development of the proposed quality model to meet both users and developer's software quality requirements. The results obtained from the assessment showed Maintainability to be the most important quality attribute followed by Security, Testability, Reliability, Efficiency, Usability, Portability, Reusability, Functionality, Availability and finally, Cost.

**Keywords**—Analytic Hierarchy Process (AHP); software quality; quality attribute; quality model; sub-attributes

## I. INTRODUCTION

Software quality is a paramount issue to all software stakeholders in a given establishment and its demand is increasing rapidly due to customer demand [1]. In the last few decades, the importance of the use of quality software has increased exponentially [2]. Software users see software as a tool to enable them to carry out their daily activities with ease, and hence, use it to perform sensitive tasks [3]. The use of less quality software can, directly and indirectly, endanger one's life [30] as well as causing huge loss to software users. As a result, many software quality models have been proposed to evaluate software quality, yet, none of these models has been widely accepted as the benchmark for assessing software quality. This is because these models do not address all the important software quality attributes that are of keen interest to stakeholders and are tailored towards meeting specific project's requirements. To address stakeholder requirements, custom software quality models have been proposed [4]. These custom made quality models offer different benefits to the software industry and research community and hence do not cover a wide scope of quality attributes.

This research presents an evaluation of software quality attributes using the Analytic Hierarchy Process (AHP). It was conducted based on a questionnaire given to stakeholders to assess the quality attributes they expect a software quality model to have. As a result, an evaluation of these quality attributes was made and represented with a graph to pictorially highlight the percentage of weight each quality attribute ranked. Ranking the software quality attributes will assist developers greatly in selecting the best quality attribute for evaluating developed software. Previous works have failed to rank quality attributes and have led to the proposal of numerous custom software quality models.

The rest of the paper is organized as follows: Section II discusses related work done on AHP, software quality models and quality attributes. Section III discusses software quality, quality models and attributes. The methodology used to select the software quality attributes is illustrated in Section IV. Section V presents the conclusion and discusses future works.

## II. RELATED WORKS

Software quality models have been reviewed by numerous researchers in addressing software quality problems. The authors in [14] evaluated the quality of software in Enterprise Resource Planning (ERP) systems using the ISO 9126 model. They offered a comparison between existing quality models and identified the quality characteristics of ERP systems but they did not rank the main quality characteristics of the model.

In [15], research was conducted on an analytical and comparative study of software usability quality factors. They analysed ten famous quality models for developing a usability model that satisfies the demand of current business software and proposed an integrated improved usability model for assuring software quality. The new usability evaluation model was proposed from ten models of McCall, Boehm, Shackel, FURPS, Nielson, SUMI, ISO 9242-11, ISO 9126, and QUIM model.

A research was conducted by [16] on an approach for enhancing software quality based on ISO 9126 quality model. They were able to propose a new quality model for integrating some quality attributes in software development.

The authors in [13] also worked on the quality assessment of Commercial-Off-The-Shelf products by adopting the ISO 9126 quality model.

Another study was conducted by [3] on software quality attributes to enhance software quality assurance. The authors did this research because, in recent times, industries are giving more attention to software quality improvement. Therefore, they focused on meeting customer perspectives of software quality to propose a new model. The limitation of the research is that it did not address availability, testability and reusability problems.

Authors in [25] worked on extending Dromey's quality model to specify the security quality requirements in a software product. They conducted the research based on the increase in cybercrimes. The model was able to enhance the security requirement of software and trained people on how to develop secure software.

A study by researchers in [26] adapted the ISO/IEC 9126 quality model to evaluate Enterprise Resource Planning (ERP) systems. The model was proposed as a result of the urge in the increasing usage of ERP systems by organisations to get faster data transactions. The researchers proposed the model to have six (6) main software quality attributes including functionality, maintainability, reliability, efficiency, usability and portability. The limitation was that the model did not address some of the most important software quality attributes such as availability, testability and flexibility. It also did not rank the quality attributes.

In [27], the authors presented a software quality model for academic information systems. Their objective was to guide academic institutions that are in the process of building their E-learning systems to evaluate and choose the appropriate software attributes that are essential to the success of the entire system. The researchers identified the key attributes for Information System's Software Quality (ISSQ) from the users' perspective to measure the quality of the E-learning system. The proposed model consisted of six (6) standard attributes with their sub-attributes. This was achieved based on the ISO/IEC 9126 model. The limitation was that the proposed model failed to evaluate the importance of quality attributes.

These researchers have shown how the use of software quality models is gaining much importance in the development of software. Nevertheless, they have not ranked the quality attributes and hence, it is difficult to know the weight of each attribute to ease decision making. This research work employs the use of the Analytic Hierarchy Process, a multi-criteria decision-making tool to evaluate software quality attributes and rank them.

Analytic Hierarchy Process (AHP) has been applied by several researchers to enhance group decisions. The researchers in [17] applied this technique to evaluate and select Commercial-off-the-shelf (COTS) components. They found AHP to be useful in making trade-offs between tangible and intangible factors in calculating the weight of COTS components. Applying these weights as coefficients of an objective function in the proposed model helped to determine the best component under constraints such as budgetary constraint, compatibility among components and system reliability. Their findings have validated AHP to be an effective and flexible tool.

AHP was applied by [4] to produce an integrated framework that applies statistical analysis to generate software quality models tailored to stakeholder specifications. They found AHP to be quite accessible and conducive for decision-making that requires the reduction of decisions complexity in pair-wise matrices.

AHP was also applied by [18] in evaluating the reliability of object-oriented software systems. They took the ISO/IEC 9126 model as the base model for the evaluation. Their results showed AHP to be useful for making decisions for the hierarchical structure of the model.

Authors in [28] applied the Analytic Hierarchy Process to develop an algorithm for evaluating software functionality. The research was due to the increase in the number of sub-attributes of software functionality quality attribute. They wanted to know the most important sub-attribute that has a great impact on software products. The AHP technique was seen to be a useful tool for the decision-making process.

In [29], the AHP technique was used to perform a risk assessment of software quality. The authors were able to construct an index system of software quality risk assessment by calculating the weight and order of risk factors. With the use of AHP, they were able to categorise risk factors into demand risk, technology risk, process risk and management risk.

The authors in [19] applied AHP to analyse software reliability. They reported that although software reliability is an important quality attribute, different stakeholders have a variety of views in that regard. Hence, they applied AHP which is designed to manage human assessment subjectively.

The Analytic Hierarchy Process has been seen to effectively aid researchers in solving complex decision-making problems in various fields but its rate of application in the software quality assurance industry is minimal. Most software quality attributes used for software quality assurance have not been ranked, hence, it is difficult to note the important attributes to use to evaluate software projects. In this research, AHP is used to rank quality attributes by using the value of their criteria weights. The higher the criteria weight, the higher its importance in evaluating software quality.

### III. SOFTWARE QUALITY

Software quality is a benchmark for measuring software requirements and the prerequisite to meet the user's specifications. Software quality involves user requirements, system design, documentation, and all the requirements needed for the development of professionally acceptable software [5]. It strictly follows the software development life cycle and evaluates and improves software performance [5]. Software quality can be enforced using software quality models.

#### A. Software Quality Models

Different software quality models have been proposed by researchers such as McCall [6], Boehm [7], Jamwal [8], Grady [9], Dromey [10] and ISO/IEC [11] among others as shown in Table I. These quality models contain quality attributes that may be used to ascertain the quality of a software product by determining how the software executes its code or how the software architecture is structured and organized with the

system’s requirements [12]. All the quality models have software quality attributes and sub-attributes used for the measurement of software quality [13]. Quality attributes and sub-attributes are used to characterize products and can be

measured. They usually end with the word “lity”. According to the ISO 9126 standard, a software quality model is expected to have the following attributes: Functionality, Reliability, Usability, Efficiency, Maintainability and Portability.

TABLE I. SOFTWARE QUALITY MODELS AND THEIR SUB-ATTRIBUTES

Quality Models	McCall	Boehm	FURPS	Dromey	ISO-9126	Glibb	Kitchenham and Pickard	Ghezzi et al.	Georgiadou	Jamwal and Jamwal	Proposed Quality Model
Maintainability	/	/		/	/		/	/	/		/
Flexibility	/	/						/			
Testability	/	/									/
Correctness	/									/	
Reliability	/	/	/	/	/		/	/	/	/	/
Efficiency	/	/		/				/	/		/
Usability	/	/	/	/	/	/	/	/	/	/	/
Portability	/	/		/	/			/	/	/	/
Reusability	/			/				/			/
Interoperability	/										
Understandability		/									
Functionality			/	/	/				/		/
Performance			/							/	
Supportability			/								
Availability						/					/
Adaptability						/					
Accuracy								/			
Robustness									/	/	
Extensibility			/								
Security									/		/
Cost										/	/
Integrity	/										
Confidentiality											
Non-Repudiation											

**B. Software Quality Attributes**

Software quality attributes are used to measure customer fulfilment of a product for other similar products. They are also used by software developers to develop quality software. These attributes include correctness, reliability, portability, efficiency, maintainability, supportability, functionality, usability, availability, among others. The software development life cycle ensures that implementing quality attributes in software development may result in the production of a well-engineered software product and is to be enforced throughout the development, implementation, and deployment phases of the software [5].

**C. Software Quality Attributes Descriptions**

This section itemizes and describes some software quality attributes.

- **Correctness:** Correctness refers to the capability of software to meet its required results.
- **Usability:** Usability is the ease of use and learnability of software by customers.
- **Efficiency:** Efficiency is the ability of software to perform well, given that tasks are completed faster while using fewer resources and saving computer power with great performance.
- **Reliability:** Reliability refers to the probability of software operating in a given environment within a specified period to perform well without encountering a breakdown.
- **Accuracy:** Accuracy refers to the degree to which a software product provides the right results during usage without encountering an error.

- **Robustness:** Robustness refers to the ability of a software product to cope with any form of error it may encounter during operation.
- **Functionality:** Functionality is the ability of software to perform the tasks for which it was intended.
- **Performance:** Performance refers to the total effectiveness of a software product.
- **Availability:** Availability refers to the degree to which a software product is operational and easily accessible when needed for usage.
- **Maintainability:** The ease with which software can be modified to correct faults or improve performance.
- **Flexibility:** Flexibility is the ability of software to adapt to possible future changes in its requirements.
- **Portability:** The measure of the ease of transferring software from one computing environment to the other.
- **Reusability:** Reusability is the use of existing tested and validated loosely coupled components in the development of software applications.
- **Testability:** Testability is the ease with which the correctness of software can be verified.
- **Understandability:** The capability of a software product to enable the user to understand whether it is suitable and its usability for specific tasks and conditions for use.
- **Interoperability:** Interoperability is the ease with which software is used with other software applications.

#### IV. ANALYTIC HIERARCHY PROCESS (AHP)

AHP is a method of multi-criteria evaluation that organizes and simplifies the decision-making process. It was originally developed by Thomas L. Saaty [20] to provide measures of judgement consistency; to derive priorities among criteria and alternatives, and to simplify the rating of preferences among decision criteria using pair-wise comparisons [21]. The AHP decision-making tool is robust and flexible in dealing with complex decision problems. It uses a multi-level hierarchical structure of objective or goal, criteria or attributes, and alternatives.

AHP is based on mathematics and psychology [22]. It helps decision-makers to find a decision that best suits their goal and their understanding of a given problem. It is a method to derive ratio scales from paired comparisons [23] and is based on a certain scale that changes subjective judgements into objective judgement and solves qualitative problems with quantitative analysis. It is simple and hence has seen its application in many fields.

##### A. Assessment of Quality Attributes

The research uses an Analytical Hierarchy Process (AHP) to perform a multi-criteria decision-making assessment to select a suitable software quality attribute for the development of the quality model. The selection will be made from eleven attributes (Maintainability M(s), Testability T(s), Reliability

R(s), Efficiency E(s), Usability U(s), Portability P(s), Reusability Re(s), Cost Co(s), Functionality Fn(s), Security S(s) and Availability A(s)) and three alternatives (“Mostly addressed”, “Doubles up as a Sub-attribute”, “Has Sub-attributes”). This information will be used to develop a hierarchical structure with the goal at the top level, the attributes at the second level, and the alternatives at the third level as shown in Fig. 1.

The hierarchical structure obtained was synthesized to determine the relative importance of each attribute to the goal. This is done using a pair-wise comparison matrix with the help of a scale of relative importance as shown in Table II.

The quality attributes used for the judgement matrix are shown in Table III. It consists of eleven (11) main attributes and thirteen (13) sub-attributes. The AHP technique was only applied to the eleven (11) main attributes.

##### B. Selection of Appropriate Software Quality Attributes using the Analytic Hierarchy Process (AHP)

The judgement matrix was determined by twenty (20) experts’ decisions, based on related research. The implementation was done using MATLAB/Simulink Software R2020b. The software allows for easy calculation and analysis for the decision-making process. It also helps in constructing the model and drawing analysis.

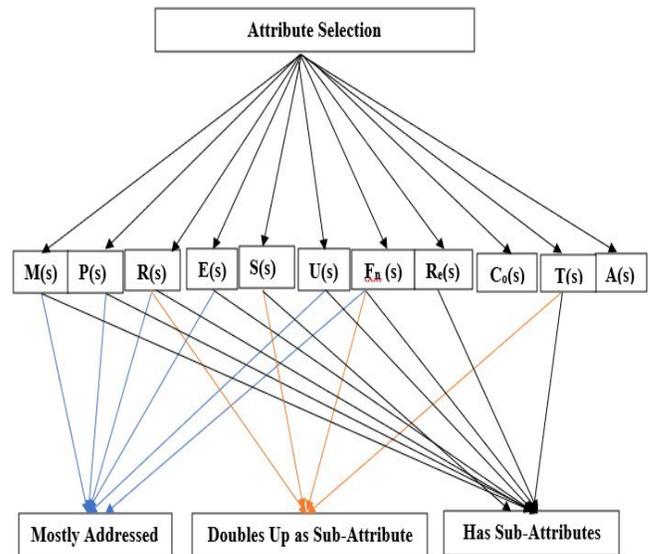


Fig. 1. Hierarchical Structure of Software Quality Attributes.

TABLE II. THE SCALE OF COMPARISON [24]

Scale of Importance	Degree of Preference
1	Equal Importance
3	Moderate Importance
5	Strong Importance
7	Very Strong Importance
9	Extreme Importance
2,4,6,8	Intermediate Values
1/3, 1/5, 1/7, 1/9	Values for Inverse Comparison

TABLE III. QUALITY ATTRIBUTES AND THEIR SUB-ATTRIBUTES

Attribute	Sub-attribute
Maintainability M(s)	Flexibility
	Extensibility
	Supportability
Usability U(s)	Understandability
Reliability R(s)	Robustness
	Accuracy
Testability T(s)	
Functionality F <sub>n</sub> (s)	Correctness
	Interoperability
Availability A(s)	
Reusability R <sub>c</sub> (s)	
Cost C <sub>o</sub> (s)	
Efficiency E(s)	Performance
Portability P(s)	Adaptability
Security S(s)	Integrity
	Confidentiality
	Non-Repudiation

C. Quality Attribute Selection Judgement Matrices

A geometric mean of the scores from the questionnaire was found and represented in Table IV for effective criteria and pair-wise comparison.

Table V shows the normalised pair-wise comparison matrix while Table VI shows the consistency matrix.

Twenty experts were given questionnaires to fill for the multi-criteria decision process. The geometric mean of these questionnaires was found by multiplying the values for each of the attributes in Table IV and setting it to the 1/nth power. The sum of each attribute was finally calculated. The geometric mean of the scores was found by

$$\left(\prod_{i=1}^n x_i\right)^{\frac{1}{n}} = \sqrt[n]{x_1 x_2 \dots x_n} \tag{1}$$

Where n is the number of terms that are being multiplied.

The normalised pair-wise comparison matrix was found in Table V by diving each of the values for the attributes in Table IV by the sum. To calculate the criteria weight, an average of the rows is found.

It is seen from Table V that the criteria weight of Maintainability is 17.37%, Testability is 13.02%, Usability is 7.22%, Functionality is 6.22%, Cost is 4.73%, Portability is 7.13%, Availability is 5.99%, Reusability is 6.86%, Security is 13.61%, Reliability is 10.35% and Efficiency is 7.49%. Maintainability is seen to have the highest weight while Cost is seen to have the lowest weight.

To check for the cost of the expert’s evaluation, the consistency of the pair-wise comparison matrix is calculated. This is done by multiplying the criteria weight by the pair-wise comparison matrix which is not normalised in Table IV as shown in Table VI. The weighted sum of the new matrix is found and then divided by the criteria weight. The overall sum is found for the calculation of  $\lambda_{max}$  and Consistency Ratio (CR). The value of the consistency ratio must be less than 0.1 to make the judgement matrix acceptable.

$$\lambda_{max} = \frac{134.04}{11} = 12.186 \tag{2}$$

$$CI = \frac{\lambda_{max} - n}{n - 1} = \frac{12.186 - 11}{10} = 0.119 \tag{3}$$

$$CR = \frac{CI}{RI} = \frac{0.119}{1.51} = 0.079 \tag{4}$$

The selection judgement matrix shows consistency since the value of the Consistency Ratio (CR) is 0.079 which is less than 0.1.

TABLE IV. GEOMETRIC MEAN OF THE FILLED QUESTIONNAIRE

Attributes	M(s)	T(s)	R(s)	P(s)	A(s)	E(s)	Fn(s)	Re(s)	S(s)	U(s)	Co(s)
<b>M(s)</b>	1.00	2.05	2.44	2.98	2.95	2.75	2.95	2.18	1.55	1.59	2.80
<b>T(s)</b>	0.49	1.00	2.04	2.30	2.99	2.02	2.85	1.90	1.20	1.31	2.10
<b>R(s)</b>	0.41	0.49	1.00	1.00	1.95	1.72	2.69	1.50	1.28	2.10	2.59
<b>P(s)</b>	0.34	0.43	1.00	1.00	1.20	0.75	0.98	1.29	1.05	1.03	1.68
<b>A(s)</b>	0.34	0.33	0.51	0.51	1.00	1.02	1.01	0.67	0.20	2.54	1.54
<b>E(s)</b>	0.36	0.50	0.58	1.33	0.98	1.00	1.02	1.59	0.28	2.85	1.50
<b>Fn(s)</b>	0.34	0.35	0.37	1.02	0.99	0.98	1.00	2.65	0.32	0.55	1.85
<b>Re(s)</b>	0.46	0.53	0.67	0.78	1.49	0.63	3.57	1.00	0.23	0.60	1.55
<b>S(s)</b>	0.65	0.83	0.78	0.95	5.00	3.57	3.13	4.35	1.00	0.87	1.90
<b>U(s)</b>	0.63	0.76	0.48	0.97	0.39	0.35	1.82	1.67	1.15	1.00	1.00
<b>Co(s)</b>	0.36	0.48	0.39	0.60	0.65	0.67	0.54	0.65	0.53	1.00	1.00
<b>SUM</b>	<b>5.36</b>	<b>7.75</b>	<b>10.26</b>	<b>13.44</b>	<b>19.60</b>	<b>15.46</b>	<b>21.56</b>	<b>19.44</b>	<b>8.79</b>	<b>15.44</b>	<b>19.51</b>

TABLE V. NORMALISED PAIR-WISE COMPARISON MATRIX

Attributes	Criteria Weight	Criteria Weight (%)
M(s)	0.1737	17.37
T(s)	0.1302	13.02
R(s)	0.1035	10.35
P(s)	0.0713	7.13
A(s)	0.0599	5.99
E(s)	0.0749	7.49
Fn(s)	0.0622	6.22
Re(s)	0.0686	6.86
S(s)	0.1361	13.61
U(s)	0.0722	7.22
Co(s)	0.0473	4.73

TABLE VI. CONSISTENCY OF PAIR-WISE COMPARISON MATRIX

Attributes	Criteria Weight (CW)	Weighted Sum Value (WSV)	WSV/CW
M(s)	0.1737	2.079816	11.973
T(s)	0.1302	1.585515	12.178
R(s)	0.1035	1.27414	12.308
P(s)	0.0713	0.864021	12.116
A(s)	0.0599	0.720668	12.029
E(s)	0.0749	0.903899	12.057
Fn(s)	0.0622	0.763373	12.274
Re(s)	0.0686	0.847724	12.359
S(s)	0.1361	1.718038	12.623
U(s)	0.0722	0.880394	12.196
Co(s)	0.0473	0.564336	11.929
<b>SUM</b>			<b>134.04</b>
$\lambda_{\max} = 12.186$ CR = 0.079			

It can be seen from Table V that Maintainability M(s) has the highest weight which is 17.37% while Cost Co(s) has the lowest weight of 4.73%. Fig. 2 shows a graphical representation of the weights of the software quality attributes.

D. Alternative Selection Judgement Matrices

The alternatives which are “Mostly addressed”, “Doubles up as Sub-attributes”, and “Has Sub-attributes” were also analysed for Maintainability M(s) as shown in Table VII.

Table VII shows that Maintainability has a higher weight of 74% for being mostly addressed and a lower weight of 11% for doubling up as a sub-attribute.

The alternatives were also analysed for Testability T(s) as shown in Table VIII.

Table VIII shows that Testability has a higher weight of 67% for being mostly addressed and a lower weight of 10% for doubling up as a sub-attribute.

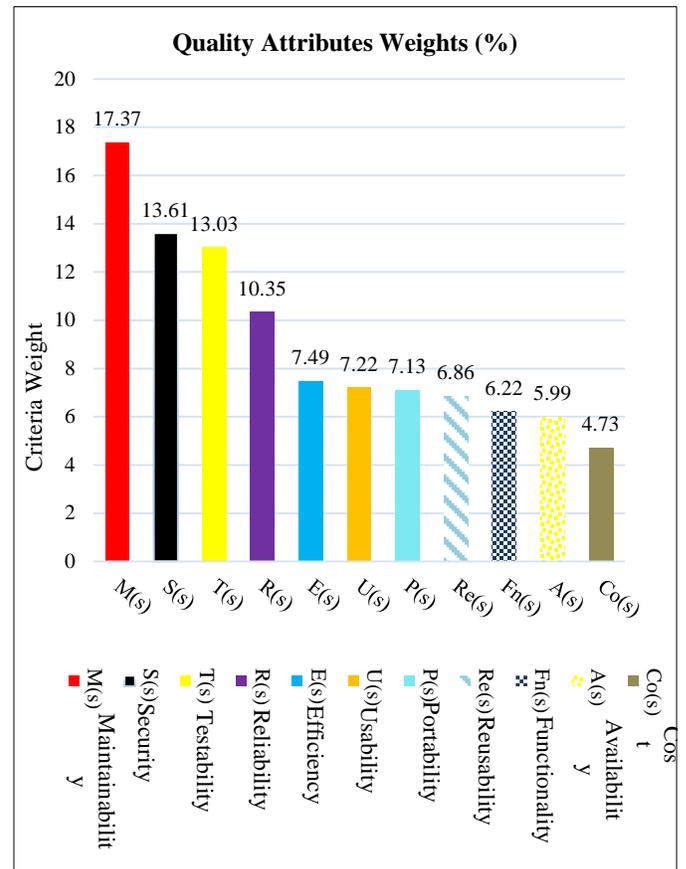


Fig. 2. Weights of the Software Quality Attributes.

TABLE VII. THE WEIGHT OF ALTERNATIVES FOR M(S)

M(s)	Has Sub-Attributes	Doubles Up as Sub-attribute	Mostly Addressed	Criteria Weight
Has Sub-Attributes	1.00	1.00	1/4	0.15
Doubles Up as Sub-attribute	1.00	1.00	1/9	0.11
Mostly Addressed	4.00	9.00	1.00	0.74
$\lambda_{\max} = 3.0749$			CR = 0.0646	

TABLE VIII. THE WEIGHT OF ALTERNATIVES FOR T(S)

T(s)	Has Sub-Attributes	Doubles Up as Sub-attribute	Mostly Addressed	Criteria Weight
Has Sub-Attributes	1.00	3.00	1/4	0.23
Doubles Up as Sub-attribute	1/3	1.00	1/5	0.10
Mostly Addressed	4.00	5.00	1.00	0.67
$\lambda_{\max} = 3.0869$			CR = 0.07496	

The alternatives were also analysed for Reliability R(s) as shown in Table IX.

Table IX shows that Reliability has a higher weight of 78% for being mostly addressed and a lower weight of 8% for doubling up as a sub-attribute.

The alternatives were also analysed for Efficiency E(s) as shown in Table X.

Table X shows that Efficiency has a higher weight of 62% for being mostly addressed and a lower weight of 10% for doubling up as a sub-attribute.

The alternatives were also analysed for Usability U(s) as shown in Table XI.

Table XI shows that Usability weights 80% for being mostly addressed and a weight of 8% for doubling up as a sub-attribute.

TABLE IX. THE WEIGHT OF ALTERNATIVES FOR R(S)

R(s)	Mostly Addressed	Has Sub-Attributes	Doubles Up as Sub-attribute	Criteria Weight
Mostly Addressed	1.00	7.00	8.00	0.78
Has Sub-Attributes	1/7	1.00	2.00	0.14
Doubles Up as Sub-attribute	1/8	1/2	1.00	0.08
$\lambda_{\max} = 3.035$		CR = 0.0304		

TABLE X. THE WEIGHT OF ALTERNATIVES FOR E(S)

E(s)	Has Sub-Attributes	Doubles Up as Sub-attribute	Mostly Addressed	Criteria Weight
Has Sub-Attributes	1.00	4.00	1/3	0.28
Doubles Up as Sub-attribute	1/4	1.00	1/5	0.10
Mostly Addressed	3.00	5.00	1.00	0.62
$\lambda_{\max} = 3.0867$		CR = 0.0747		

TABLE XI. THE WEIGHT OF ALTERNATIVES FOR U(S)

U(s)	Mostly Addressed	Has Sub-Attributes	Doubles Up as Sub-attribute	Criteria Weight
Mostly Addressed	1.00	9.00	8.00	0.80
Has Sub-Attributes	1/9	1.00	2.00	0.12
Doubles Up as Sub-attribute	1/8	1/2	1.00	0.08
$\lambda_{\max} = 3.075$		CR = 0.0649		

The alternatives were also analysed for Portability P(s) as shown in Table XII.

Table XII shows that Portability weighs 56% for being mostly addressed and a weight of 9% for doubling up as a sub-attribute.

The alternatives were also analysed for Reusability Re(s) as shown in Table XIII.

Table XIII shows that Reusability has a weight of 41% for having sub-attributes and a weight of 26% for doubling up as a sub-attribute.

The alternatives were also analysed for Functionality Fn(s) as shown in Table XIV.

Table XIV shows that Functionality's weightiness for being mostly addressed is 57% and 10% for doubling up as a sub-attribute.

TABLE XII. THE WEIGHT OF ALTERNATIVES FOR P(S)

P(s)	Has Sub-Attributes	Doubles Up as Sub-attribute	Mostly Addressed	Criteria Weight
Has Sub-Attributes	1.00	5.00	1/2	0.35
Doubles Up as Sub-attribute	1/5	1.00	1/5	0.09
Mostly Addressed	2.00	5.00	1.00	0.56
$\lambda_{\max} = 3.054$		CR = 0.0465		

TABLE XIII. THE WEIGHT OF ALTERNATIVES FOR Re (S)

Re(s)	Mostly Addressed	Doubles Up as Sub-attribute	Has Sub-Attributes	Criteria Weight
Mostly Addressed	1.00	1.00	1.00	0.33
Doubles Up as Sub-attribute	1.00	1.00	1/2	0.26
Has Sub-Attributes	1.00	2.00	1.00	0.41
$\lambda_{\max} = 3.054$		CR = 0.0463		

TABLE XIV. THE WEIGHT OF ALTERNATIVES FOR Fn (S)

Fn(s)	Has Sub-Attributes	Doubles Up as Sub-attribute	Mostly Addressed	Criteria Weight
Has Sub-Attributes	1.00	4.00	1/2	0.33
Doubles Up as Sub-attribute	1/4	1.00	1/5	0.10
Mostly Addressed	2.00	5.00	1.00	0.57
$\lambda_{\max} = 3.0247$		CR = 0.0213		

The alternatives were also analysed for Availability A(s) as shown in Table XV.

Table XV shows that Availability has a weight of 60% for doubling up as a sub-attribute and a lower weight of 17% for being most addressed.

The alternatives were also analysed for Cost Co(s) as shown in Table XVI.

Table XVI shows that Cost has a weight of 77% for doubling up as a sub-attribute and a weight of 11% for having sub-attributes.

The alternatives were also analysed for Security S(s) as shown in Table XVII.

Table XVII shows that Security has a weight of 56% for doubling up as a sub-attribute and a weight of 9% for having sub-attributes.

The overall weights for the software quality attribute selection are summarised in Table XVIII.

TABLE XV. THE WEIGHT OF ALTERNATIVES FOR A(S)

A(s)	Mostly Addressed	Has Sub-Attributes	Doubles Up as Sub-attribute	Criteria Weight
Mostly Addressed	1.00	1.00	1/5	0.17
Has Sub-Attributes	1.00	1.00	1/2	0.23
Doubles Up as Sub-attribute	5.00	2.00	1.00	0.60
$\lambda_{max} = 3.0951$		CR = 0.08196		

TABLE XVI. THE WEIGHT OF ALTERNATIVES FOR C<sub>o</sub> (S)

Co(s)	Has Sub-Attributes	Mostly Addressed	Doubles Up as Sub-attribute	Criteria Weight
Has Sub-Attributes	1.00	1.00	1/9	0.11
Mostly Addressed	1.00	1.00	1/5	0.13
Doubles Up as Sub-attribute	9.00	5.00	1.00	0.77
$\lambda_{max} = 3.0389$		CR = 0.0336		

TABLE XVII. THE WEIGHT OF ALTERNATIVES FOR S(S)

S(s)	Mostly Addressed	Has Sub-Attributes	Doubles Up as Sub-attribute	Criteria Weight
Mostly Addressed	1.00	2.00	1/2	0.35
Has Sub-Attributes	1/2	1.00	1/9	0.09
Doubles Up as Sub-attribute	2.00	9.00	1.00	0.56
$\lambda_{max} = 3.0745$		CR = 0.0642		

TABLE XVIII. THE WEIGHTS FOR SOFTWARE QUALITY ATTRIBUTE SELECTION

Element	Weight
<b>Alternatives</b>	
Mostly Addressed	0.520
Doubles up as Sub- attributes	0.221
Has Sub-attributes	0.259
<b>Criteria or Attributes</b>	
Maintainability	0.1737
Testability	0.1302
Reliability	0.1035
Efficiency	0.749
Usability	0.722
Portability	0.713
Reusability	0.686
Security	0.1361
Functionality	0.622
Availability	0.599
Cost	0.473
<b>Combined Consistency: 0.057</b>	

The results in Table XVIII show that “Mostly Addressed” is the highest-ranking software quality alternative with 52% and “Has Sub- attribute” is the lowest ranking alternative with 22%. The result also shows Maintainability as the highest-ranking software quality attribute with 17%. Table XVIII also shows that the overall analysis is consistent since the value of CR is 0.057 which is less than 0.1.

## V. RESULTS AND DISCUSSIONS

The software quality attributes have been evaluated and according to Table IV, Maintainability is seen to weigh 17.37%, Testability has a percentage of 13.02%, Reliability has a percentage of 10.35, Efficiency has a percentage of 7.49, Usability has a percentage of 7.22, Portability has a percentage of 7.13, Reusability has a percentage of 6.86, Functionality has a percentage of 6.22, Security weighs 13.61, Availability has a percentage of 5.99 and Cost has a percentage of 4.73. This was pictorially represented in Fig. 2.

Tables VII, VIII, ..., XVII has shown that Maintainability has a higher weight of 74% for being mostly addressed and a lower weight of 11% for doubling up as a sub-attribute. Testability weight of 67% for being mostly addressed and a weight of 10% for doubling up as a sub-attribute. Reliability has 78% for being mostly addressed and a weight of 8% for doubling up as a sub-attribute. Reliability is seen to also have 78% for being mostly addressed and a weighs 8% for doubling up as a sub-attribute. 62% was the weight of Efficiency for being mostly addressed and 10% for doubling up as a sub-attribute. Usability’s weightiness for being mostly addressed is 80% and 8% for doubling up as a sub-attribute. Portability also has a weight of 56% for being mostly addressed and a weight of 9% for doubling up as a sub-attribute. 41% was the weight of Reusability for having sub-attributes and 26% for doubling up as a sub-attribute. Functionality also has a weight of 57%

for being mostly addressed and a weight of 10% for doubling up as a sub-attribute. 60% was also the weight of Availability for doubling up as a sub-attribute and 17% for being mostly addressed. Cost has a weight of 77% for doubling up as a sub-attribute and a weight of 11% for having sub-attributes. Finally, Security is seen to have 56% for doubling up as a sub-attribute and 9% for having sub-attributes.

## VI. CONCLUSION AND FUTURE WORK

The paper uses a multi-criteria decision-making analysis based on the expert's evaluation and the use of the Analytic Hierarchy Process (AHP) to rank software quality attributes. A hierarchical model is presented for the AHP process. The results show the criteria weight of Maintainability to be 17.37%, Testability to be 13.02%, Reliability to be 10.35%, Efficiency to be 7.49%, Usability to be 7.22%, Portability to be 7.13%, Reusability to be 6.86%, Security to be 13.61%, Functionality to be 6.22%, Availability to be 5.99% and Cost Co(s) to be 4.73%. Maintainability is therefore the most important quality attribute followed by Security, Testability, Reliability, Efficiency, Usability, Portability, Reusability, Functionality, Availability and Cost.

The future work will include the integration of AHP with Linear Programming (LP) to select the most important software quality attribute among several attributes. The criteria weights produced from the AHP technique will serve as function coefficients in LP to build a linear model. Sensitivity analysis will also be performed to check changes in criteria weight and effect on the attributes.

### REFERENCES

- [1] I. Gambo, A. Soriyan, and P. Achimugu, (2011) "Software Architecture Performance Quality Model: Qualitative Approach", ARPN Journal of Systems and Software, Vol. 1, No. 1, pp. 28-33.
- [2] S. Slaughter, D. E. Harter, and S. A Slaughter, (2000), "Process Maturity and Software Quality: A Field Study", International Conference on Information Systems, pp. 407 - 411.
- [3] N. B. Kassie, J. and Singh, (2020) "A Study on Software Quality Factors And Metrics to Enhance Software Quality Assurance", International Journal of Productivity and Quality Management, Vol. 29, No. 1, pp. 24-44.
- [4] M. G. Siavvas, K. C. Chatzidimitriou, and A. L. Symeonidis, (2017), "QATCH - An adaptive framework for software product quality assessment", Expert Systems With Applications, 43 pp.
- [5] M. K. Sharma, (2017), "A study of SDLC to develop well-engineered software", International Journal of Advanced Research in Computer Science, Vol. 8, No. 3, pp. 520-523.
- [6] J. A. McCall, and P. K. Richards, (1977) "Factors in Software Quality: Concept and Definitions of Software Quality", Final Technical Report, Vol. 1, 168 pp.
- [7] B. W. Boehm, J. R. Brown, H. Kaspar, M. Lipow, G. McLeod, and M. Merritt, (1978) "Characteristics of Software Quality", North-Holland Publishing Company, 169 pp.
- [8] R. S. Jamwal, and D. Jamwal, (2009), "Issues and Factors For Evaluation of Software Quality Models", Proceedings of the 3rd National Conference, pp. 1 - 6.
- [9] R. B. Grady, (1992), Practical Software Metrics for Project Management and Process Improvement, Prentice Hall Inc., Englewood Cliffs, NJ, USA, 270 pp.
- [10] G. R. Dromey, (1995), "A Model for Software Product Quality", IEEE Transaction on Software Engineering, Vol. 21, No. 2.
- [11] ISO/IEC 9126-1 (2001), "Software Engineering - Product Quality - Part 1: Quality Model", Vol. 1, International Organization for Standardization: Geneva, 25 pp.
- [12] O. Kononenko, O. Baysal, and M. W. Godfrey, (2016), "Code Review Quality: How Developers See It", IEEE/ACM 38th IEEE International Conference on Software Engineering, pp. 1028 - 1038.
- [13] S. Parthasarathy, C. Sridharan, T. Chandrakumar, and S. Sridevi, (2020) "Quality Assessment of Standard and Customized COTS Products", International Journal of Information Technology Project Management, Vol. 11, No. 3, pp. 1-13.
- [14] T. A. Alrawashdeh, M. Muhairat, and A. Althunibat, (2013) "Evaluating the Quality of Software in ERP Systems Using the ISO 9126 Model", International Journal of Ambient Systems and Applications (IJASA), Vol. 1, No.1, 9 pp.
- [15] A. Kabir, M. U. Rehman, and S. I. Majumdar, (2016) "An Analytical and Comparative Study of Software Usability Quality Factors". 7th IEEE International Conference on Software Engineering and Service .
- [16] B. B. Rohila, and A. G. Dinker, (2014) "An Approach for Enhance the Software Quality Based on Quality Model", International Journal of Emerging Technology and Advanced Engineering, Vol. 4, No. 1, pp. 356-361.
- [17] S. Verma, and M. K. Mehlatat, (2017) "Multi-criteria optimization model integrated with AHP for evaluation and selection of COTS components", A Journal of Mathematical Programming and Operations Research, pp. 1-16.
- [18] S. K. Dubey, and A. Mishra, (2014) "Fuzzy Qualitative Evaluation of Reliability of Object-Oriented Software System", IEEE International Conference on Advances in Engineering & Technology Research (ICAETR), pp. 1-5.
- [19] F. Febrero, M. A. Moraga, and C. Calero, (2017) "Software Reliability as User Perception Application of the Fuzzy Analytic Hierarchy Process to Software Reliability Analysis", IEEE International Conference on Software Quality, Reliability and Security, pp. 1-8.
- [20] T. L. Saaty, (1977), "A Scaling Method for Priorities in Hierarchical Structures", Journal Mathematical Psychology, pp. 234-281.
- [21] B. D. Khwanruthai, (2012) "How to do AHP analysis in Excel The Analytical Hierarchy Process - AHP", 21pp.
- [22] O. Taylan, A. O. Bafail, R. M. S. Abdulaal, and M. R. Kabil, (2014) "Construction Projects Selection And Risk Assessment By Fuzzy AHP And Fuzzy TOPSIS Methodologies", Applied Soft Computing Journal, Elsevier, pp. 1-12.
- [23] K. Teknomo, (2006) "Analytic Hierarchy Process (Ahp) Tutorial" <http://people.revoledu.com/kardi/tutorial/ahp/>, Accessed: 15 February 2020.
- [24] T. L. Saaty, (2003), "Decision Making with the Analytic Hierarchy Process", International Journal Services Sciences, Vol. 1, No. 1, pp. 83-98.
- [25] S. Zafar, M. Mehboob, A. Naveed, and B. Malik, (2013), "Security quality model: an extension of Dromey's model", Software Quality Journal, Issue 1, Vol. 23, pp. 29-54.
- [26] T. S. Alanazi, M. Akour, M. Anbar, and A. Alsadoun, (2019), "Enterprise Resource Planning Quality Model ERPQM", 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), IEEE, pp. 1-5.
- [27] J. A. Al-Nawaiseh, Y. Helmy, and E. Khalil, (2020), "A New Software Quality Model For Academic Information Systems: Case Study E-Learning System", International Journal of Scientific and Technology Research, Vol. 9, No. 1, pp. 271-282.
- [28] S. Mahmudova, and Z. Jabrailova, (2020), "Development of an algorithm using the AHP method for selecting software according to its functionality", Journal of Soft Computing, 8 pp.
- [29] M. Yujun, L. Lingli, D. Shuaijun, and L. Guofeng, (2019), "AHP-Based Software Quality Risk Assessment Method for Information System", Scientific Conference on Network, Power Systems and Computing (NPSC), pp. 189-193.
- [30] M. Toapanta, J. Nazareno, R. Tingo, F. Mendoza, A. Orizaga, and E. Mafla, (2018), "Analysis of the Appropriate Security Models to Apply in a Distributed Architecture". IOP Conference Series: Materials Science and Engineering, 5 pp.

# SVM Machine Learning Classifier to Automate the Extraction of SRS Elements

Ayad Tareq Imam<sup>1</sup>, Aysh Alhroob<sup>2</sup>  
Faculty of Information Technology  
Isra University, Amman, Jordan

Wael Jumah Alzyadat<sup>3</sup>  
Faculty of Science and Information Technology  
Al-Zaytoonah University, Amman, Jordan

**Abstract**—The process of extraction of software entities such as system, use case, and actor from an English natural language description of a user's software requirements is a linguistic and semantic process of a natural language processing application. Entity extraction is known to be a complicated and challenging problem by researchers in the fields of linguistics or computation, due to the ambiguities in natural languages. This paper presents a named entity recognition method called SyAcUcNER (System Actor Use-Case Named Entity Recognizer), for extracting the system, actor, and use case entities from unstructured English descriptions of user requirements for the software. SyAcUcNER uses one of the Machine Learning (ML) approaches, that is, the Support Vector Machine (SVM) as an effective classifier. Also, SyAcUcNER uses a semantic role labeling process to tag the words in the text of user software requirements. SyAcUcNER is the first work that defines the structure of a requirements engineering specialized NER, the first work that uses a specialized NER model as an approach for extracting actor and use case entities from English language requirements description, and the first time an SVM has been used to specify the semantic meanings of words in a certain domain of discourse; that is the Software Requirements Specification (SRS). The performance of SyAcUcNER, which utilizes WEKA's SVM, is evaluated using a binomial technique, and the results gained from running SyAcUcNER on text corpora from assorted sources give weighted averages of 76.2% for precision, 76% for recall, and 72.1% for the F-measure.

**Keywords**—Information extraction; named entity recognition; machine learning; support vector machine; software requirement specification; WEKA; I-CASE

## I. INTRODUCTION

The system, use case, and actor are the main entities of the Software Requirements Specification (SRS), which is an unformatted Natural Language (NL) text description of a system. The extracting of these entities is considered the first step in the development of desired information system, as the actors are the individuals that use the system like humans, external software, etc., in which each actor has certain roles, and the use cases are used to (1) identify the functional requirements of the developed system that would be used by actors, (2) design the system's architecture, (3) control the implementation of the system, (4) verify and validate the developed system via generating test cases [1].

Based on the above, the extracting of the system, actor, and use case entities from SRS has been recognized as a key step in analyzing software user requirements and it is achieved by using systematic definitions of these entities [2]. Usually, a

manual approach, which was described algorithmically by [3] and [4], is used to achieve the process of extracting SRS elements.

Due to the unstructured style of the written SRS, certain problems exist that impose a careful linguistic analysis by a human to be accomplished properly. As a consequence, the manual approach can be error-prone and time-consuming [5] [6]. To facilitate and speed up the performing of extracting the SRS elements from an unstructured and natural language-formed user requirement text, a set of solutions have been proposed to automate this process.

The previously proposed solutions for automating the extraction of SRS fall into two approaches. The first one is the production rules approach, which is, in general, has shortcomings like vagueness, inefficiency (time-consuming execution, intelligent interpreter, and difficulty to follow the execution control), absence of learning ability, and the resolution's conflict [7] [8] [9]. The second approach is the connectionist approach – or the Artificial Neural Networks (ANN), which is (in addition to be computationally expensive) has some problems like the poor ability to predict, the excessive training required for developing a solution, the long time that is required to develop a network, and the unexplainable answer (Blackbox) [10] [11]. ANN approach is a Machine Learning (ML) method, which has other methods. Because of the problems that ANN has, this paper proposes the use of another ML method that is the Support Vector Machine (SVM) method to automatically extract system, actor, and use case entities from unstructured NL requirements text documents in English.

An SVM is used to create a learning model based on a supervised learning approach that uses pre-labeled training data to train the model to classify these data [12]. SVM is a non-probabilistic binary classifier that categorizes data into several classes. The binary classification SVM achieves classification by mapping input data to classes (hyperplanes) in an N-dimensional space based on a maximal margin, where N is the number of features of a data point [12]. SVM is a very useful classifier of undistributed data and irregularly distributed data, which can be of different types like text, images, audio, and other types. This is seen in the different and many real-world applications where SVM is used such as sentiment analysis, handwriting recognition, a cancer diagnosis.

Although there are many classification algorithms in machine learning, yet, SVM has been shown to achieve

significantly better and more robust classification than other supervised learned- classification algorithms due to the following outstanding properties [12] [13]:

1) SVM is distinguished in learning by:

- SVM has no overfitting problem.
- SVM can apply to semi-supervised learning models also.
- SVM works stably and it generalizes well to data not included in the training data set or that data that its features would be changed. This is because the SVM classification approach is principally reliant on a subset of points only in its work to maximize the gap (margin) between nearby points of classes. It means that only an inliers subset of points is helpful and no need to consider outliers points.
- SVM is a fast-learning algorithm as the kernel function of SVM is performed for the classification per training sample. Worthy to note that the Polynomial kernel was proved as a better factor in SVM.
- SVM is robust, which is shown by its ability to produce a unique solution.

2) SVM is more efficient in high  $n$ -dimensional space, in cases where the number of samples is less than the number of dimensions and is relatively memory efficient.

3) SVM delivers accurate results due to the following:

- The generated hyperplane creates a clear margin to separate classes, and as the large margin is as a more corrected classification of data would be gained. The soft margin is used with non - linearly separable data and the hard margin is used with linearly separable data.
- The convex optimization nature of SVM makes the answer a global minimum rather than a local minimum, which in turn yields more optimality confidence in the results.

4) SVM can be adapted to work with different data types.

This is because SVM has a built-in kernel function, which is a technology that provides the ability to solve any complex problem. Note that Kernel is a non-parametric (linear or nonlinear) identifiable function that comes with different forms depending on the data it operates on.

5) Generally, the SVM classifier has better computational complexity than the other classifiers. SVM has a very little execution time than the Artificial Neuron Network (ANN). SVM has a faster prediction with better classification accuracy than the Naive Bayes classifier. SVM has less time complexity than the logistic regression classifier. SVM is more robust than the logistic regression, just as there is some bias in the training data set.

6) The availability of library SVM classifiers in many programming languages and packages such as MATLAB, Weka, and Python makes the work with SVM so easy.

As shown, the advantages of SVM make it an attractive method that can be used instead of ANN. Worth mentioning that SVM will underperform and being unsuitable when the data sets are large has more noise (overlapped classes) and has no clear probabilistic justification to have classification [12]. To achieve the goal of automating the extraction of SRS elements, our work should answer the following research questions:

- How can SVM be used to extract certain entities from an unstructured text, and.
- What is the performance of a system that utilizes SVM for extracting SRS elements?

Section 2 of this paper illustrates background theoretical issues and Section 3 examines related works and approaches. Section 4 describes the proposed approach, which is followed by a discussion and evaluation of the experimental results in Section 5, and finally, the conclusions, findings, and recommendations are presented in Section 6.

## II. BACKGROUND

This paper is about using the SVM machine learning classifier as the main part of a Named Entity Recognition (NER) system to automate the extraction of SRS elements.

NER is an ML-based process that is used to find and classify names in unstructured or semi-structured texts. These goals are achieved by annotating the words in the text words with the names of categorized entities in the real world, such as locations, places, organizations, companies, persons, individuals, etc. Stanford CoreNLP [14] and the Apache OpenNLP [15] are two well-known examples of NER that extract real-world entities from a text. Also, there are NER models for extracting beneficial information from biomedical texts, such as mentions of proteins and genes and the relationships between them [26]. There are two types of NER methods: the first is an ontology-based NER, which strongly relies on updates of knowledge to successfully distinguish known terms and concepts in unstructured or semi-structured texts [16], and the second is a deep learning NER, which aims (in addition to recognizing terms and concepts) to cluster words by using a word embedding technique that attempts to understand both the semantics of a word and the syntactic relationship between words [17]. As NER is a central subfunction that extracts and classifies certain information (names in a text) from either semi-structured or unstructured text, it is considered an important sub-task of open information extraction (OIE).

OIE is a process that creates a structured representation of information in an unstructured or semi-structured text. The resulting structured representation is usually in the form of  $n$ -ary propositions [18]. OIE aims to extract all types of relations that may exist in a text, whether these are pre-known relations or under discovery. Based on this approach, OIE supports the independent extraction of relations from small, large, and heterogeneous corpora within a specific domain. Automation of the OIE process needs to be efficient, to rely on unsupervised extraction strategies, and to consider corpus heterogeneity [19]. The OIE process is achieved by using

several types of NL processing approaches at the semantic level, all of which function to infer the semantics of a word from its particular linguistic attributes. These attributes are linguistic annotations of a word and are used by a processing technique to recognize a word's semantics (or connotation) within a specific domain. Annotation, for example with part-of-speech (POS) tags, is accomplished by using natural language processing (NLP) tools such as parse trees, syntactic, and dependency parsers [20] [9].

NLP is of great importance in creating human-machine interfaces, and accordingly has become an attractive research field, aiming to find and define algorithms, methods, and approaches to give computers the ability to communicate with a human via natural language [9]. NLP is dedicated to allowing a computer system to perform analysis and comprehension, and to specify the meanings of words or even statements that are written in NL. NLP is a difficult issue in computer science; this is due to the nature of NL, as it naturally suffers from the issues of ambiguity and expressiveness, which easily lead to problems with misunderstanding [21]. In general, working with NLP has moved towards viewing the analysis processing of language as being disintegrated into different sub-processes, illustrating the theoretical linguistic singularity for each of the lexical, syntactic, semantic, and pragmatic levels of NLP [20]. The essential view is that the statements are first investigated according to their syntax; this gives a structure that is increasingly amenable to examination regarding semantics. The next stage, which is a pragmatic analysis, aims to specify the true meaning of the text or speech in the context. The three core subprocesses are syntax, semantic, and pragmatic, all of which serve as a starting point in the processing of texts formed using NL [20]. The standard analysis stages in NLP are [20] [9]:

- 1) *Tokenization*: The process of breaking up a sentence into elements called tokens.
- 2) *Lexical analysis*: A process that aims to check whether a word belongs to a language and to find the part of speech (POS) for the word, or to reveal the class of a word (i.e., verb, noun, or preposition). The lexical analysis also includes the morphological processing of a word, which aims to isolate the stem of the word and its affixes.
- 3) *Syntactic analysis*: This applies the grammar of the language (using a parsing algorithm) to identify the legal structure of the input statement.
- 4) *Semantic analysis*: This is the process of extracting the exact meaning from the text.
- 5) *Pragmatic analysis*: This aims to infer the purpose of the use of the word/text in situations and requires knowledge about the domain of discourse. It is achieved by reinterpreting the text as it really implies.

In short, the linguistic and semantic analysis of a text is carried out either as a semantic analysis of the whole text as a single unit or as a semantic analysis of individual words in a text. The first approach is used to recognize the intention or sentiment of a speaker, and the second is used to extract specific information from a text, or in other words to convert semi-structured and unstructured text to a structured form.

Here, NER has a key role in the semantic stage of NLP in terms of extracting the meaning of words and sentences in addition to their relationships.

### III. RELATED WORKS AND APPROACHES

Automation of the manual approach to extracting actors and use cases from software requirements statements shows that several types of NLP tools and approaches have been used for extracting certain semantics from software functional requirements described in natural language.

The first approach described here is the use of the production rules that govern linguistic properties to extract the elements of the software requirements that are required to develop each use case diagram and class diagram. This approach was utilized by the UMGAR system [22]. A similar technique known as a rule-based approach was proposed by [23] for automatically extracting use cases and goal models from unformatted, NL, and textual documents of requirements. This approach combines a number of methods to detect goals and the entities of use cases along with their relationships from the textual document. The semantic parameterization of textual specifications is used to guide the detection process of the rules. Worth to report here that the Genetic Algorithm (GA) can be utilized as a supporting step – for optimization purposes- to select the best set of production rules that should be manually created earlier. The approach can be seen in the work of [24] to discover the best classification rules for the Car, Zoo, and Mushroom classes, and the work of [25] that used GA (with treebank) to develop a syntactic analyzer to enhance the Parseval score of seed grammar rules.

Production rules may be supported by an NLP tool to facilitate the development of more precise recognition rules. A hybrid NLP tool that combines production rules with predefined types of use cases and actors is used by [1]. Also, a combined NLP and domain ontology approach was used in RAPID, a scheme proposed by [26] that takes textual requirements in NL form and extracts the primary concepts and their relationships to create unified modeling language (UML) diagrams.

An approach using a set of semantic heuristics rules to generate the patterns used to extract the use case model, based on a general NLP tool, was proposed by [27]. The software requirements processed in this work are Arabic natural language texts, and the generated patterns depend on the sentence structure. The Stanford parser is the NLP tool utilized in this approach. This scheme follows the work of [21], which uses an open NLP tool called Semantic Business Vocabulary and Rules to extract object-oriented models from user software requirement specifications (SRS).

Conversion of the description of requirements from a natural language form to structured natural language as a prior step in utilizing other NLP analyzing processes is the approach used by [28]. The conversion process is facilitated by an elicitation process, both of which form part of an expert system that elicits requirements from different stakeholders and maintains a knowledge base that supports the future extraction of certain elements from similar requirement descriptions. A very similar approach is used by [29], who proposes an

approach that takes requirements in NL form and converts them to an intermediate structured representation using grammatical knowledge patterns and the dependency analyzing of the requirements statements. This intermediate representation is used to create a class diagram.

An approach using POS, pre-processing, and parsing to extract certain UML models, called GUEST, is proposed by [30]. This is a semi-automated rule-based approach that aims to specify models of the goal and use case from unformatted textual requirements documents. In this scheme, a number of different techniques are utilized to discover and classify the goals, use cases, and their relationships from a text, and semantic parameterization of the textual specifications is carried out. In two selected case studies, GUEST is used to process software user requirements described in NL text, and producing activity and sequence diagrams. A Recursive Object Model (ROM) diagram is utilized to extract semantic information from requirements by [31]. This extracted semantic information then forms the elements required by system modeling language (SysML), which is similar to UML, to produce different system models.

Without denying the achieved results gained by supporting the rule-based approach by GA, NLP tools, heuristic style, and the modeling approach, the shortcomings of the rule-based approach still exist. The general shortcomings of the rule-based approach have been reported in the introduction. The best-reported achievement of the rule-based approach is the one that comes from the work of Marinos et al [1], which was 96% of precision.

The alternative approach to the rule-based approach is the connectionist approach that uses Artificial Neural Networks (ANN) to elicit the SRS's elements. This is a Machine Learning (ML) approach that had been agreed as a good solution to the problems accompanied by the rule-based approach. ANN, together with Semantic Role Labeling (SRL), was suggested by Al-Hroob et al [32] to extract the use case and actor SRS entities from NL statements of user requirements, as this work is the best-reported achievement that is 47.2% of precision.

#### IV. PROPOSED SYACUCNER APPROACH

Examination of the related works and approaches described above inspired us to seek a new approach to extract SRS

semantics, namely the system, actor, and use case. We aimed to find an approach that relies on the linguistic (lexical and semantic) attributes of a word to discover its true SRS semantics.

In this work, we view NER as a process of extracting a structured form (that is, a system, an actor, and a use case form) from semi-structured or unstructured text (i.e. a user requirements text). Here, NER is applied to the specific domain of the user requirements of the software, rather than a real-world domain. NER is accomplished as a mapping process of certain nouns into a predefined system or actor classes of the software requirement domain and certain verbs into a predefined use case class of the software requirements domain. In fact, NER has previously been used in a specific domain by [33], who developed a rule-based NER model for knowledge extraction of evidence-based dietary recommendations (in the biomedical domain).

In our suggested SyAcUcNER approach, NER is an SVM-based model that uses certain linguistic attributes of a word to recognize the entities of the system, the use case, and the actor from a textual description of software requirements. As illustrated in Fig. 1, SyAcUcNER is created during the training phase and is used for extraction during the testing phase. A subprocess involving the linguistic annotation of a statement's tokens is performed in both phases to prepare the data that will be used for recognition by the SVM data mining model in the training phase and SyAcUcNER in the testing phase.

##### A. NL Functional Requirements

The data set used to train SVM contains 66 English language statements with different structures, representing software requirements. We collected these statements from various sources, such as books and examples in the literature, and also from actual software analysis tasks. In each statement, the tokens representing a system, an actor, and a use case of SRS are manually defined, and their linguistic attributes (lexical category, SRL, and dependency relations) are automatically extracted and exported to an Excel spreadsheet. Due to the exceptional importance of the data set in creating an effective classification model, certain properties are considered when selecting these 66 NL statements of functional requirements. These properties are the numbers and types of system, use cases, and actors that exist in an NL functional requirements statement.

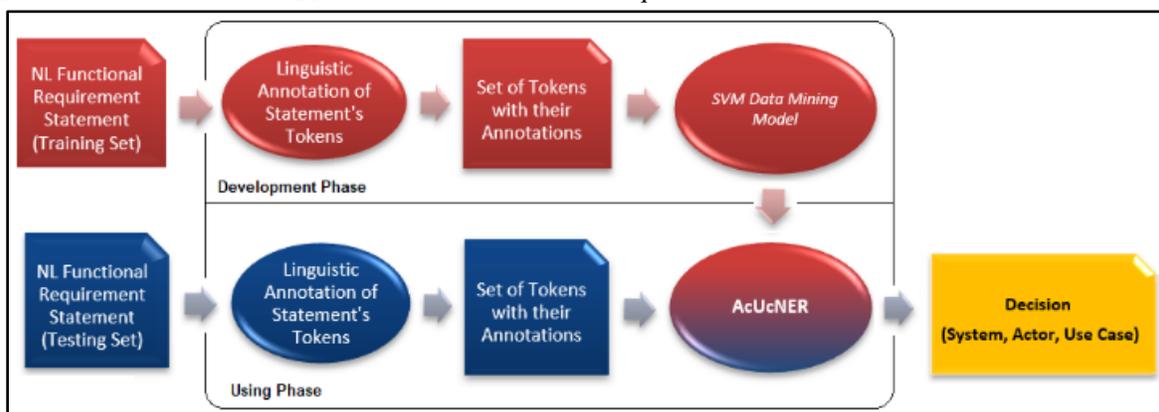


Fig. 1. The Proposed SyAcUcNER Approach.

### B. Annotation of the Tokens of the Sentence

The SRSs are tokenized into words, and each word is given linguistic attributes that are used to distinguish the word. The tokenization of a statement aims to isolate the words within it, as a first step in eliciting the system, actors, and use cases. In this paper, we use the following linguistic attributes of a word to distinguish its true semantics in an NL functional requirement statement (system, actor, and use case):

- Lexical attribute: This is the linguistic type of a word in a language. In English, these include a noun, verb, adjective, adverb, conjunction, particle, and adposition [20] [9]. This attribute is usually given with the word in a dictionary. The realization of the lexical category of a word is automatically achieved using computerized NLP systems [9].
- SRL attribute: This is the thematic role property of a noun within a statement (rather than the lexical semantics of a word).

The annotation of semantic roles is an approach in which the arguments (nouns) of a predicate (usually a verb) are classified based on a predefined set of participant types (annotations). These participant types are either the semantic relationships between the arguments of the verb or the circumstance that is described by the verb. The participant types (i.e., the annotations), which are known as semantic or thematic roles, are defined by linguistics [34] [35] [36], as illustrated by Table I, which lists the known thematic roles of a noun. SRL is the process of automatically assigning a semantic role to a noun [9]. In SRL, the verb is considered the predicate, and the semantic role labels or annotations that label a verb's arguments (nouns) are used to specify the true meaning of the verb (predicate) itself. The author in [37] gives an example to illustrate the use of the SRL approach to realize the semantics of a verb by explaining how to differentiate between break and hit verbs: a hit verb has the argument (Agent, Instrument, Place) and the verb break has the arguments (Agent, Instrument, Object). In practice, the semantics of verbs have been used in a number of studies where the verb is the core element of a linguistic process, for example, the development of an approach for converting pseudocode to C# [38].

- Dependency (clausal argument) relations attribute: Dependency relations are a set of directed binary grammatical relationships that exist among the words of a text. These relations are used to encode significant hidden information that results from the analysis of a complex phrase structure. Dependency grammars are the formalisms that use clausal argument relation annotations to tag binary grammatical relationships between the syntactic words (or lemmas) in a sentence. This type of grammar and its parsing scheme is of key importance in dealing with morphologically rich languages that have a relatively free order of words [39] [9]. Fig. 2 illustrates an example of a method based on dependency grammars.

Clausal argument (dependency) relations are defined (among other types of dependency) in a universal dependency (UD) set, and this annotation method uses a dependency parsing process to achieve this task [9]. UD dependency banks are available for more than 50 languages. This is due to the fact that each language has its own set of dependencies and may or may not share these with other languages; in addition, some languages have no UD. This means that a balance must be found between universality and meaningful dependencies, and with other requirements such as parsing efficiency, ease of human annotation, etc. Another challenge is presented by the vagueness that limits the identification of all UD classes [8].

Although there are continuing efforts to define a cross-linguistically and computationally useful set of dependency relations, it is worth mentioning here a linguistically motivated study of UD that is handled by [41]. Table II shows a subset of the clausal argument relations in UD (others are found at <https://universaldependencies.org/u/dep/>).

TABLE I. LIST OF THEMATIC ROLES

Thematic Roles	Definition
Agent	An action's doer/instigator, denoted by the predicate
Patient	An action's 'undergoer', denoted by the predicate
Theme	An action's moved entity, denoted by the predicate
Experiencer	An action's living-entity practitioner, denoted by the predicate
Goal (direction)	An object's destination, indicated by a transfer event
Beneficiary	The entity that gets the benefit denoted by the predicate
Source (origin)	The location from which something moves
Instrument	The medium used to act, denoted by the predicate
Locative	The situation/location in which the action occurred
Stimulus	Accidental sensory trigger
Force or natural cause	The entity that does the action
Recipient	The entity that denotes a change in ownership, possession
Time	The time of occurrence of an action
Manner	How an action is accomplished
Purpose	The reason for performing an action
Cause	The reason for the action occurring

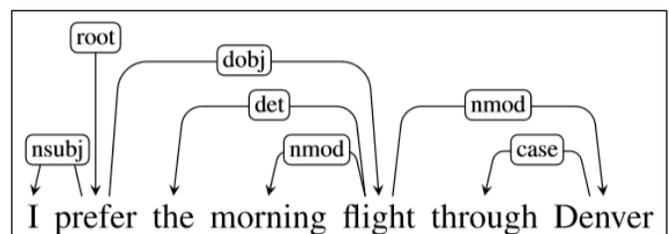


Fig. 2. Results of Dependency Parsing of a Sentence [9].

TABLE II. SELECTED DEPENDENCY RELATIONS FROM THE UD SET [40]

Clausal argument relations	Description
advmod	adverbial modifier
amod	adjectival modifiers
aux	auxiliary
cc	coordinating conjunction
ccomp	clausal complement
conj	conjunct
dep	dependent
det	determiner
dobj	direct object
iobj	indirect object

To facilitate the process of extracting the SRL and dependency relationships between the words in an SRS, we used an NLP software tool that can provide these linguistic attributes for SRS tokens in English. The LTH (Lunds Tekniska Högskola) System for Frame-Semantic Structure Extraction (or SRL) software tool is used in this work, as it allows for dependency parsing and SRL in addition to other NLP processes such as tokenization, POS-tagging, lemmatizing, morphological tagging, and graph visualization [42]. Fig. 3 illustrates the semantic parsing results yielded by the LTH system for an SRS. The LTH system provides a table

of annotation data for tokens (the second table of parsing results) based on a CoNLL-2009 shared task.

A CoNLL-2008 shared task is used to define the format of the data provided in a CoNLL-2009 shared task, with some modifications related to enhancing the performance of the CoNLL-2009 shared task over the CoNLL-2008 shared task. Although they are similar for all-natural languages, they may vary in terms of content [43]. The lexical attribute of a token is obtained from the predicted part of the speech (PPOS) field (coded as NN for the name, VB for the verb, etc.). The dependency relation attribute is obtained from the PDEPREL field. The semantic roles of the arguments of a predicate are obtained by following the hyperlink of the predicate (verb) that appears in the parsing table (the first table in Fig. 3). For example, the arguments of the predicate (verb) change.01 shown in Fig. 4, are 'the user' (coded as A0, i.e. an Agent semantic role), and 'the meal date' (coded as A1, i.e. a Patient semantic role).

It is important to note the differences between the standard values of the lexical, SRL, and dependency relations and those of CoNLL-2009 (the core of the LHT system used here). The latter aims to perform and evaluate SRL using a dependency-based representation to predict syntactic and semantic relations [44]. CoNLL-2009 [45] provides a more complicated model of syntactic dependencies, based on a belief that more syntactic dependencies lead to more effective semantic processing, especially in applications such as IE.

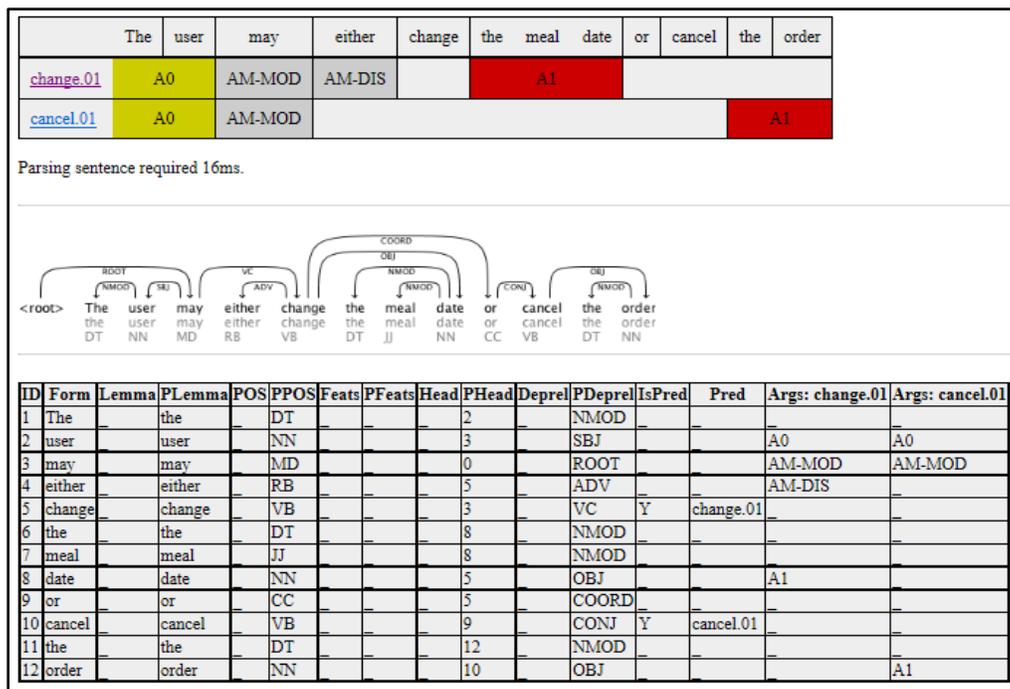


Fig. 3. Semantic Parsing of a Software Requirement Statement using LTH [42].

Predicate: <i>change</i>																	
<b>Roleset id:</b> <i>change.01</i> , <i>transform</i> , <b>Source:</b> , <b>vncls:</b> , <b>framnet:</b>																	
<i>change.01</i> : CHANGE-V NOTES: "Start state" and "thing changing" are usually the same, but there can be cases where they are separate. Reserve use of Arg3 for these cases. (from <i>change.01-v</i> ) CHANGE-N NOTES: Roleset based on verb entry <i>change.01</i> . VerbNet classes 26.6.1-45.4. (from <i>change.01-n</i> )																	
<b>Aliases:</b>																	
<table border="1"><thead><tr><th>Alias</th><th>FrameNet</th><th>VerbNet</th></tr></thead><tbody><tr><td><i>change</i> (v.)</td><td></td><td></td></tr><tr><td><i>change</i> (n.)</td><td></td><td></td></tr><tr><td><i>make_change</i> (l.)</td><td></td><td></td></tr><tr><td><i>changing</i> (n.)</td><td></td><td></td></tr></tbody></table>	Alias	FrameNet	VerbNet	<i>change</i> (v.)			<i>change</i> (n.)			<i>make_change</i> (l.)			<i>changing</i> (n.)				
Alias	FrameNet	VerbNet															
<i>change</i> (v.)																	
<i>change</i> (n.)																	
<i>make_change</i> (l.)																	
<i>changing</i> (n.)																	
<b>Roles:</b>																	
"Start state" and "thing changing" are usually the same, but there can be cases where they are separate. Reserve use of Arg3 for these cases. (from <i>change.01-n</i> )																	
<b>Arg0-PAG:</b> <i>causer of transformation</i> (vnrole: 26.6.1-1-Agent, 45.4-Agent)																	
<b>Arg1-PPT:</b> <i>thing changing</i> (vnrole: 26.6.1-1-Patient, 45.4-Patient)																	
<b>Arg2-PRD:</b> <i>end state</i> (vnrole: 26.6.1-1-Result)																	
<b>Arg3-VSP:</b> <i>start state</i> (vnrole: 26.6.1-1-Material)																	
<b>Example:</b> <i>agentive</i>																	

Fig. 4. SRL for Predicate Change.01 [42].

### C. Set of Tokens with Annotation

The linguistic analysis information (lexical, dependency relationships, and SRL) resulting from the LTH system software tool were manually assigned to an Excel spreadsheet of tokens (for a given SRS) with their annotations. We considered only tokens that were system, actor, or use case.

As shown in Fig. 1, there are two versions of the set of tokens with annotations. The first, which is used in the training phase, contains the tokens and their linguistic annotations (lexical, SRL, and dependency relations), which take the form of a table with text values. The SRS identity of a word (token) is specified manually, forming a training set of data that can be used to train the SyAcUcNER (SVM-based), model. The textual contents of this table can be converted to a numeric form, allowing them to be handled by the SVM in the next processing step. The second version of the set of tokens and annotations is used in the testing phase and is similar to the first except that the SRS's entity is not manually assigned to each token. Instead, SyAcUcNER is responsible for performing this assignment or other word recognition of the SRS identity of a token. In both versions of the table, the contents are numerically coded and saved as a .csv file, conforming with the format required by Weka software, in which its SVM was used to perform the classification of the tokens. The coding of the word (token) was neglected, and coding only the linguistic features (lexical, SRL, and dependency relation) with their corresponding SRS.

We developed and implemented an algorithm to code and save the table of the set of tokens, as shown.

---

### *Create\_Coded\_Data\_File (Table of tokens with their features and annotations)*

---

Begin

For all tokens in the table

- Code the lexical attribute field according to the LexicalCodeTable
- Assign LexicalCodeValue to its column in the Coded\_Data Table
- Code the SRL attribute field according to the SRLCodeTable
- Assign SRLCodeValue to its column in the SRLData Table.
- Code the dependency relation attribute field according to the DepRelCodeTable
- Assign DepRelCodeValue to its column in the Coded\_Data Table
- Code the SRS Field according to the SRSCodeTable
- Assign SRSCodeValue (in term of char 'c' and a sequence) to its column in the Coded\_Data Table

End For

Save Coded\_Data Table in a .csv file.

End

---

We used Excel software to maintain tables of the software statements, their tokens, linguistic attributes, and codes. We used the VBA function in Excel to implement the Create\_Coded\_Data\_File algorithm. In practice, this function forms a pre-processing step ensuring that the values of the targeted attributes conform to the constraints of Weka, which is used in the next processing step.

#### D. SVM Data Mining Model

Based on our view of the system, use case, and actor semantics of SRS as classes, we used SVM to generate and optimize combinations of classifications for each of these SRS's semantics.

In the example shown in Fig. 5, where SVM is used for induction purposes, the training data are represented as vectors  $\{X_1, \dots, X_n\}$  in a domain  $D$ , where  $X_i \in D$  and their labels are represented as  $\{Y_1, \dots, Y_n\}$ . The vectors positioned on one side of a hyperplane would be labeled as  $Y_\alpha$ , and the vectors on the other would be labeled as  $Y_\varepsilon$ . The support vectors are the lying instances that closest to the hyperplane that is the decision surface [46].

Since we use SVM in this work, the training data vectors  $\{X_1 \dots X_n\}$  are required, where  $X_i$  is represented as  $\{x_1, x_2, x_3\}$  in English language (El) space  $X \subseteq El$ . The labels  $\{Y_1, \dots, Y_n\}$  are also needed, where  $Y_i \in \{1,2,3\}$ , representing  $\{\text{System, Actor, Use Case}\}$ . These training data were prepared using the `Create_Coded_Data_File` function given above. In general, SVM projects data in space  $(X)$  to a higher-dimensional feature space  $(f)$  using a Mercer kernel operator  $K$ . A set of classifiers are formed as follows [46]:

$$f(x) = (\sum_{i=1}^n \alpha_i K(X_i, X)) \quad (1)$$

In the case where  $K$  satisfies Mercer's condition,  $K(a,b)$  we can be rewritten as [47]:

$$K(a,b) = \Phi(a) \cdot \Phi(b) \quad (2)$$

where  $\Phi: X \rightarrow F$ , and “ $\cdot$ ” symbolizes the inner product operation.

Thus,  $f$  in (1) can be rewritten as:

$$f(x) = w \cdot \Phi(x), \text{ where } w = \sum_{i=1}^n \alpha_i \Phi(X_i) \quad (3)$$

Consequently, the use of  $K$  enables us to implicitly project the data into space  $(f)$ , which usually has higher dimensional features. SVM can then be used to map the  $\alpha$ is, which agrees with the maximal margin hyperplane in  $(f)$ . Changing kernel functions would implicitly project the data from space  $X$  into space  $f$ , where their hyperplanes agree with the decision boundaries of the more complex features in space  $X$  [47] [46]. SVM is a supervised learning method, in which a learning algorithm utilizes pre-labeled training data to develop a classification model that outlines classes and their distinguished data values. The resulting trained classification model can be used to classify new data. SVM has been extended to perform non-linear classification, multi-class classification, and regression analysis [13] [48]; therefore, is recognized as a robust classifier.

Weka (Waikato Environment for Knowledge Analysis) is a machine learning software technology that offers implementation of SVM in addition to other machine learning algorithms [49]. It is free software, licensed under the GNU General Public License, and was developed at the University of Waikato, New Zealand.

The SVM in Weka can handle numerical input data saved in an Excel file with only one worksheet, as a .csv file. The `Create_Coded_Data_File` VBA macro yields the `Coded_Data.csv` file, which contains the coded SRS classes and the value of their linguistic attributes as a table. The header of this table is the metadata of its fields, which are  $a_1$  (representing the lexical attribute code),  $a_2$  (representing the SRL attribute code),  $a_3$  (representing the dependency relation attribute), and  $a_4$  (representing the SRS class attribute code), where ‘a’ means ‘attribute’. It is important to note that the values  $a_4$  are nominally in the form of a char  $c$  (meaning ‘class’) along with numbers such as  $c_1, c_2$ . Weka's SVM is referred to as ‘SMO’ in its classifier list. This stands for sequential minimal optimization, and it is an efficient optimization training algorithm for SVM [13] [49].

The training data file was loaded via the Open file command button. The attributes of the data set were displayed in the Attribute submenu, in addition to other related information about the dataset. The classes (i.e. system, actor, and use case in this study) appear in different colors in the lower right-hand corner of the Weka Explorer interface.

Weka's SVM is a Java class with certain properties, and these can be displayed by clicking the text box near the Choose command button. In this work, the properties of the SMO were set using trial and error to obtain the most accurate SVM-based NER model.

The SyAcUcNER model produced in this research is a multi-class classification model that maps input data to system, actor, or use case classes. To achieve multi-class classification with Weka's SMO (i.e., an SVM), the classification method was set to Hastie and Tibshirani's pairwise coupling (also known as ‘1-vs-1’). In order to achieve accurate possibility estimates, an option is used that fits the calibration models to the SVM's outputs [50] [51]. When the properties are set, the SMO is then trained, and this is achieved via the Start command button in the Classify tab of the Explorer window in Weka. The classifier output (analysis of the classification performance) is then displayed in the lower right-hand corner of the Weka Explorer window. Fig. 6 shows one of the training runs.

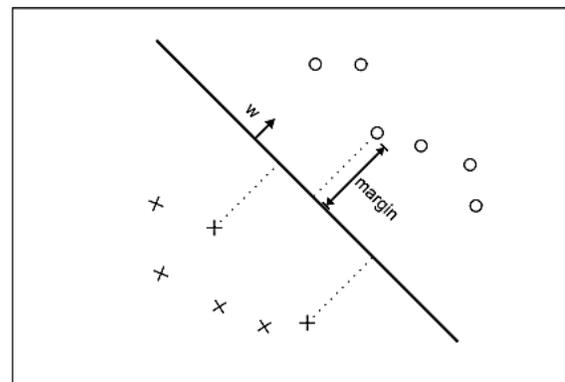


Fig. 5. A Simple SVM for Induction [46].

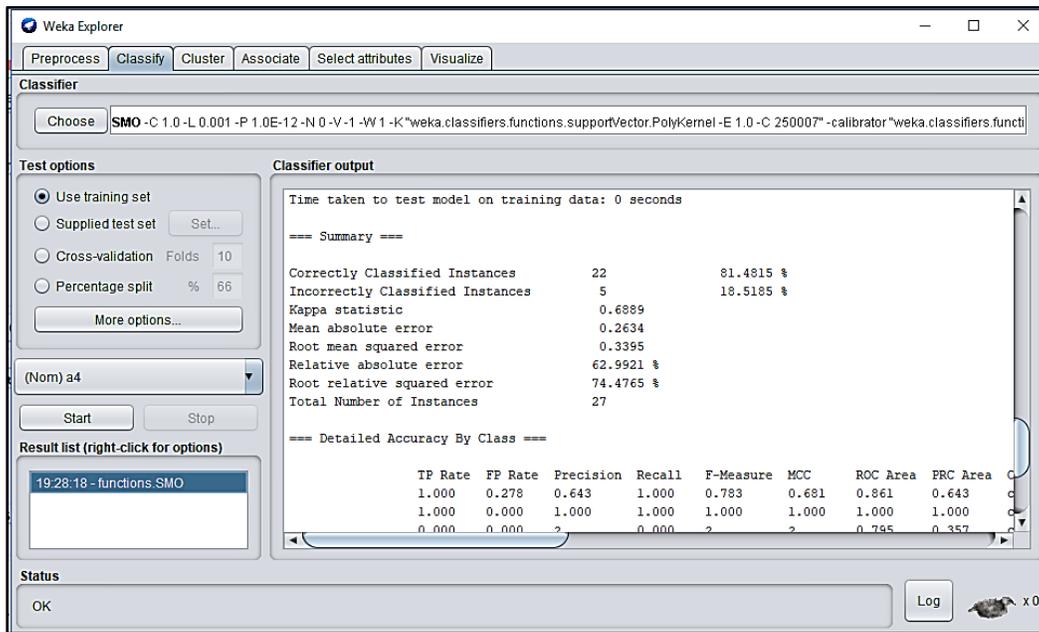


Fig. 6. Running (Training) Phase of Weka's SMO Function [52].

The finalized and trained SMO model is then saved to an external file so that it can be loaded later and used to make predictions using the testing data. The SyAcUcNER Model

The final trained SyAcUcNER model is a specialized named entity recognition model for software requirements engineering based on SVM. This model can then perform the classification of testing data (that have been pre-processed) in the same way as for the training data. The testing data represent the actual problems that a software requirement analyzer needs to solve. The saved SyAcUcNER model has first loaded it from its file; this is achieved by following the same steps used to

save the trained model but selecting the option Load model instead of the Save model. Predictions are made for the new testing data by loading the test and then selecting the Classify tab, the Test options pane, and the Supplied test set option. The file format of the output predictions is set to .csv, and the evaluation metrics utilize each of the elements of the binomial approach (TP, FP, Recall, Precision, and F-measure) and the number of correct and incorrect predictions. When the Start command button is clicked, the predictions for each test instance are listed in the Classifier output pane. Fig. 7 illustrates a testing run for 99 instances of the testing data.

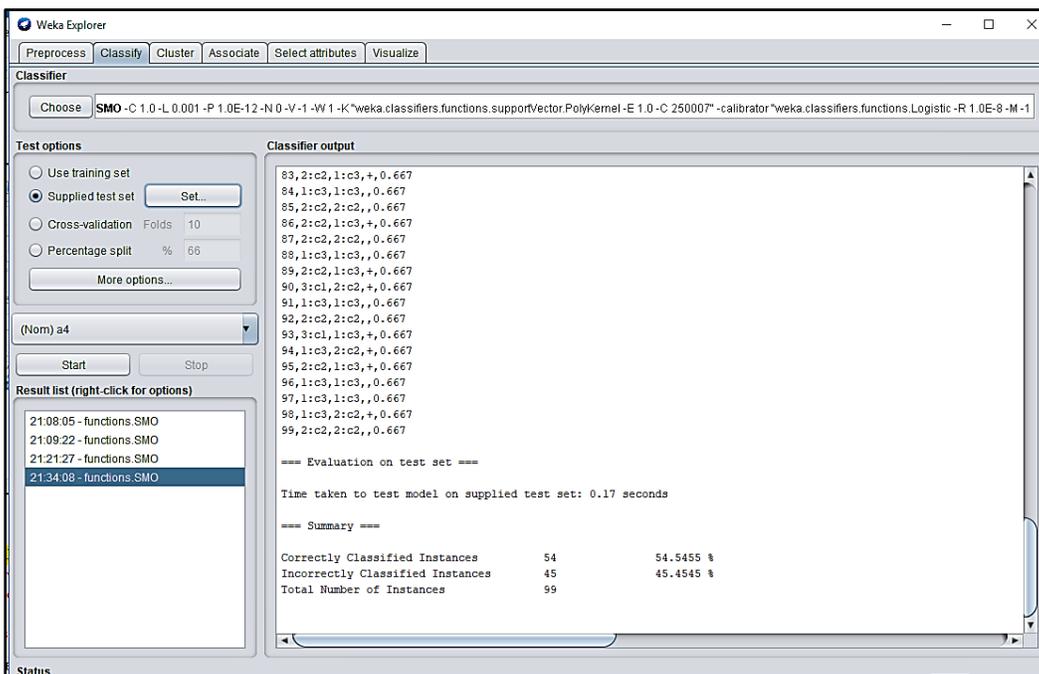


Fig. 7. Using the Trained SyAcUcNER Model on Testing Data [52].

## V. RESULTS AND EVALUATION

The performance of the SyAcUcNER model and the selection of distinguishing features (lexical, SRL, and dependency relations) were assessed for a given testing data set by selecting the Supplied test set option in the Test option pane of the Classify tab in the Weka Explorer interface.

We scored SyAcUcNER's performance in terms of its accuracy, defined as the quality degree of a class achieved by the proposed model compared with the true quality degree for the same class [22]. Accuracy was quantified by calculating the ratio of the number of correctly classified cases to the total number of classified cases, and was mathematically described using the following formula [53]:

$$\text{Accuracy} = \frac{\text{number of correctly classified cases}}{\text{total number of cases}} \quad (4)$$

The use of this naïve definition of accuracy to score the performance of a classification model overlooks both the real threats from the different forms of errors and the ability to be free from error depending on the distribution of the classes in a dataset while calculating the accuracy. A better analysis of the error (in terms of recognizing the types of wrong classification results) can be achieved by using a two-dimensional confusion matrix. Each row of the confusion matrix contains a forecasting class and its recorded incidence number, while each column contains the actual class and its recorded incidence number. An increase in the number of classes in the classification leads to a larger confusion matrix, causing a significant problem; this can be solved by classifying the results as either positive or negative relative to the target class, thus giving four different numbers [54] [55]:

- True positive (TP) value: The number of correct positive classifications.
- True negative (TN) value: The number of correct negative classifications.
- False-positive (FP) value: The number of incorrect positive classifications.
- False-negative (FN) value: The number of incorrect negative classifications.

As illustrated in Table III, these values are used to calculate the set of performance metrics. Finally, we made a number of train courses, each with different settings for the properties in the SMO object (Weka's SVM).

TABLE III. PERFORMANCE METRICS [54] [55]

Metric	Formula
Percentage of TP value (TP rate)	$TP / (TP + FN)$
Percentage of FP value (FP rate)	$FP / (FP + TN)$
Percentage of TN value (TN rate)	$TN / (TN + FP)$
Percentage of FN value (FN rate)	$FN / (FN + TP)$
Percentage of TP to all true values (Precision)	$TP / (TN + TP)$
Percentage of all true results (Accuracy)	$TP+TN / (TP+FN+FP+TN)$
Precision & recall harmonic mean (F1 Score)	$2*(\text{Precision}*\text{Recall}) / (\text{Precision}+\text{Recall})$

We used a common agreement among the users of Weka, which is the trying of a suite of different values of kernels and C parameters could lead to the best achievement. Thus, we got good accuracy in terms of a weighted average of 76.2 percent for precision, 76 percent for recall, and 72.1 percent for the F-measure. Using this configuration, we obtained the highest F1 scores of 21.4 percent for the system entity, 82.5 percent for the use-case entity, and 76.8 percent for the actor entity. The weighted average of F1 was 72.1 percent.

## VI. CONCLUSIONS, FINDINGS, AND RECOMMENDATIONS

In this work, we have proposed a solution to the problem of the automatic extraction of the SRS's entities: the system, the use case, and the actor as a specialized SRS NER that is called SyAcUcNER and uses the SVM to extract SRS elements from an unstructured English language textual document of user requirements. This systematic approach was inspired by the Intelligent Computer Aided Software Engineering (I-CASE) principle [56] and the known NER's function, which is the extraction of certain entities from an unstructured or semi-structured text written in NL.

The SyAcUcNER approach is implemented as software that has embedded other readymade free software tools such as the LTH system (for the extraction of NLP frame-semantic structure) and Weka (that offers SVM). This method facilitates and speeds up the development process and makes the work more robust. The proposed SyAcUcNER has been evaluated using a confusion matrix technique; we believe that this method is a realistic one since it gives the evaluation basing on a comparison with human achievement, rather than a comparison with other systems. The accuracy of SyAcUcNER can be described as good, based on a weighted average of 76.2 percent for precision, 76 percent for recall, and 72.1 percent for the F-measure. A comparison of the results from IT4RE [32], which extracts only the use case and actor, with those of SyAcUcNER, that extracts the system, use case, and actor, gives some interesting results. The best F-measure for IT4RE was 71 percent, while for SyAcUcNER, this was 72.1 percent.

The use of a new suite of linguistic properties, i.e., the lexical, SRL, and dependency relations, demonstrates the effectiveness of SyAcUcNER in reaching such good accuracy. We believe that SyAcUcNER can also be used to recognize more entities, especially if more effective NLP tools are used that can handle the linguistic problems arising from the particular text to be processed, as reported by [32]. The well-structured design of SyAcUcNER also enables it to act as a framework for similar future works. Besides, the use of Weka may allow another data mining machine to be used in this specialized NER rather than SVM. In addition to the achievements in terms of accuracy, the contributions made by this work include a new definition of an SRS-specialized NER and the use of an SVM (i.e., a data mining machine) for NLP-oriented applications at the semantic level. It should be noted that the work of [46] aimed to classify text, rather than engaging in deeper NLP tasks like SyAcUcNER, which performs semantic analysis in the SRS domain. The main contribution of this work is a framework for specialized NER applications, and hence, a general NER structure can be defined and implemented as an object for various discourses.

Last but not the least, we suggest, as future work, to consider the problem of revealing the true meaning of an entity as a complex ambiguity that may be handled by using the Relative-Fuzzy approach, as defined and used by [57].

#### REFERENCES

- [1] M. G. Georgiades and A. S. Andreou, "Formalizing and Automating Use Case Model Development," *The Open Software Engineering Journal*, vol. 6, pp. 21-40, 2012.
- [2] Q. Stiévenart, J. Nicolay, D. M. Wolfgang, and C. D. Roover, "A general method for rendering static analyses for diverse concurrency models modular," *Journal of Systems and Software*, vol. 147, pp. 17-45, 2019.
- [3] E. M. Jebri, A. T. Imam and M. Al-Fayuomi, "An Algorithmic Approach to Extract Actions and Actors (AAEAA)," in *Proceedings of the International Conference on Geoinformatics and Data Analysis*, Prague, Czech, 2018.
- [4] H. A. Nassar, A. Alhroob and A. T. Imam, "An Algorithmic Approach for Sketching Sequence Diagram (AASSD)," in *Proceedings of the International Conference on Advances in Image Processing*, Bangkok, Thailand, 2017.
- [5] I. Sommerville, *Software Engineering*, 10th ed., Essex, England: Pearson, 2015.
- [6] R. S. Pressman and B. R. Maxim, *Software Engineering: A Practitioner's Approach*, 8/e, NY, USA: McGraw-Hill Global Education Holdings, LLC, 2015.
- [7] G. F. Luger, *Artificial Intelligence: Structures and Strategies for Complex Problem Solving*, 6th ed., Pearson, 2011.
- [8] A. Copestake, *Natural Language Processing: PartII Overview of Natural Language Processing (L90): PartIII/ACS*, Cambridge, 2017.
- [9] D. Jurafsky and J. H. Martin, *Speech and Language Processing*, vol. 3, London: Pearson London, 2018.
- [10] I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning*, Cambridge, MA: MIT Press, 2016.
- [11] A. Oleinik, "What are neural networks not good at? On artificial creativity," *Big Data & Society*, vol. 6, no. 1, pp. 1-13, 2019.
- [12] R. Goswami, *Selected Topics in Machine Learning*, Michigan, USA: Independently published, 2018.
- [13] B. Bayat, C. Krauss, A. Merceron and S. Arbanowski, "Supervised Speech Act Classification of Messages in German Online Discussions," in *The 29th AAAI International Florida AI Research Society Conference*, Florida, USA, 2016.
- [14] C. D. Manning, M. Surdeanu, J. Bauer, J. Finkel, S. J. Bethard, and D. McClosky, "The Stanford Core NLP Natural Language Processing Toolkit," in *The 52nd Annual Meeting of the Association for Computational Linguistics: System Demonstrations*, Baltimore, Maryland, USA, 2014.
- [15] T. A. S. Foundation, "Welcome to Apache OpenNLP," 2018. [Online]. Available: <https://opennlp.apache.org/>.
- [16] V. Karkaletsis, P. Fragkou, G. Petasis, and E. Iosif, "Ontology Based Information Extraction from Text," in *Knowledge-Driven Multimedia Information Extraction and Ontology Evolution*, Berlin, Heidelberg, Springer, 2011, pp. 89-109.
- [17] J. Li, A. Sun, J. Han and C. Li, "A Survey on Deep Learning for Named Entity Recognition," *IEEE Transactions on Knowledge and Data Engineering*, p. Early Access Article, 2020.
- [18] P. Groth, M. Lauruhn, A. Scerri and R. D. Jr, "Open Information Extraction on Scientific Text: An Evaluation," in *The 27th International Conference on Computational Linguistics*, Santa Fe, New Mexico, USA, 2018.
- [19] M. Banko, M. J. Cafarella, S. Soderland, M. Broadhead and O. Etzioni, "Open Information Extraction from the Web," in *The 20th international joint conference on Artificial intelligence*, Hyderabad, India, 2017.
- [20] N. Indurkha and F. J. Damerau, *Handbook of Natural Language Processing*, London, U.K: Chapman & Hall, 2010.
- [21] M. Mohanan and P. Samuel, "Software Requirement Elicitation Using Natural Language Processing," in *Innovations in Bio-Inspired Computing and Applications*. Advances in Intelligent Systems and Computing, vol. 424, Cham , Springer, 2016, pp. 197-208.
- [22] D. K. Deeptimahanti and M. A. Babar, "An Automated Tool for Generating UML Models from Natural Language Requirements," in *International Conference on Automated Software Engineering*, Auckland, New Zealand, New Zealand, 2009.
- [23] T. H. Nguyen, J. Grundy, and M. Almorisy, "Rule-Based Extraction of Goal-Use Case Models from Text," in *10th Joint Meeting on Foundations of Software Engineering*, Bergamo, Italy, 2015.
- [24] R. Robu and S. Holban, "A Genetic Algorithm for Classification," in *International Conference on Computers and computing*, Canary Islands, Spain, 2011.
- [25] M. Junczys-Dowmunt, "A Genetic Programming Experiment in Natural Language Grammar Engineering," in *15th International Conference on Text, Speech and Dialogue*, Brno, Czech Republic, 2012.
- [26] P. More and R. Phalnikar, "Generating UML Diagrams from Natural Language Specifications," *International Journal of Applied Information Systems*, vol. 1, no. 8, pp. 19-23, 2012.
- [27] N. Arman and S. Jabbarin, "Generating Use Case Models from Arabic User Requirements in a Semiautomated Approach Using a Natural Language Processing Tool," *Journal of Intelligent Systems*, vol. 24, no. 2, pp. 277-286, 2015.
- [28] M. Murtaza, J. H. Shah, A. Azeem, W. Nisar, and M. Masood, "Structured Language Requirement Elicitation Using Case Base Reasoning," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 6, pp. 4393-4398, 2013.
- [29] R. Sharma, P. K. Srivastava, and K. K. Biswas, "From Natural Language Requirements to UMLClass Diagrams," in *IEEE Second International Workshop on Artificial Intelligence for Requirements Engineering (AIRE)*, Ottawa, ON, Canada, 2015.
- [30] S. Gulia and T. Choudhury, "An Efficient Automated Design to Generate UML Diagram from Natural Language Specifications," in *6th International Conference - Cloud System and Big Data Engineering (Confluence)*, Noida, India, 2016.
- [31] W. Wan, H. Cheong, W. Li, Y. Zeng, and F. Iorio, "Automated Transformation of Design Text ROM Diagram into SysML Models," *Advanced Engineering Informatics*, vol. 30, no. 3, pp. 585-603, 2016.
- [32] A. Al-Hroob, A. T. Imam and R. Al-Heisa, "The Use of Artificial Neural Networks for Extracting Actions and Actors from Requirements Document," *Information and Software Technology*, vol. 101, pp. 1-15, 2018.
- [33] T. Eftimov, B. K. Seljak, and P. Korošec, "A rule-based named-entity recognition method for knowledge extraction of evidence-based dietary recommendations," *PLOS ONE*, vol. 12, no. 6, pp. 1-32, 2017.
- [34] L. M. Berk, *English Syntax: From Word to Discourse*, NY, USA: Oxford University Press, 1999, p. 315.
- [35] T. E. Payne, "Summary of Semantic Roles and Grammatical Relations," 2007. [Online]. Available: <https://pages.uoregon.edu/tpayne/EG595/HO-Srs-and-GRs.pdf>.
- [36] V. Punyakanok, D. Roth and W.-t. Yih, "The importance of syntactic parsing and inference in semantic role labeling," *Computational Linguistics*, vol. 34, pp. 257--287, 2008.
- [37] C. J. Fillmore, "Types of Lexical Information," in *Semantics: an interdisciplinary reader in philosophy, linguistics and psychology*, London, U.K, Cambridge University Press, 1971, pp. 370 - 392.
- [38] A. T. Imam and A. J. Alnsour, "The Use of Natural Language Processing Approach for Converting Pseudo Code to C# Code," *Journal of Intelligent Systems*, vol. 28, no. 3, p. 362, 2019.
- [39] T. Osborne and T. Gross, "Constructions are catenae: Construction Grammar meets Dependency Grammar," *Cognitive Linguistics*, vol. 23, no. 1, p. 163-214, 2012.
- [40] M.-C. d. Marneffe, T. Dozat, N. Silveira, K. Haverinen, F. Ginter, J. Nivre and C. D. Manning, "Universal Stanford dependencies: A cross-linguistic typology," in *Ninth International Conference on Language Resources and Evaluation*, Reykjavik, Iceland, 2014.
- [41] Universaldependencies.org, "Universal Dependencies," 2017. [Online]. Available: <https://universaldependencies.org>.

- [42] D. o. C. S. Lund University, "Try the semantic role labeler," 2019. [Online]. Available: <http://barbar.cs.lth.se:8081/>.
- [43] J. Hajič, M. Ciaramita, R. Johansson, D. Kawahara, M. A. Martí, L. Márquez, A. Meyers, J. Nivre, S. Padó, J. Štěpánek, P. Straňák, M. Surdeanu, N. Xue and Y. Zhang, "The CoNLL-2009 Shared Task: Syntactic and Semantic Dependencies in Multiple Languages," in CoNLL '09 Proceedings of the Thirteenth Conference on Computational Natural Language Learning: Shared Task, Boulder, Colorado, 2009.
- [44] K. Hacioglu, "Semantic Role Labeling Using Dependency Trees," in 20th international conference on Computational Linguistics, Geneva, Switzerland, 2004.
- [45] R. Johansson and P. Nugues, "Extended Constituent-to-Dependency Conversion for English," in The 16th Nordic Conference of Computational Linguistics (NODALIDA 2007), Tartu, Estonia, 2007.
- [46] S. Tong and D. Koller, "Support Vector Machine Active Learning with Applications to Text Classification," *Journal of Machine Learning Research*, vol. 2, no. 1, pp. 45-66, 2001.
- [47] C. J. C. Burges, "A Tutorial on Support Vector Machines for Pattern Recognition," *Data Mining and Knowledge Discovery*, vol. 2, no. 2, p. 121-167, 1998.
- [48] M. Fern, D. Delgado, E. Cernadas, S. Barro and D. Amorim, "Do we Need Hundreds of Classifiers to Solve Real World Classification Problems?," *Journal of Machine Learning Research*, vol. 15, no. 1, pp. 3133-3181, 2014.
- [49] G. Holmes, A. Donkin and I. H. Witten, "Weka: A machine learning workbench," in Second Australia and New Zealand Conference on Intelligent Information Systems, Brisbane, Australia, 1994.
- [50] S. Keerthi, S. Shevade, C. Bhattacharyya and K. Murthy, "Improvements to Platt's SMO Algorithm for SVM Classifier Design.," *Neural Computation*, vol. 13, no. 3, pp. 637-649, 2001.
- [51] Nabble, "Explanation of SMO Parameters?," 2019. [Online]. Available: <http://weka.8497.n7.nabble.com/Explanation-of-SMO-Parameters-td21768.html>.
- [52] R. S. R. Boddu and S. Kalyanapu, *Waikato Environment for Knowledge Analysis: Data Mining Tool*, Mauritius: LAP LAMBERT Academic Publishing, 2019, pp. 87-112.
- [53] C. W. Ahn and R. Ramakrishna, "A Genetic Algorithm for Shortest Path Routing Problem and The Sizing of Populations," *IEEE Transactions on Evolutionary Computation*, vol. 6, pp. 566 - 579, 2002.
- [54] Kohavi and Provost, "The Case Against Accuracy Estimation for Comparing Introduction Algorithm," in ICML '98 Proceedings of the Fifteenth International Conference on Machine Learning, 1998.
- [55] D. L. Olson and D. Delen, *Advanced Data Mining Techniques*, 1st ed., Springer, 2008, p. 38.
- [56] A. T. Imam, A. J. Al-Nsour and A. Al-Hroob, "The Definition of Intelligent Computer Aided Software Engineering (I-CASE) Tools," *Journal of Information Engineering and Applications*, vol. 5, no. 1, pp. 47-56, 2015.
- [57] A. T. Imam, "Relative-Fuzzy: A Novel Approach for Handling Complex Ambiguity for Software Engineering of Data Mining Models," De Montfort University, Leicester, UK, 2010.

# Artificial Intelligence: Machine Translation Accuracy in Translating French-Indonesian Culinary Texts

Muhammad Hasyim<sup>1</sup>  
Hasanuddin University  
French Literature Study Program  
Cultural Science Faculty, Makassar, Indonesia

Firman Saleh<sup>2</sup>  
Hasanuddin University  
Local Language Study Program  
Cultural Science Faculty, Makassar, Indonesia

Rudy Yusuf<sup>3</sup>  
Hasanuddin University  
Japanese Language Study Program  
Cultural Science Faculty, Makassar, Indonesia

Asriani Abbas<sup>4</sup>  
Hasanuddin University  
Indonesian Literature Study Program  
Cultural Science Faculty, Makassar, Indonesia

**Abstract**—The use of machine translation as artificial intelligence (AI) keeps increasing and the world's most popular translation tool is Google Translate (GT). This tool is not merely used for the benefits of learning and obtaining information from foreign languages through translation but has also been used as a medium of interaction and communication in hospitals, airports and shopping centers. This paper aims to explore machine translation accuracy in translating French-Indonesian culinary texts (recipes). The samples of culinary text were taken from the internet. The research results show that the semiotic model of machine translation in GT is the translation from the signifier (forms) of the source language to the signifier (forms) of the target language by emphasizing the equivalence of the concept (signified) of the source language and the target language. GT aids to translate the existing French-Indonesian culinary text concepts through words, phrases and sentences. A problem encountered in machine translation for culinary texts is a cultural equivalence. GT machine translation cannot accurately identify the cultural context of the source language and the target language, so the results are in the form of a literal translation. However, the accuracy of GT can be improved by refining the translation of cultural equivalents through words, phrases and sentences from one language to another.

**Keywords**—Machine translation; Google translation; accuracy; culinary texts; artificial intelligence

## I. INTRODUCTION

The information age has changed the social order of the world. Its presence allows global society to be able to interconnect countries with different language backgrounds. Language barriers are not a challenge in interacting and communicating between individuals and groups. Translation applications help people communicate easily. This can be seen in communication through social media, for example, Facebook and Twitter.

Sergey Brin, the co-founder of Google, received a fan letter from Korea. Brin was very curious about the contents of the letter which was written in Korean. But Brin doesn't speak. He ran the message through GT that he had. The letter was translated into, "the sliced raw fish shoes it wishes. Google

green union thing" [1]. From that moment on, he realized the importance of machine translation (applications) which aids people to communicate with each other from various parts of the world. Brin also developed a GT tool that can not only be used in the Windows version but also in the Android version.

With the advancement of translation applications, machine translation can match translation done by humans. Based on a survey conducted by Google in 2016, GT can perform translations in various levels of accuracy that are equivalent to human translators, for example from Spanish, Chinese and French to English and vice versa GT is believed to have very high accuracy results in translating English to Spanish, French, Chinese, or vice versa from these respective languages to English. Also, Google asked bilingual people to compare the output of Google machine translation with GMNT (Google Neural Machine Translation) technology and human translation. The sentences used for translation example were taken randomly from Wikipedia or news article. On a scale of 0 to 6, the GMNT machine-scored an average of 5.43 or only a slight difference from the human translation score of 5.55. Google concluded that the new version of Google translation (GMNT) is believed to be 64 to 87 per cent more accurate than the previous engine (PBMT). It means that the new version of GT has a high level of accuracy that matches the human reference translation [2].

With translation applications capabilities that can match human translation, the use of translation applications (machine) has increased. Based on Google data, 600 million people are using the GT application. With 90 per cent of users are outside the US USA [3]. A study showed that because limited English language proficiency (LEP) is common in emergency patients in Spanish hospitals and many hospitals do not have formal written translations, many providers use automatic translation software, such as GT. A recent study utilizing professional translators to evaluate machine translation outputs in Spanish and Chinese showed that GT has a very high level of accuracy. Google Translate allows hospital staff and patients to communicate with each other [4].

Indonesia itself is the top ten most countries users of GT in the world. The growth of GT users in Indonesia is considered very high. Each year, the growth of these machine translation users in Indonesia reaches more than 300 per cent on mobile devices and 94 per cent on desktop web. Indonesians use GT to read articles or chat [5]. In college learning activities, GT is used as a learning medium for translating foreign news items [6]. Although use of Google translate in Indonesia has been widely used as a communication medium, there has not been much research on the accuracy of the outputs of GT from Indonesia into English and so on. This paper will examine the accuracy of GT in translating French-Indonesian culinary texts (recipes) from a semiotic perspective.

There has been many studies on translation, among others, translation accuracy using machine translation [7]; [4]; [8], times in novels translation [9], equivalence in translation [10], ideology in translation [11] and [12], gender-specific translation [13], metaphor translation [14] and errors in translation [15].

The main issue that has always been the focus of translation study is the transfer of messages (meaning) from the source language to the target language. The message is information conveyed from the source language and transferred to another language. The readers in the source language have the same understanding of the information conveyed to the target language readers. Semiotically, the message (information) is a signifier, and the meaning of the message generated by the message is a sign [16]. Information messages are signs formed from the relationship between the signified and signifier physically generated (media) by the sender (a person, author or device) to the recipient.

The role of the translator (human) is to transfer information messages to the target language acquired by the translator. The role of the translator is how to make the target language reader understand the information message being transferred. The recipient (reader) gets direct information (message) conveyed by the translator. Whatever is conveyed by the translator as the receiver and the sender will be accepted by the reader as the receiver. This process is called interlingual translation [17]. The readers can understand information messages based on the meaning of the message from the translator and readers do not have direct communication with the sender (author) of the source language.

In the context of machine translation with information technology, the translator in question is Artificial Intelligence (AI) which refers to a simulation of human intelligence in a machine programmed to think like humans and imitate their actions. Machine translation or translation applications are AI which has messages as translators that replace humans who have the role of diverting information messages from the source language to various other languages that have been provided by machine translators [8]. The machine translator already has a database of vocabulary and grammar from one language to another. Humans as application users run translation machines by entering information messages as the source language and translated into the target language.

The issue that will be discussed in this paper is how the process of machine translation from one source language to another. The author will discuss it using a semiotic perspective. Questions related to machine translation are how accurate is the machine translator from French to Indonesian. The analytical data is French culinary texts (recipes) retrieved from the internet.

## II. MACHINE TRANSLATION AND SEMIOTICS

The translation is an activity of transferring information messages from the source language to the target language. The focus of translation activities is to transfer information messages to another language acquired by the recipient (reader). The main objective of translation activities is how the target language reader understands the message being transferred. Catford [18] defines translation as the process of changing text from one language to another. Catford emphasizes translation activities on text transfer. Nida and Taber [19] states, "Translating consist in producing in the receptor language the closest natural equivalent to the message of the source language, first in meaning and secondly in style". This definition focuses on how to find the closest equivalent of the receiving language to the source language. Larson [20] defines translation by re-expressing the same meaning using lexicons and grammatical structures that are appropriate in the target language and cultural context. Larson emphasized translation activities based on meaning. According to him, translation is a transfer of meaning from the source language to the target language. Meaning is more important because it cannot be changed, while form may change.

Machine translation (MT) is a translation activity using computer software to translate verbal text (information messages) from one language to another. MT is a branch of computational linguistics that studies the use of computer software in translation activities. At a basic level, MT performs the simple substitution of words, phrases and grammar from one language to another. Online-based machine translation systems use machine learning technologies to translate large amounts of text to and from supported languages. The MT service translates text from the source language into different languages.

In the semiotic perspective, information messages conveyed in verbal language are symbols, which are built on the elements of signifier and signified. A signifier is a physical record of an information message in certain media and a signified is a concept generated by a signifier (a physical record of an information message). The semiotic translation is a significant transfer activity [21]. MT is an activity of transferring signs (verbal language). A signifier is a physical record of an information message in the source language and a signified is the concept of a physical record of an information message. The transfer activity in MT is to transfer the concept (signified) of the physical record of information messages from the source language into a signifier, a physical record of information messages into the target language. Signifier in the target language of the concept transfer activity as signifier from the source language. So, the concept of an information

message as a signified in the source language has the same concept as a signified in the target language.

The recipients (readers) get direct information messages conveyed by MT. Anything that the machine translator transferred will be received by the reader as an information message in the target language. The concept of information messages as signified of the source language is transferred by using the target language signifier. Concepts that are transferred by machine translators semiotically use other language codes as a signifier.

The concept (signified) has universal properties in all languages. The signifier differentiates between one language and another by using the same concept. In a semiotic perspective, translation emphasizes the signified (concept). When we refer to the concept, something that is signified, then the concept of 'holiness', the signifier in English is 'horse', in Indonesian it is 'horse', and in French, 'cheval' and so on. The translation is the transfer of signifier from the source language to the original language based on the concept that is signified.

### III. RESEARCH METHOD

The study used qualitatively. The research method used descriptive using qualitative analysis [22]. Semiotics is the theoretical framework for answering research problems. The author uses a semiotic model to examine the accuracy of MT (Google translate). The research object is culinary texts (recipes) taken from online media in French and GT is used to translate French text into Indonesian. The sample was culinary texts (cooking recipes). The writer chose one recipe text (pumpkin soup) which familiar in Indonesian culture. Thus, the primary data is the French culinary text retrieved from the internet and the translated text using GT.

The online text data analysis procedure is entering primary data (culinary text) in the source text column (option in French). Then, the writer chose Indonesian as the target language. After the source text data is in Google translate the application, then the translate button was pressed. The author made a table of the translation outputs consisting of two columns. The first column is the source text and the second column is the translated text. The table of translation output is used as the main data for analysis.

A semiotic model (signifier-signified-signifier) was used to assess the accuracy of translation with GT. The author analyzes the source text signifier and target text signifier and analyzes the concepts of equivalence (signified) in the target language (Indonesian).

### IV. RESULTS AND DISCUSSION

#### A. Culinary Text Translation (Food Recipe)

Source Texte (French): Soupe au potiron (Signifier/form)

Ingrédients

- 1 kg de potiron
- 300 g de carotte
- 200 g d'oignon
- 200 g de poireau

- Beurre
- 3 gousses d'ail
- 1 bouquet garni
- 40 cl de crème fraîche
- Sel

Préparation

Temps Total: 1h25

Préparation: 25 min

Cuisson: 1 h

1) Tailler les légumes en gros dés. Les faire suer dans le beurre.

2) Mouiller avec 1,5 l d'eau. Ajouter l'ail écrasé et le bouquet garni. Cuire 1 heure.

3) Passer au moulin à légume ou au mixer. Ajouter la crème fraîche, et servir chaud.

Target Texte (Indonesien): Sup Labu (Pumpkin soup/signifier/form)

Bahan (Ingredients):

- 1 kg labu (1 kg of pumpkin)
- 300 g wortel (300 g of carrot)
- 200 g bawang bombay (200 g of onion)
- 200 g daun bawang (200 g of leek)
- Mentega (butter)
- 3 siung bawang putih (3 cloves of garlic)
- 1 karangan bunga garni (1 bouquet garni)
- 40 cl krim segar (1 bouquet garni)
- Garam (salt)

Meaning-Signified (concept):

1) In the text title section, the name of the dish can be identified as the translation outputs from Google Translate have the same equivalent in the Indonesian text. This means that Google translate uses the same concept (marker) for French and Indonesian.

2) Likewise, the ingredients translation for making pumpkin soup. Google Translate can translate using equivalents in Indonesian. Thus, Google translate uses the concept as the same marker in French as the source language and Indonesian as the target language.

3) The same thing goes for translating pumpkin soup cooking preparations. Google translate can divert informational messages with the same equivalence in Indonesian as the target language. Google translate can translate concepts (markers) to produce meanings that are equivalent to the source language.

**B. Google Translate: Translation Equivalent**

Translation equivalent is the equivalence of source text with target text [10]. Meanwhile, Liu argues [23] that equivalence is a relationship between words or phrases from two or more languages that have the same meaning. The definition of equivalence can be strengthened by Russell's statement (1959) that no one can understand the word 'cheese' unless he has non-linguistic knowledge about cheese [24]. Russel's opinion shows that the word 'cheese' as a marker in English cannot be understood if it is not associated with cheese as an external object, which then becomes a sign in one's mind. People cannot understand a word as a signifier, the word 'cheese' if the word is not associated with something signified, Russel calls it the term non-linguistic acquaintance. So, something signified (concept) is outside the sign itself (signifier). Jacobson [25] argues that there is no sign (signatum) without a signifier (signum).

Catford [18] provides a different explanation of equivalence. According to him, translation equivalent activities are rarely found in the target language. One factor is the problem of grammatical differences, for example, demonstrative translation. The source language and target language can have equivalences when they are exchanged in certain situations. For example, the English demonstrative word, 'this' (singular), 'this book' and the plural "these", these books are translated in Indonesian into the demonstrative word 'ini' (this) which means singular and Indonesian does not acknowledge plural demonstrative words. The plural demonstrative equivalence can be exchanged in other situations using the plural noun, namely 'these books' (these books). In Indonesian, the plural in demonstrative is the noun, while in English, the word demonstrative and noun. Concerning Catford's opinion, translation equivalent is a transfer not based on meaning but based on the exchange of situations from the source language to the target language.

Equivalence in MT (GT) emphasizes the concept (signified) in the source language and target language. The translation process is the transfer of the form (signifier) from the source language to the form (signifier) of the target language using the same concept as the equivalent. So, the translation equivalent model in culinary texts is signifier 1 (source language) - signified - signifier 2 (target language). GT can translate words, phrases and sentences denotatively which emphasizes the equivalence of concepts between the source language and the target language. We can take the example in Table I from the text of the recipe for pumpkin soup (French to Indonesian).

Likewise, the conceptual equivalence of sentences. As an example, in the culinary text. GT translates sentences from the source language to the target language by emphasizing the equivalence of concepts (signified).

The equivalence of concept in sentences on Google translate:

1) Tailler les légumes en gros dés. Les faire suer dans le beurre. \ Potong sayuran menjadi kubus besar. Keringkan dengan mentega (Cut the vegetables into large cubes. Sweat them in the butter).

2) Mouiller avec 1,5 l d'eau. Ajouter l'ail écrasé et le bouquet garni. Cuire 1 heure. Basahi dengan 1,5 liter air. Tambahkan bawang putih yang dihancurkan dan karangan bunga. Masak selama 1 jam. (Wet with 1.5 l of water. Add the crushed garlic and the bouquet garni. Cook for 1 hour).

3) Passer au moulin à légume ou au mixer. Ajouter la crème fraîche, et servir chaud. Lewatkan mesin penggiling sayuran atau blender. Tambahkan krim segar dan sajikan panas (Pass through a vegetable mill or a blender. Add the crème fraîche, and serve hot).

The semiotic model in the translation of equivalence of concepts in machine translation (GT) is Signifier (form) 1 in the source language - Signified (concept) - Signifier (form) 2 in the target language. GT transfers the form from the source language to the target language with the same concept (signified) as the conceptual equivalent.

TABLE I. EQUIVALENCE OF CONCEPTS IN GOOGLE TRANSLATE

Source text (French) Signifier (form)	Target text (Indonesian) Signifier (form)
<p>SOUPE AU POTIRON</p> <ul style="list-style-type: none"> <li>• 1 kg de potiron</li> <li>• 300 g de carotte</li> <li>• 200 g d'oignon</li> <li>• 200 g de poireau</li> <li>• Beurre</li> <li>• 3 gousses d'ail</li> <li>• 1 bouquet garni</li> <li>• 40 cl de crème fraîche</li> <li>• Sel</li> </ul>	<p>Sup Labu (Pumpkin soup)</p> <ul style="list-style-type: none"> <li>- 1 kg labu (1 kg of pumpkin)</li> <li>- 300 g wortel (300 g of carrot)</li> <li>- 200 g bawang bombay (200 g of onion)</li> <li>- 200 g daun bawang (200 g of leek)</li> <li>- Mentega (butter)</li> <li>- 3 siung bawang putih (3 cloves of garlic)</li> <li>- 1 karangan bunga garni (1 bouquet garni)</li> <li>- 40 cl krim segar (1 bouquet garni)</li> <li>- Garam (salt)</li> </ul>

**C. The Issue of Cultural Translation in Machine Translation (Google Translate)**

The issue found in MT (GT) is a cultural equivalence. Can GT know the culture of the source language and target language culture and how to differentiate the translation of words, phrases, sentences and culture? Previously, it has been explained that GT can translate words, phrases and sentences with the equivalent concept and denotation meaning. This means that the GT application has compiled a database of words, phrases and sentence grammar in the GT electronic dictionary. The issue found in machine translation is cultural.

One of the definitions of culture that always becomes an issue in translation is the way of life, whose manifestation is seen in the form of behaviour and the results are visible materially, which is obtained through the process of habituation and learning in society and passed from generation to generation. Hoed [9] states that culture is unique to certain communities and its mastery is through a process of habituation and learning from generation to generation. Because it is unique to society, no culture is the same. The concept of translation in culture is the transfer of cultural equivalents from the source language into the target language. An example of an equivalent French culinary culture is the word 'cuillère à café' (coffee spoon) which has the Indonesian equivalent of 'teaspoon'. French people have the habit of using

a small spoon that is used to stir coffee drinks with the term 'cuillère à café'. Meanwhile, Indonesian people have the habit of using the word 'teaspoon' to stir tea, coffee, etc. French culture acknowledges the term cuillère à café for a small spoon that is usually used for drinking (coffee) and Indonesian culture acknowledges the term teaspoon used for tea drinks.

MT such as GT cannot translate cultural equivalents from the source language to the target language. In the text of French recipes above, there are several cases of cultural translation. For example, the sentences (1) mouiller avec 1,5 l d'eau (wet with 1.5 l of water) and (2) ajouter le bouquet garni (add the bouquet garni), (3) passer au moulin à légume ou au mixer (pass through a vegetable mill or a blender). Sentence 1 translated into Indonesian becomes wet with 1.5 litres of water. The context of the sentence referred to in Indonesian in the sentence is to pour 1.5 litres into the container (pour water into ....) which already contains pumpkin soup ingredients. The word mouiller according to the dictionary means to wet (wet). But in the context of this sentence, it is put, add water into the container. Indonesian culture (point of view) to put water in a container, for example, a pot is to use the word pour, add instead of wetting for the context of adding water in a container. Sentence 2 ajouter le bouquet garni translates to add a wreath. The general term used in Indonesian culture in a culinary context is the word bouquet garni (the name for several spices tied together to add flavour to the broth). So, sentence 2 should be translated to add bouquet garni (add the bouquet garni). The term bouquet garni was absorbed from English and became a term in the culinary field in Indonesian. Sentence 3 Passer au moulin à légume ou au mixer translates to skip through a vegetable mill or a blender. The context in Indonesian culture in the sentence is to mix the ingredients into a vegetable grinder or mixer (mix the ingredients into a vegetable grinder or mixer). The word passer (verb) means to miss. However, the Indonesian cultural context referred to in this sentence is mixing pumpkin soup ingredients into a mixer. Indonesian culture does not use the term passing the ingredients into a mixer, but instead mix the ingredients into a mixer (mix the ingredients into a vegetable grinder or mixer).

The different (cultural) perspective between the two languages (source and target) cannot be acknowledged by MT in culinary texts (recipes). MT has not been able to completely transfer the cultural equivalence from the source language to the target language. Thus, in the perspective of semiotics, the signifier is a form of the source language and signified is a cultural meaning or concept from the source language to the target language. In translation activities, the first signifier as a source is changed to the second signifier as the target language (Indonesian) and the signified (concept) is a cultural equivalence.

GT is a translation tool that can certainly add to the cultural equivalence database of the various translation cases found. By updating translation engine databases such as GT which can include additional vocabulary, phrases, grammar and cultural equivalences, machine translators can improve the accuracy of translation from one language to another. Along with the increasing users of translation machines like GT, GT is not merely used as a translation application but has become a medium of communication between individuals, groups and

organizations. Various machine translators have been provided in various public facilities, such as hospitals for communication services between hospital staff and patients, supermarkets, airports, etc.

## V. CONCLUSION

Online machine translator, GT has become a translator application used all over the world. This shows the enormous benefits of this translation application. The function of the machine translator GT is not merely a translation application to obtain information from foreign languages, but this application has served as a medium of interaction and communication in public facilities, for example in hospitals, airports and shopping centres. The conclusion of the research on the accuracy of GT as machine translation with a semiotic perspective on French-Indonesian culinary texts in this paper is that GT uses the semiotic model of machine translation from the signifier (form) of the source language to the signifier (form) of the target language by emphasizing the equivalence of the concept (signified) source language and target language. GT can accurately translate the corresponding French-Indonesian culinary text concepts using words, phrases and sentences. The machine translator GT has encountered problems with translating cultural equivalents in French and Indonesian culinary texts. GT has not been able to accurately identify the cultural context of the source language and target language, so the results are in the form of a literal translation.

## REFERENCES

- [1] Zainuddin Ahmad. Kelahiran Mesin Penerjemah dan Masa Depan Google Translate, in <https://tirto.id/cxS2>, 2017.
- [2] Widiatanto, Yoga Hastyadi. Mesin Penerjemah Makin Mirip Manusia in <https://tekno.kompas.com/>, 2016.
- [3] Pertiwi, W. K. 2018. Pengguna Google Translate Melonjak Selama Piala Dunia 2018" in <https://www.kompas.com/>, 2018.
- [4] Kreger, V., Aintablian, H., Diamond, L., Taira, R.B. Google Translate as a Tool for Emergency Department Discharge Instructions? Not So Fast! *Annals of Emergency Medicine*, 74, (4), Supplement, S5-S6, 2019.
- [5] Jumatulaini. Analisis Keakuratan Hasil Penerjemahan Google Translate dengan Menggunakan Metode Back Translation. *Alsuniyat: Jurnal Penelitian Bahasa, Sastra, dan Budaya Arab*, 3 (1), 2020, pp.77-87.
- [6] Al-Ayubi, M. Shalehuddin. Utilization Of Google Translation As A Learning Medium At Foreign News Text Translation. *Jurnal Teknodik*, 21 (2), 2017, pp.155-166.
- [7] Groves, Michael, Mundt, Klaus. Friend or foe? Google Translate in language for academic purposes. *English for Specific Purposes*, 37, 2015, pp.112-121.
- [8] Stapleton, P., Ka Kin, B.L. Assessing the accuracy and teachers' impressions of GoogleTranslate: A study of primary L2 writers in Hong Kong. *English for Specific Purposes*, 56, 2019, pp.18-34.
- [9] Hoed, Benny. Kala dalam Novel: Fungsi dan Penerjemahannya. sebuah kajian tentang penerjemahan Perancis-Indonesia. Yogyakarta, Gadjah Mada University Press, 1992.
- [10] Panou, Despoina. Equivalence in Translation Theories: A Critical Evaluation. *Theory and Practice in Language Studies*. 3(1), 2013, pp.1-6.
- [11] Valerio, Anna. Translation and ideology: a critical reading. *Procedia - Social and Behavioral Sciences*. 70, 2013. pp.986 – 996.
- [12] Kuswarini, Prasuri. A Shift of Ideology in the Translation of Karl May's *Work Und Friede auf Erden!* into the Indonesian Language. *International Journal of Comparative Literature & Translation Studies*. 2 (3), 2014, pp.42-49.
- [13] Hernández, Daniel Gallego, Igualada, Miguel Tolosa et Masseur, Paola. Traducción de géneros económicos de l'espagnol vers l'allemand, le

- français et l'anglais et vice-versa. Enquête auprès d'entreprises exportatrices. *Meta*.63 (1), 2018, pp.30–46.
- [14] Elena, Burmakova & Marugina, I. Nadezda. Cognitive Approach to Metaphor Translation in Literary Discourse. *Procedia - Social and Behavioral Sciences*. 154, 2014, pp.527-533.
- [15] Wongranu, Pattanapong. Errors in translation made by English major students: A study on types and causes. *Kasetsart Journal of Social Sciences*. 38, 2017, pp.117–122.
- [16] Danesi, Marcel. (2010). *Pengantar Memahami Semiotika Media*. Jogjakarta, Jalasutra, 2010.
- [17] Hasyim, M., Nursidah,, Hasjim, M. Online advertising: How the consumer goods speaks to women. *Opcion*, 35 (89), 2019, pp.826–845.
- [18] Catford, J.C. *A Linguistic Theory of Translation*. Oxford University Press, 1978.
- [19] Nida E.A., & Taber C.R. *The theory and practice of translation*. Leiden, E.J. Brill, 1982.
- [20] Larson, M.L. *Meaning Based Translation: A Guide to Cross-Language Equivalence*. Lanham & London, University Press of Amerika, 1989.
- [21] Hasyim, M., Arafah, B., Kuswarini, P. The new Toraja destination: Adding value 'Toraja coffee' of the sustainable tourism development. *IOP Conference Series: Earth and Environmental Science*, 2020, 575(1), 012072, 2020.
- [22] Teng, M.B.A., Hasyim, M. The philosophy of kajaolaliddong: A basic pattern of life and culture in bugis and makassar. *Systematic Reviews in Pharmacy*, 11(12), 2020, pp.1548–1552.
- [23] Liu, Lixiang. Partial equivalences in bilingual dictionaries: Classification, causes and compensations. *Lingua*, 214, 2018, pp.11–27.
- [24] Russell, Bertrand. *Logical positivism*. *Revue Internationale de Philosophie*, 1959.
- [25] Jakobson, Roman. On linguistic aspects of translation. In: Venuti, L. (Ed.), *The Translation Studies Reader*. 3rd ed. Routledge, London/New York, 2012, pp. 126–131.

# A Generic Approach for Allocating Movement Permits During/Outside Curfew Period during COVID-19

Yaser Chaaban

Department of Computer and Information Sciences  
Faculty of Sciences and Arts, Taibah University, AIUla Branch  
Al-Madinah, Saudi Arabia

**Abstract**—During the coronavirus (COVID-19) pandemic, different exciting concepts around solutions, technical components, smartphone applications, and novel wireless services emerged, which were needed in order to adjust to the new lifestyle standards. In this context, social distancing was imposed to prevent or decrease further transmission of COVID-19. In other words, research results have shown that slowing the spread of COVID-19 is the most efficient way to save people's lives and relieve the burden on health-care systems. This social distancing can be tracked using cell phone movement/data. This paper presents a new approach/algorithm for allocating and optimizing/adapting the movement permits during/outside curfew periods inside workplaces, buildings, companies and institutions. This approach is an effective tool to reduce the spread of COVID-19 by promoting health safety during the pandemic, especially in places where social distancing can be difficult. Consequently, this paper presents a technological solution to automate the process of distributing movement permits in workplaces. The research results showed that the proposed strategy of social distancing inside buildings is effective enough to flatten the curve. Furthermore, health authorities do not have to mandate stay-at-home orders to slow the spread of COVID-19. Consequently, this paper introduces a solution for the resource sharing problem (resource allocation problem), where multiple agents (people or robots) of a system move reliably in their environment. The biggest concern of these agents is to avoid collisions (infections). As a result, the experiments performed in this paper showed the high performance of the designed algorithm complying with COVID-19 social distancing regulations.

**Keywords**—COVID-19 pandemic; social distancing; resource allocation problem; movement permits

## I. INTRODUCTION

Nowadays, scientific research is announcing the opening of the application period around the world for the institutional funding initiative of strategic studies. Many universities or organizations have new priorities and research topics so proposals must align with the coronavirus (COVID-19) pandemic topic. In all instances, strategic research was approved by ministries for research and innovation, ministries of high education, and organizations such as the World Health Organization (WHO) [1]. Simultaneously, the future of distance education and E-Learning became more interesting and necessary during the COVID-19 pandemic. Furthermore,

digital technologies in health services, new techniques in infectious diseases management, comprehensive approaches for COVID-19 prevention, screening and management, and state-of-the-art diagnostics of COVID-19 became critical enablers for our society. All these topics represent current challenges in population health. In this context, many brands, organizations, and governments are trying to find digital platforms such as special websites, mobile-friendly websites, virtual reality, and smartphone applications to manage particularly the new lifestyle standard of COVID-19 [2].

Another idea related to the concept of "flatten the curve" [3] is the social distancing strategy. Social distancing also called "physical distancing", can be tracked using cell phone data or movement. This data is important to identify how many times was a certain region, area, or intersection walked on.

In essence, this paper focuses on designing a control algorithm for providing human agents inside workplaces with planned movement permits. This will enable agents to move safely in their shared environment during the COVID-19 pandemic. Accordingly, avoiding infections (collisions) and reducing journey times are needed by implementing a social distancing strategy.

This research paper is organized as follows: Section 2 provides a survey of related work concerning social distancing policies implemented in response to COVID-19. In Section 3, the roles of software applications developed during COVID-19 are discussed. Section 4 raises the question: Are technology solutions ready for life after COVID-19? After that the objectives of the proposed approach/algorithm will be briefly discussed in Section 5. Section 6 describes the scenario of this paper, where agents trying to move in a shared environment inside workplaces during COVID-19. Moreover, the new approach will be presented in Section 7, containing trajectory planning and the developed algorithm. Section 8 presents the evaluation of the proposed algorithm using two metrics. After that, Section 9 concludes this paper. Finally, the future work is explicated in Section 10.

## II. RELATED WORKS

As mentioned above, various projects and research topics are dealing with the COVID-19 pandemic around the world. In this section, it is concentrated on related works that focus on implementing a social distancing policy due to the COVID-19

pandemic. It is also worth mentioning here that some concepts, algorithms, or policies related to social distancing are relevant to this work. Another aspect that is of interest is the allocation of movement permits during COVID-19, particularly in those places where ensuring social distancing is difficult.

In honeybee systems, honeybees cannot practice any social distancing. However, they work together in very close spaces as a healthy community. Consequently, honeybees work together to fight diseases, whereas humans can learn how they can tackle the COVID-19 pandemic [4]. Furthermore, a beehive gives humanity important insights during pandemics, where all complex interactions are carried out in order to preserve a healthy life of groups within the beehive [5].

During the COVID-19 pandemic, the concept of "flattening the curve" became the most discussed and researched subject by governments and researchers. It is a public health concept reducing the spread of the COVID-19. Siobhan Roberts presented an interesting article towards flattening the COVID-19 curve. He showed that reducing the spread of the COVID-19 infection is as necessary as halting it [6]. Although the best goal would be to completely eradicate the pandemic, slowing it down is also extremely critical for managing COVID-19. In this context, the author presented some mitigation measures towards the COVID-19 pandemic, e.g., social distancing to keep the population apart in time and space, actual self-isolation and quarantine [6].

Another related work in this context was introduced by Jackson Ryan in [7]. The author discussed the relation between social distancing and the concept of "flatten the curve" during the COVID-19 pandemic. He mentioned that many medical experts recommended more stringent social distancing, restricting/canceling mass gatherings, suspending business for many companies in certain sectors, etc. This means that such recommendations would help to impose social distancing during an epidemic and consequently slowing the spread of disease [7].

In this regard, several projects dealing with contact tracing applications. In [8], a new survey of COVID-19 contact tracing applications was conducted by Nadeem Ahmed et al. These smartphone applications are used to trace all recent contacts of people that were newly identified as positive infected with COVID-19. The authors presented an overview of several proposed smartphone tracing application examples. Additionally, they mentioned some future research directions for designing such applications towards improving tracing, large adoption by individuals, and safety performance [8]. Based on those, centralized/ decentralized/hybrid approaches (system architectures) used for developing tracing applications of COVID-19 were discussed. Additionally, the survey reported the pros and cons of each architecture, diverse attack and protection models, different implementation complexity and operating costs [8].

A more detailed discussion of such applications will be given in the section "Software application roles and responsibilities".

Regarding the implementation of social distancing policies to prevent the COVID-19 pandemic, several approaches from the literature were pointed out. Interesting work was analyzed to study the benefits and also the costs in the case of enforcing social distancing with the aim to flatten the curve of COVID-19 [9]. Linda Thunström and others pointed out that using social distancing, on one hand, will help save lives during the pandemic. Moreover, on the other hand, social distancing leads to very high costs for society as a result of decreased economic activities. The authors used epidemiological and economic forecasting to analyze the benefit-cost of controlling COVID-19 [9].

Another related work in this context was introduced by Arnab Ghorai and others [10]. The authors suggested a digital solution that enforces a social distancing policy using the Deep Learning technique. This technique detects any violation of the imposed social distancing using a tolerated threshold (pre-defined limit on several participants). To achieve this observation, a CCTV camera was installed so that a video stream could be captured. Accordingly, detecting and tracking the humans' motions are carried out by utilizing the PoseNet model (a machine learning model) [10].

Furthermore, the University of Texas M. D. Anderson Cancer Center presented an article dealing with the implementation of social distancing policies [11]. The article showed the relation between practicing social distancing and sustained reduction in COVID-19 transmission. It is a significant study that includes 50 US states and 134 nations, where its result indicates that social distancing can be enforced as an effective public health tool [11].

In addition to these studies, Per Nilsen and others introduce a new framework for analyzing a social distancing policy implementation in the context of the battle against the COVID-19 [12]. This framework aims to merge knowledge from two fields, where elements from implementation science and policy research can be combined. Accordingly, the author suggested a protocol for a comparative study of two countries, Sweden and Denmark. The comparative study reveals similarities and differences between both countries towards preventing the spread of the COVID-19 [12].

Although there are many studies/works made in the literature aiming to reduce the spread of COVID-19, a study of developing a novel algorithm, which allocates movement permits inside workplaces during/outside curfew period, does not exist yet (it is at least extremely rare reported in the literature).

Furthermore, most efforts introduced or suggested in the literature are trying to help the practice of social distancing towards "flattening the curve" during the COVID-19 pandemic. Such attempts will ultimately cost humanity and the economy a lot, tragic human consequences and economic uncertainties, which lead to disastrous results.

This work represents the first approach towards introducing an algorithm by enabling individual human agents to move safely inside workplaces avoiding infections according to COVID-19 social distancing guidance.

### III. SOFTWARE APPLICATION ROLES AND RESPONSIBILITIES

There is a wide variety of software applications, which are developed to protect people during the COVID-19 pandemic, to manage public health emergencies, or to reduce the number of COVID-19 infections. One of the more interesting roles of these applications was providing instant and live information about the number of COVID-19 infections in a city or a country. In this case, early detection of possible infections will be insured directly after a user of this application shows COVID-19 symptoms. Furthermore, some software applications are trying to distribute movement permits to people that request them during curfew in necessary cases. Additionally, these applications update the permit requesters status during the curfew period to warn them as soon as they are closing to isolated or infectious areas. The more important role of those applications could be played by reporting all suspected cases of COVID-19 so that other people can receive healthcare services timely.

An interesting example of such an application is Tawakkalna App [13]. It is an official app issued by the Saudi Data and Artificial Intelligence Authority (SDAIA) in cooperation with the Saudi Ministry of Health. The goal of this app is to prevent the spread of COVID-19. Tawakkalna App makes it easy to issue movement permits during the curfew period. Additionally, it can be utilized for various health care purposes during the COVID-19 pandemic [13].

In this context, Corona-Warn is another aspect of the intended applications. For example, the Corona-Warn-App in Germany [14] is an app that traces infection chains of COVID-19 in Germany. This application uses a decentralized approach to warn users about exposure to COVID-19. The German government asked SAP and Deutsche Telekom subsidiary T-Systems to develop a Corona-Warn-App in May 2020. They are trying to integrate further information into the application, such as: the latest pandemic situation. The developers have summarized the steps of how the application works. Firstly, collect nearby identifiers using the Exposure Notification System on smartphones, where it should be regularly scanned for identifiers of other smartphones using Bluetooth, and consequently the identifiers can be stored locally. Secondly, communicate test results (optional) of users with symptoms. The tested users utilize the QR code that they received during their test to access their results themselves. Thirdly, distribute list of keys of COVID-19 confirmed users. Users with positive test results can voluntarily upload their last 14 days' temporary keys to the server. Fourthly, check for exposure to COVID-19 confirmed users. In this meantime, the Exposure Notification System will locally check if there is any matching between the downloaded list of users' keys which were tested positive and the locally collected Rolling Proximity Identifiers. If there is any successful match (exposure), the app user will receive immediately suitable support, if necessary [14].

### IV. ARE TECHNOLOGY SOLUTIONS READY FOR LIFE AFTER CORONA?

Life after COVID-19 is new and not the same as before. Therefore, technology solutions should be the premier provider of services in society after COVID-19. In this context, movement permits during the COVID-19 pandemic is one of the more interesting solutions.

To understand the main goal, the next comparison is performed between the public health strategy, flatten the curve, and establishing a robust technical computer system.

Fig. 1 denotes how the public health strategy, called "flatten the curve", is used to slow the spread of a pandemic. The sharp curve shows the spread of a pandemic caused by a disease, for example, the COVID-19 virus, if no intervention (no proactive measures) strategies are provided through a community. This means that infected cases would rise rapidly if no interventions were made aiming to mitigate the spread. To reduce the daily infections and consequently to flatten the curve, some interventions (proactive measures, non-pharmaceutical) would be necessary, such as social distancing, hand washing, isolation, etc. Therefore, with intervention, the second curve (successfully flattened curve) becomes much flatter in the scenario of the COVID-19 pandemic.

Fig. 2 shows the main idea of establishing a robust technical system, which can tolerate faults, deviations, and disturbances that could be occurred in the system. The approach, in this figure, aims to make the system capable to return to its normal state with minimal central proactive measures (intervention) after disturbances, faults, or other problems [17]. Additionally, it can operate under real-time conditions, because a short response time is critical to the success of such robust systems. Moreover, robust technical systems should continue working effectively to fulfill their major tasks in cases of disturbances. Fault or disturbance tolerance plays an important role in avoiding system failures. This approach considers three cases of the system operation: firstly, operation without disturbance, secondly, operation with disturbance without intervention, and finally, operation with a disturbance with the intelligent intervention [17].

In this figure, the system performance is represented by throughput, as an example. If no disturbances occur, the performance of the system (throughput) should be equal to 1 (i.e., at its best). However, in the case of any disturbance occurrence, the system performance would start to collapse over time, if no corrective actions are taken in time. Otherwise, the system performance will recover over time when any disturbance occurs, only if intelligent and corrective intervention is quick enough. In other words, the system performance lasts longer despite disturbance occurrence [17].

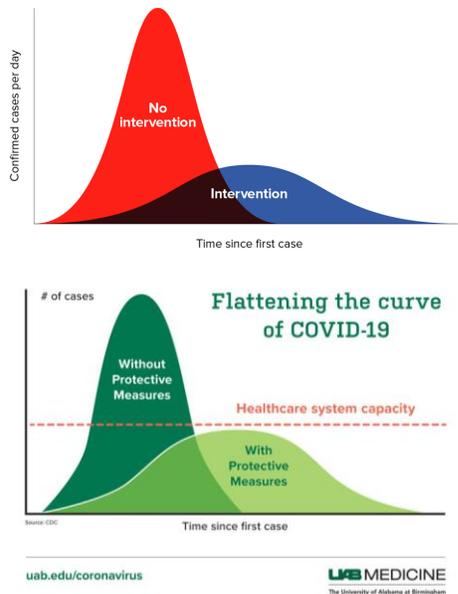


Fig. 1. The Public Health Strategy "Flatten the Curve" [7] [15].

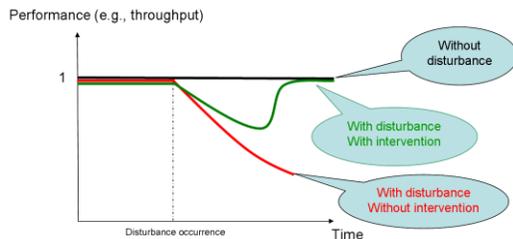


Fig. 2. Robust Technical System with Disturbance Occurrence [16].

### Result of comparison

According to the previously introduced comparison of both Fig. 1 and 2, this section summarizes the results of this comparison as follows:

- The disturbance occurrence represents the start of the pandemic.
- Systems continue working effectively and fulfilling their major tasks would represent the peak of hospitalizations.
- System failures represent the peak of a pandemic spread.
- Intelligent intervention represents precautionary measures, giving/adapting movement permits, imposing social distancing, etc.

### V. OBJECTIVES OF THE APPROACH

This section will briefly discuss the objectives of the proposed approach/algorithm in this paper. It forms a connection to utilize computer science algorithms/concepts to adapt our life under the COVID-19 pandemic. A more detailed discussion will be given in the "The Approach" section later.

In the context of this paper, a technology solution is presented to practice social distancing in certain places, where

social distancing could be difficult. Such places can be inside workplaces, buildings, companies, and institutions. The goal is to optimize/adapt the movement permits in these places during/outside the curfew period. Additionally, it represents a strategy allowing the agents (people, robots) of the system to move reliably in their environment. For this reason, public health measures (precautionary measures) have to be enforced so that the spread of COVID-19 can be prevented or at least be reduced in workplaces. Furthermore, this paper proposes a solution for the resource allocation problem, called the resource sharing problem, where multiple agents (people, robots) moving in a shared environment trying to avoid collisions (infections).

### VI. THE SCENARIO

This section presents the application scenario proposed in this paper, where agents (people, robots) move in a shared environment inside workplaces during the pandemic period. They are trying to cross and move around as fast as possible using movement permits during/outside the curfew period. Furthermore, this section describes the required technique, which may include various capabilities. These capabilities are necessary to ensure that all agents can move safely avoid collisions (infections) in their workplaces.

Since many of the mitigation efforts of COVID-19 use computer models, graphics and simulations, an application scenario should be chosen so that it has a strong relationship with social distancing. Consequently, the application scenario introduced in this paper has a key role in giving/adapting movement permits for agents (people, robots) crossing a shared environment (resource allocation problem) inside buildings, e.g., the workplaces as depicted in Fig. 3. For this reason, a crossway control algorithm based on resource sharing is used. Such scenarios assemble the required concerns, which will be utilized to avoid collisions (infections) in workplaces.

In this scenario, a resource-sharing conflict arises. It is called a resource sharing problem (resource allocation problem). This problem should be resolved to prevent any collision within the shared place. Therefore, the coordination of agents is used later for the evaluation of the proposed scenario. In this context, a route planning algorithm is responsible for calculating the route with the shortest overall distance, if it exists, where safety is not overlooked in the presence of infections during the COVID-19 pandemic. Therefore, crowds in workplaces can be avoided helping to reduce the spread of COVID-19. In this regard, the proposed approach in this paper can use trajectories, where every agent travels using its planned trajectory. Additionally, adapting these trajectories according to the degree of safety is needed. For the special application domain, agents can be categorized into two classes: people (human) and robots.

When agents represent people in the applied scenario, then adapting trajectories (reallocation movement permits) is important to avoid infections in workplaces. However, if agents represent robots in other challenging scenarios, adapting such trajectories (adjusting movement permits) is required to avoid collisions in companies, workplaces or causing traffic jams.

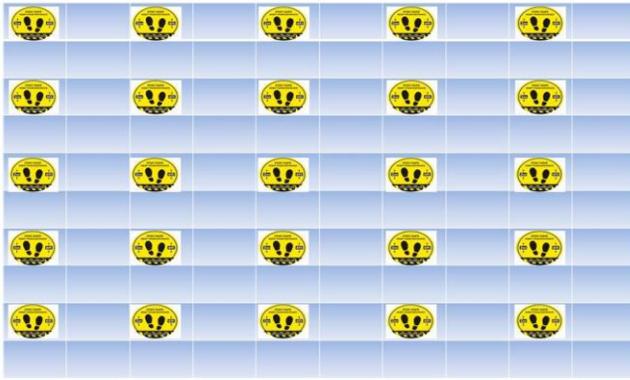


Fig. 3. The Shared Environment.

Finally, nowadays software products are using security cameras, which are based on AI to track social distancing. This is essential to counter the overcrowded facilities so that compliance with health guidelines, such as mask-wearing and social distancing, can be ensured or enforced as long as possible.

## VII. THE APPROACH

The new approach presented in this paper is intended to allocate and optimize/adapt all permits of agent's (people, robots) movement during/outside curfew periods. These agents are trying to move safely inside workplaces, buildings, companies, and institutions. In this approach, safety measures will be taken into consideration during the COVID-19 pandemic. This approach distinguishes between two different kinds of agents.

In the first case, agents represent people so that this approach reduces the spread of COVID-19, where policies for promoting the health safety of workplaces during a pandemic are needed. Therefore, preventing infections and avoiding crowds in workplaces is one of the main keys to safety. Furthermore, determining the most suitable social distancing according to the actual conditions will be necessary. Consequently, the next step is observing the maintaining of a suitable social distancing range and readjusting it if needed.

In the second case, agents represent robots that are safely moving in companies/workplaces aiming to avoid collisions. Additionally, agents are trying as quickly as possible to reach their target positions without any collision at all times.

In both cases, the general problem domain of this paper can be represented as a resource allocation problem (resource sharing problem) where several agents must travel from a source to a destination in a shared environment. Therefore, any proposed solution should be able to cope with this problem. The introduced approach in this paper chooses coordination mechanisms that can deal with the resource allocation problem. The coordination of these agents can be achieved through trajectory planning or path planning. Such planning should consider all agents moving in the shared environment and also the environment geometry in the configuration space-time  $(x, y, t)$ . That means, the environment can be seen as a shared space over time.

According to the scenario presented in this paper, agents (people or robots) are trying to move safely in their environment to avoid collisions (infections). Additionally, every agent should get a reservation representing its route in the environment. This reservation can be configured as a recommendation to agents. It consists of the coordinates  $(x, y, t)$ . This means that a reservation is a collision-free trajectory that can be used to coordinate the system agents. The agent should obey its planned reservations (trajectory), but this is not always guaranteed. Especially, in dynamic environments agents could have full autonomy and consequently, they have their own decisions and actions. Therefore, agents, in such cases, will not follow their recommended reservations. Consequently, an observation of the shared space (environment) is necessary to detect if agents obey the planned reservations (movement permits). If there is any deviation, then a reallocation process of resources should be initiated immediately so that all movement permits can be re-evaluated and consequently re-issued for all affected agents, if required.

### A. Trajectory Planning

Nowadays, "safety measures", "keep a safe distance", "please keep your distance", "keep safe social distance", "keep physical distancing" are common signs everywhere. To achieve that, this section introduces the collision-free trajectories, which are required for all agents to move safely. These agents, using their planned trajectories, have to satisfactorily fulfill precautionary measures and health guidelines imposed by governments and safety authorities.

Intuitively, there will not be any conflict if every agent gets its trajectory uniquely. Therefore, a centralized control unit is required to calculate unique trajectories. As mentioned above, the trajectory planning in this paper is used as coordination mechanisms so that resource sharing problems can be solved, where agents move in a shared environment.

Firstly, all agents have local rules to move before they entered the shared environment as depicted in Fig. 4. This means, when people/robots leaving their rooms/base stations /home bases in workplaces and approaching a shared area (well-defined environment/crossroad/company yard), they do not need any planned trajectories from the centralized control unit. Otherwise, planned trajectories should be given for all agents inside the shared environment. These trajectories represent movement permits during/outside the curfew period. Additionally, these trajectories can be recalculated aiming to adapt/optimize the movement permits according to the actual conditions and safety degree.

The centralized control unit (trajectories planner) can simulate the agent's route through the shared environment. This simulation must consider the latest reserved trajectories for other agents using the configuration time-spaces, which is an extension of the configuration space of robots by a time axis. This should be done for every agent approaching the shared environment. The trajectory planner used in this paper is centralized so that it possesses a global view of all shareable resources that leads in turn to allocate collision-free trajectories.

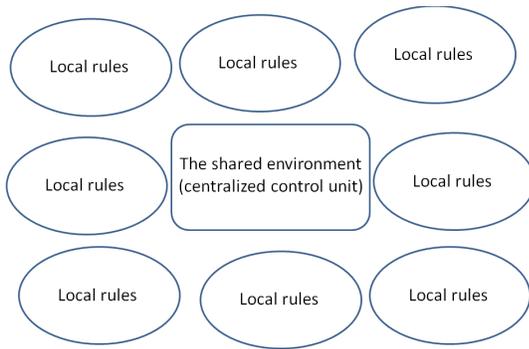


Fig. 4. Local Rules Outside the Shared Environment.

Every calculated route (trajectory) can be represented and planned as a vector (n-tuple) of points. Each point is modeled as space-time entities (objects) so that the  $(x_i, y_i)$  coordinates will be occupied at a time moment  $t_i$ .

$$\text{calculated route} = \{(x_1, y_1, t_1), (x_2, y_2, t_2), \dots, (x_n, y_n, t_n)\} \text{ with } 1 \leq i \leq n; i, n \in \mathbb{N} \quad (1)$$

### B. Algorithm

The algorithm serves as a basis to give an overview of how the centralized control unit works. It reacts according to input possibilities: request permission, agent class (people/robots), social distancing size. After handling the input values, it plans the most suitable routes (trajectories) as movement permits for agents. Furthermore, it can send emergency instructions if needed to send any warning signals to the participants in the case of an emergency. Additionally, it will adapt/recalculate these movement permits in two cases: firstly, if agents do not obey the planned routes. Secondly, if the given social distancing size was changed based on a new defined degree of safety. Accordingly, the input and output of the proposed algorithm can be summarized as follows:

Input: request permission, agent class (people/robots), social distancing size.

Output: movement permits (giving/adapting), reservations, calculated trajectories (new/adapt), emergency instructions.

In this algorithm, the Euclidean distance, which is a straight-line from a given point to the goal point, is the heuristics used to estimate the cost of reaching the goal point. Using these heuristics will ensure finding the shortest path (if it exists) and consequently planning optimal paths inside shared environments. This distance can be determined using the formula as described in the next equation:

$$\min \| (x_s, y_s) - (x_g, y_g) \| ; (x_s, y_s): \text{start point}, (x_g, y_g): \text{goal point} \quad (2)$$

Comparing to the algorithm described above, an adapted algorithm, which can be used in this approach, can have the following features:

- The function `recalculateRoutesOfAffectedAgents()` can be used to recalculate trajectories if some agents violate the planned routes. In this context, the presence of modified policies of social distancing size (SDS) can be taken into account.

- The function `ModifySocialDistancingSize (SDS)` is used when the current social distancing policy is modified by the state or the city to force new requirements or to give recommendations. This can be possible by reopening after the COVID-19 lockdown but under modified social distancing orders and regulations.

### Algorithm: Overview of "Movement Permits During Corona" Algorithm

```

AlgorithmMovementPermitsDuringCorona (startPoint,
goalPoint)
BEGIN
Input (RP, AC, SDS); // RP: request a permission,
AC: agent class, SDS: social distancing size.
Initialise (C, RSM, startPoint); //C: calculated
Route, RSM: Resource Sharing Map
CostSoFar (startPoint) = 0;
bestCalculatedRouteSoFar (startPoint) = startPoint;
updatedRSM = insertToRSM (startPoint), Cost
(startPoint) = 0;
while not isEmpty (updatedRSM) do
nextPoint =
returnNextPointFromRSM(updatedRSM);
if (nextPoint = goalPoint) then
return bestCalculatedRouteSoFar ();
end if
for all neighbours in RSM(nextPoint) do
=
calculateTheRestPartOfRoute(nextPoint,
t, SDS); RPR
calculateTheCostOf (RPR);
bestCalculatedRouteSoFar
(neighbours) = nextPoint;
end for
end while
if (situation = emergency) then
findTheBeingWell-
preparedForTheEmergency ();
return bestEmergencyInstructions ();
end if
Output (movement permits, emergency instructions).
END
    
```

## VIII. PERFORMANCE EVALUATION

In this section, an initial evaluation of the algorithm proposed in this paper is presented. It uses the model of a shared environment inside workplaces during the pandemic period as depicted in Fig. 3. As mentioned above, in this paper, agents (people or robots) move within a shared environment. This application scenario served as a test bed for the evaluation of the approach presented in this thesis.

Since the trajectories planning plays an important role in the user application scenario to achieve high throughput (performance), an evaluation of this algorithm is necessary under different loads of agents. In this regard, we assume that there won't be any deviations from planned trajectories. Furthermore, we assume that the social distancing size (SDS) is equal to 1 cell in the modeled shared environment.

In future work, on one hand, the handling of deviations from planned routes should be studied and considered. Moreover, on the other hand, modified social distancing size (SDS) should be taken into account.

Additionally, two metrics were used for evaluating the approach: throughput and mean waiting time. Firstly, throughput presents the total number of agents that left the shared area (environment) over time (#Agents/tick). Secondly, mean waiting time presents the average time (iterations/ticks) needed by agents to cross the shared environment.

All required experiments have been carried out based on a MAS simulation using the "Repast" (Recursive Porous Agent Simulation Toolkit) framework [18].

A. Evaluation Scenarios

To compare the system performance in different evaluation scenarios, two simulation parameters were used for measuring the system performance. Firstly,  $A_{max}$  presents the maximum number of all agents in the whole system. Secondly,  $P_{rate}$  is the production rate of agents in the whole system (agent flow rate). Modifying the values of  $A_{max}$  and  $P_{rate}$  will be useful for ensuring effective performance of the proposed approach in different combinations of the simulation parameters. Particularly, this effectiveness of system performance can be guaranteed even in crowding, e.g. during rush hour for employees arriving for their work; where it would be difficult for them to get their work done at their company during the pandemic.

Both defined metrics for performance evaluation were measured in a simulation interval between 0 and 3000 ticks (time steps). As depicted in Fig. 4, agents can flow in all directions, and consequently, four directions should be taken into account.

In this scenario, the shared environment is represented as a 10x10 grid cell, where every cell can be considered as a reservation tile. For example, the throughput and the mean waiting time (MWT) of the system were measured in the case that the production rate of agents ( $P_{rate}$ ) in the whole system is 5 agents/tick. Furthermore, the measurement was repeated in the cases that the maximum number of agents in all directions (inside and outside the shared environment) is 40, 60, 80, 100, 120, and 500 agents. It is worth mentioning that the case of 500 agents in all directions can be seen as a crowding threshold (an extreme case) in this scenario. Additionally, a series of experiments were performed by changing the production rate of agents ( $P_{rate}$ ) in the whole system: 10, 13, 18, 20 agents/tick.

B. Results

1) *Throughput measurement:* Fig. 5 displays the system throughput per time unit (#Agents/tick) for the evaluation scenario described above using some combinations of both simulation parameters:  $A_{max}$ ,  $P_{rate}$ . As mentioned earlier, The throughput was measured for a simulation interval between 0 and 3000 ticks.

Fig. 5 shows that from the simulation time/iteration 115 (it is an approximation and not an accurate simulation time) agents start leaving the shared environment. This can be

explained by the fact that the shared environment was free from agents at the simulation start. This in turn leads to the system throughput per time unit, which is 0 during the simulation interval between 0 and 115. However, shortly after that, the system throughput per time unit (#Agents/tick) is constantly increasing with the passage of simulation time. This can be traced back to the system throughput per time unit as it goes in fair proportion to the number of agents. However, there is a single exception to this statement only in the extreme case/crowding threshold (500 agents in all directions). In this case, the system performance reaches only a value of around 9400 agents. That is because the maximum number of agents, in this case, is greater than the capacity of the whole designed environment. Consequently, it concludes that the system throughput per time unit is increasing steadily within the environment's capacity (resource consumption) with the number of agents for all possible combinations of both simulation parameters. It is worth reminding that one tick in the used "Repast" simulator means one-time step.

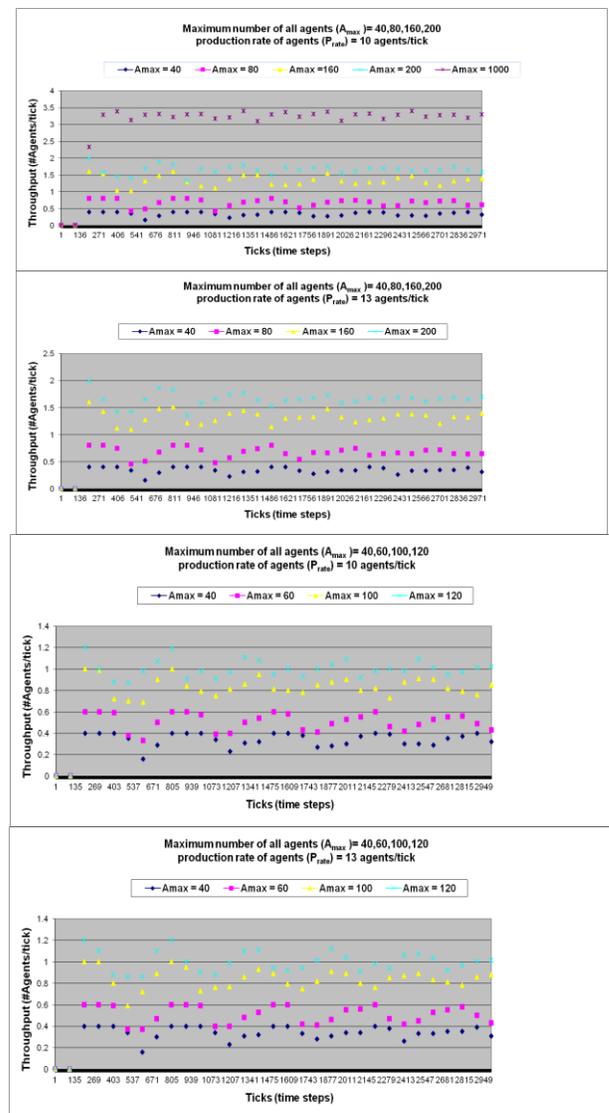


Fig. 5. The System throughput Per Time unit (#Agents/Tick) for the Evaluation Scenario for a Simulation Interval between 0 and 3000 Ticks

2) *Mean waiting time measurement (MWT)*: This metric can be evaluated in many cases as the first metric, throughput, mentioned above. However, it is noteworthy in this context that the mean waiting time is calculated in an extreme case. In this case,  $A_{max} = 1000$  is the maximum number of all agents in the whole system inside and outside the shared environment. This case represents a crowding threshold, where the maximum number of agents is in fact greater than the capacity of the shared environment. Consequently, such measurement will give an environmental protection to authority by calculating the longest waiting time spent by agents crossing a shared environment during the pandemic period.

In this context, several experiments have been carried out aiming to study the mean waiting time in different values of production rate ( $P_{rate}$ ) of agents. Therefore, the values of the mean waiting time of all agents and their standard deviations were calculated after the simulation end time in the extreme case ( $A_{max} = 1000$ ) as depicted in Table I.

As a result, despite having big values of agents, the designed system has low mean waiting times (Latencies) with small standard deviations. That applies in different production rates of agents, where the worst mean waiting time was  $\Phi 4.290499947151464 \pm 1.3562567367584307$  in case of the biggest  $P_{rate}$  applied in simulation experiments of this paper.

Furthermore, this exploratory qualitative study also measured total waiting times (aggregated latencies) and mean waiting times (mean latencies) in normal cases (not only the extreme case), e.g., by  $A_{max}=200, P_{rate}=8$  during the whole simulation period.

Firstly, Fig. 6 shows the total waiting times (aggregated latencies) in the case of  $A_{max}=200, P_{rate}=8$  during the whole simulation. The experimenter here can see that the worst total waiting times which agents experience is about 250 ticks as depicted in Fig. 6.

Secondly, Fig. 7 shows the mean waiting times (mean latencies) in the case of  $A_{max}=200, P_{rate}=8$  at any time during the experiment simulation. The designer here will see that the worst mean waiting time which can be measured is ca. 1.3 ticks as depicted in Fig. 7.

Thirdly, Fig. 8 shows the maximum waiting times (maximum latencies) in the case of  $A_{max}=200, P_{rate}=8$  during the whole experiment. These measurements showed that the biggest waiting time which can be experienced is 7 ticks as depicted in Fig. 8.

TABLE I. MEAN WAITING TIMES (LATENCIES) OF ALL AGENTS AND THEIR STANDARD DEVIATIONS AFTER THE SIMULATION END TIME IN THE EXTREME CASE

$A_{max}$	$P_{rate}$	mean waiting time (Latency in ticks)	standard deviations
1000	5	2.7831321540062435	0.9451051160462923
	7	3.528389521237694	1.4656030736537114
	10	3.872145144076841	1.836589145239349
	13	4.147975811584978	1.5825953904261338
	15	4.290499947151464	1.3562567367584307

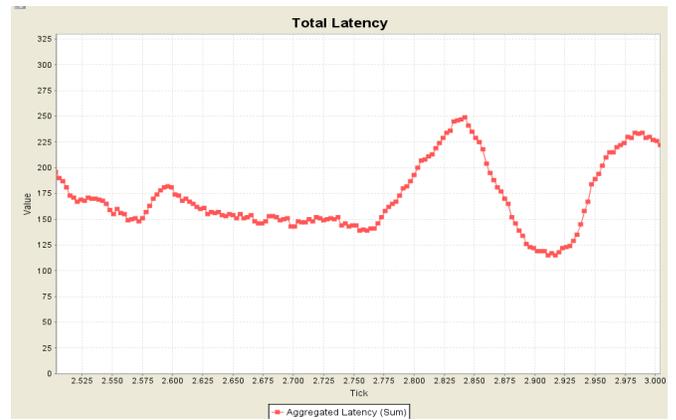


Fig. 6. Total mean Waiting Time (Aggregated Latencies) by  $A_{max}=200, P_{rate}=8$ .

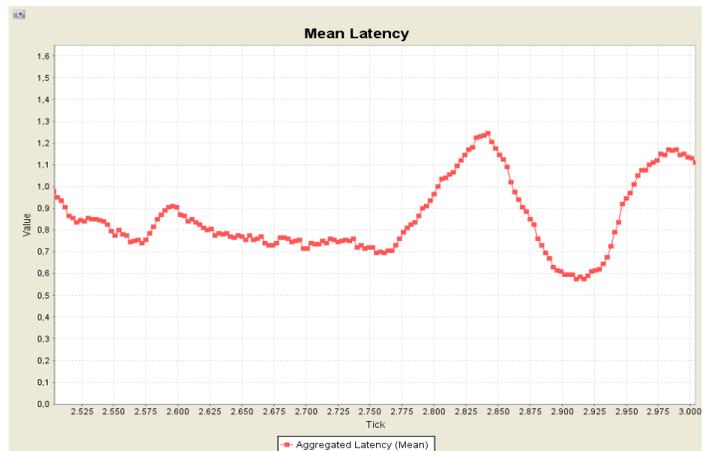


Fig. 7. Aggregated mean Waiting Time (mean Latency) by  $A_{max}=200, P_{rate}=8$ .

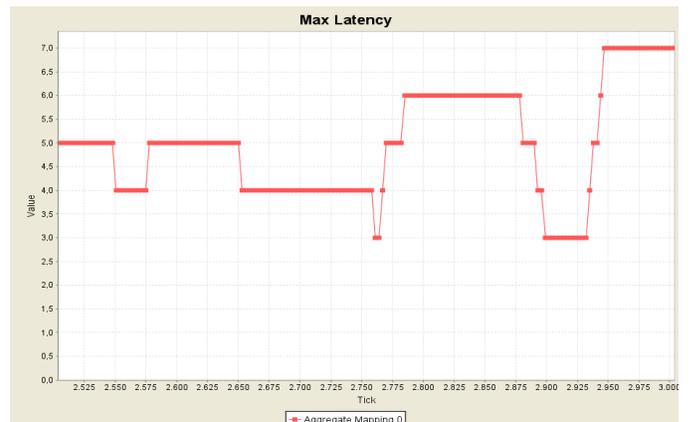


Fig. 8. Maximum Waiting Times (Maximum Latencies) by  $A_{max}=200, P_{rate}=8$ .

IX. CONCLUSION

The tightened measures against COVID-19 are supported by a clear majority all over the world these days. This in turn led many authorities in the world to restrict movement and range of motion or even impose nationwide shutdowns. In this case, lockdown also caused a shut down of social life during the COVID-19 pandemic. Therefore, studies were initiated

aiming to prevent the imposition of such lockdowns and consequently to mitigate the bad economic impacts on society and businesses. In this context, this paper presented a new approach/algorithm as a technical solution towards achieving a desired target safety margin despite COVID-19 disturbances. This approach was trying to adapt the social distancing by movement permits inside workplaces, institutions, companies, and big buildings. On other hand, the paper proposed a possibility for solving the problem called "resource sharing problem" or "resource allocation problem". It supposes that the designed system consists of many agents representing people or robots aiming to reserve suitable resources of their shared environment. The evaluation of the proposed algorithm that manages all movement permits (resource allocations) showed the high performance of this algorithm (high throughput values and low waiting times or latencies). Additionally, all experiments were based on various loads of agents to ensure their safe and reliable operation.

## X. FUTURE WORK

Comparing to the algorithm evaluation described above, an extension is necessary to incorporate detailed results and expanded experiments. Especially, detecting and handling possible deviations from routes planned from the algorithm would be the first step in future work. Furthermore, taking into account that social distancing size (SDS) can be modified due to changed policies and procedures would be the second step in the future work as well. After that, the paper extension will be satisfactory evidence of compliance with the applicable requirements of Corona-stipulated social distancing.

## REFERENCES

- [1] The World Health Organization (WHO). <https://www.who.int/> [access July 2020].
- [2] Healthcare Market Research. "Technology Solutions - Coronavirus (COVID-19) Case Study". Pages : 18 - Publisher : GlobalData - Report code : ASDR-536189 , 2020. [access October 2020]. Available from <https://www.asdreports.com/market-research-report-536189/technology-solutions-coronavirus-covid-case-study>.
- [3] IEEE ProComm. "Flatten the Curve: Why certain messages catch on". IEEE Professional Communication Society (ProComm). 05 May, 2020. <https://procomm.ieee.org/flatten-the-curve-why-certain-messages-catch-on/>.
- [4] R. Bonoan and P. Starks. "Honey bees can't practice social distancing, so they stay healthy in close quarters by working together". The Conversation. Aug 14, 2020. [theconversation.com](http://theconversation.com).
- [5] R. Bonoan and, P. Starks. "Honey Bees Stay Healthy In Such Close Quarters". The innerself . August , 2020. [innerself.com](http://innerself.com).
- [6] S. Roberts. "Flattening the Coronavirus Curve". The New York Times. ISSN 0362-4331, 27 March 2020. [access July 2020]. <https://www.nytimes.com/article/flatten-curve-coronavirus.html>.
- [7] J. Ryan. "Coronavirus pandemic: How social distancing can help flatten the curve". CNET, 16 March 2020. [access July 2020]. <https://www.cnet.com/news/coronavirus-pandemic-how-social-distancing-can-help-flatten-the-curve/>.
- [8] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, et al. "A Survey of COVID-19 Contact Tracing Apps" in IEEE Access, vol. 8, pp. 134577-134601, 2020, doi: 10.1109/ACCESS.2020.3010226. <https://ieeexplore.ieee.org/document/9144194>.
- [9] L. Thunström, S. C. Newbold, D. Finnoff, M. Ashworth, and J. F. Shogren. "The Benefits and Costs of Using Social Distancing to Flatten the Curve for COVID-19" in Journal of Benefit-Cost Analysis, 11(2):1-27, April 2020, doi: 10.1017/bca.2020.12. <https://doi.org/10.1017/bca.2020.12>.
- [10] A. Ghorai, S. Gawde, and D. Kalbande. "Digital Solution for Enforcing Social Distancing". Proceedings of the International Conference on Innovative Computing & Communications (ICICC) May 31, 2020, Available at SSRN: <https://ssrn.com/abstract=3614898> or <http://dx.doi.org/10.2139/ssrn.3614898>.
- [11] University of Texas M. D. Anderson Cancer Center. "Implementation of social distancing policies correlates with significant reduction in SARS-CoV-2 transmission: Study of 50 US states and 134 nations reinforces social distancing as effective public health tool". ScienceDaily. Available at: [www.sciencedaily.com/releases/2020/07/200730161025.htm](http://www.sciencedaily.com/releases/2020/07/200730161025.htm).
- [12] P. Nilsen, I. Seing, C. Ericsson, O. Andersen, N. Thórný Stefánsdóttir, T. Tjørnhøj-Thomsen, et al. "Implementing social distancing policy measures in the battle against the coronavirus: protocol of a comparative study of Denmark and Sweden". In Implementation Science Communications 1, 77 (2020). <https://doi.org/10.1186/s43058-020-00065-x>.
- [13] Saudi Data and Artificial Intelligence Authority (SDAIA). "Tawakkalna App". About Tawakkalna, 2020. <https://ta.sdaia.gov.sa/en/index> [access July 2020].
- [14] The German government, SAP and Deutsche Telekom subsidiary T-Systems. "Corona-Warn-App App in Germany". About Corona-Warn-App in Germany, 2020. <https://www.coronawarn.app/en/> [access October 2020].
- [15] H. Herfurth. "What exactly does it mean to 'flatten the curve'? UAB expert defines coronavirus terminology for everyday life". April 28, 2020, The University of Alabama at Birmingham (UAB). <https://www.uab.edu/news/youcanuse/item/11268-what-exactly-does-it-mean-to-flatten-the-curve-uab-expert-defines-coronavirus-terminology-for-everyday-life>.
- [16] Y. Chaaban and C. Müller-Schloer. "A Survey of Robustness in Multi-Agent Systems", in Cognitive13: proceedings of the Fifth International Conference on Advanced Cognitive Technologies and Applications, 2013, pp. 7-13.
- [17] Y. Chaaban. "A Methodology for Designing Robust Central/Self-Organising Multi-Agent Systems", in International Journal of Computer Information Systems and Industrial Management Applications, Vol. 6, 2014, pp. 571-581
- [18] RePast (Recursive Porous Agent Simulation Toolkit) framework. <http://repast.sourceforge.net/>, [accessed, September 30, 2020].

# Internet of Things Security: A Review of Enabled Application Challenges and Solutions

Mona Algarni<sup>1</sup>, Munirah Alkhalaiwi<sup>2</sup>, Abdelrahman Karrar<sup>3</sup>  
College of Computer Science and Engineering  
Taibah University  
Medina, Saudi Arabia

**Abstract**—The Internet of Things (IoT) has been widely used in every aspect of life. The rapid development of IoT technologies raises concerns regarding security and privacy. IoT security is a critical concern in the preservation of the privacy and reliability of users' private information. The privacy concern becomes the biggest barrier to further usage of IoT technology. This paper presents a review of IoT application areas in smart cities, smart homes, and smart healthcare that leverage such techniques from the point of view of security and privacy and present relevant challenges. In addition, we present potential tools to ensure the security and preservation of privacy for IoT applications. Furthermore, a review of relevant research studies has been carried out and discusses the security of IoT infrastructure, the protocols, the challenges, and the solutions. Finally, we provide insight into challenges in the current research and recommendations for future works. The reviewed IoT applications have made life easier, but IoT devices that use unencrypted networks are increasingly coming under attack by malicious hackers. This leads to access to sensitive personal data. There is still time to protect devices better by pursuing security solutions with this technology. The results illustrate several technological and security challenges, such as malware, secure privacy management, and non-security infrastructure for cloud storage that still require effective solutions.

**Keywords**—*Internet of things; internet of things application; internet of things privacy; internet of things architecture; internet of things security; challenges; security protocol*

## I. INTRODUCTION

The modern technological revolution has become an integral part of our lives. Internet-enabled devices produce Internet crowding, as they contain large amounts of data that make the device useful. This technology provides access to information in real-time; one example of this is home monitor systems. IoT can improve productivity and reduce sudden breakdowns due to risks and disasters. Access to any information is made easy thanks to modern phones and technologies' smart devices. IoT-enabled devices are characterized by sensors and small computing equipment that are used communicate with other devices and connect to them. With the progress of IoT, which focuses on increasing productivity, reducing costs, and improving quality of life, the

privacy of the information transmitted through smart devices must be preserved. After the Internet managed to make the world a small village that is easy to navigate between its branches in less time and effort, it is now possible to attract things to connect them to the Internet automatically without the need for human intervention.

There are security flaws in IoT technology that are difficult to correct with software updates, making IoT vulnerable to piracy and information manipulation. For example, home surveillance cameras are an easy target for hackers as a hacker can violate homeowners' privacy. Some smart watches have also been found to contain security flaws that allow hackers to track users' locations. Maintaining the confidentiality of user data is essential to consumer confidence. Still, in reality, many of these devices, especially the cheap ones, do not give importance to privacy issues such as data encryption. There is a need to address defects in IoT hardware and software, which, since they are difficult to correct through software updates, have to be tackled during the design of these devices [1].

This topic has been chosen because IoT technology facilitates our daily lives and makes communication between electronic devices more accessible. Besides these features, security and privacy must be provided during the connection of these devices. It is necessary to study IoT security to maintain user privacy, improve performance, spread security awareness related to IoT technology, and integrate the physical world and the security of IoT technology. Secure IoT helps improve data efficiency, accuracy, and privacy.

A comparison of this paper with previous review and survey papers on IoT security is presented in Table I, and a summary of the previous work is outlined to summarize the key contributions of the present study's review. The specific contributions of this paper are as follows:

- IoT security challenges in the context of its applications are reviewed.
- An overview of the various security tools and solutions for IoT is presented.

TABLE I. COMPARISON OF THIS PAPER WITH CURRENT IoT SECURITY SURVEY AND REVIEW PAPERS (COVERED: √, NOT COVERED: X)

Year	References	Highlights	Type	IoT Architecture	IoT Features	IoT Security Requirements	Security Protocols for IoT	IoT Applications	Security Challenges in IoT	Categorization of Security Issues	IoT Security Solutions	Solutions Provided by Blockchain	Solutions Provided by Edge Computing
2012	(Suo et al.) [38]	Provided an in-depth analysis of the architecture and security features of the IoT and its requirements. The main security technologies such as encryption and its algorithms, communication security and sensor data protection, and the main challenges it faces it also discussed	Review	√	√	√	X	X	√	X	X	X	X
2016	(Yamashita et al.) [34]	Discussed the challenges facing the IoT from the security aspect. Provided an overview of IoT securing features and discussed the security solutions to protect user data.	Review	√	√	√	X	X	X	X	√	X	X
2016	(Tyler) [36]	This review analysed the literature on IoT security, discussed the security standards, and proposed a framework for IoT's key security requirements.	Review	X	X	X	X	X	√	X	X	X	X
2017	(Khan & saleh) [32]	Presented a review of security specifications, issues, challenges, and solutions according to the IoT-layered architecture and analysed blockchain technology for IoT security issues.	Review	√	X	√	X	X	√	√	X	√	X
2018	(Joshi et al.) [14]	Provided a review of different challenges and security defences in IoT-layered architecture.	Survey	√	X	√	X	X	√	X	X	X	X
2018	(Burhanuddin et al.) [39]	Provided a review of IoT security challenges and analysed the primary and secondary IoT security specifications, followed by a description of the possible threats against these specifications.	Review	X	X	√	X	X	√	X	X	X	X
2019	(Perwej et al.) [40]	Provided a review of IoT security attacks, solutions, and guidelines to secure IoT devices.	Review	X	X	X	X	X	√	X	√	X	X
2019	(Sultan et al.) [41]	Provided a review of IoT security requirements, challenges, and outlined limitations after blockchain deployment.	Review	X	X	√	X	X	√	X	X	√	X
2019	(Abdullah et al.) [42]	Provided a review of security issues, specifications in IoT layers and presented blockchain technology as a potential IoT security solution.	Review	√	X	√	X	X	√	X	X	√	X
2020	(Mrabet et al.) [20]	Introduced a five-layer IoT architecture and reviewed security threats and solutions based on the proposed IoT architecture.	Survey	√	X	X	X	X	√	X	√	X	X
2021	<b>This research</b>	Presents a review of IoT security challenges in the context of its applications and various security tools to secure the IoT. Besides, it discussed the structure and layers of the IoT, protection protocols, IoT security features, and requirements. This paper dealt with challenges and issues in IoT technology and presented effective solutions to solve the issues.	Review	√	√	√	√	√	√	√	√	√	√

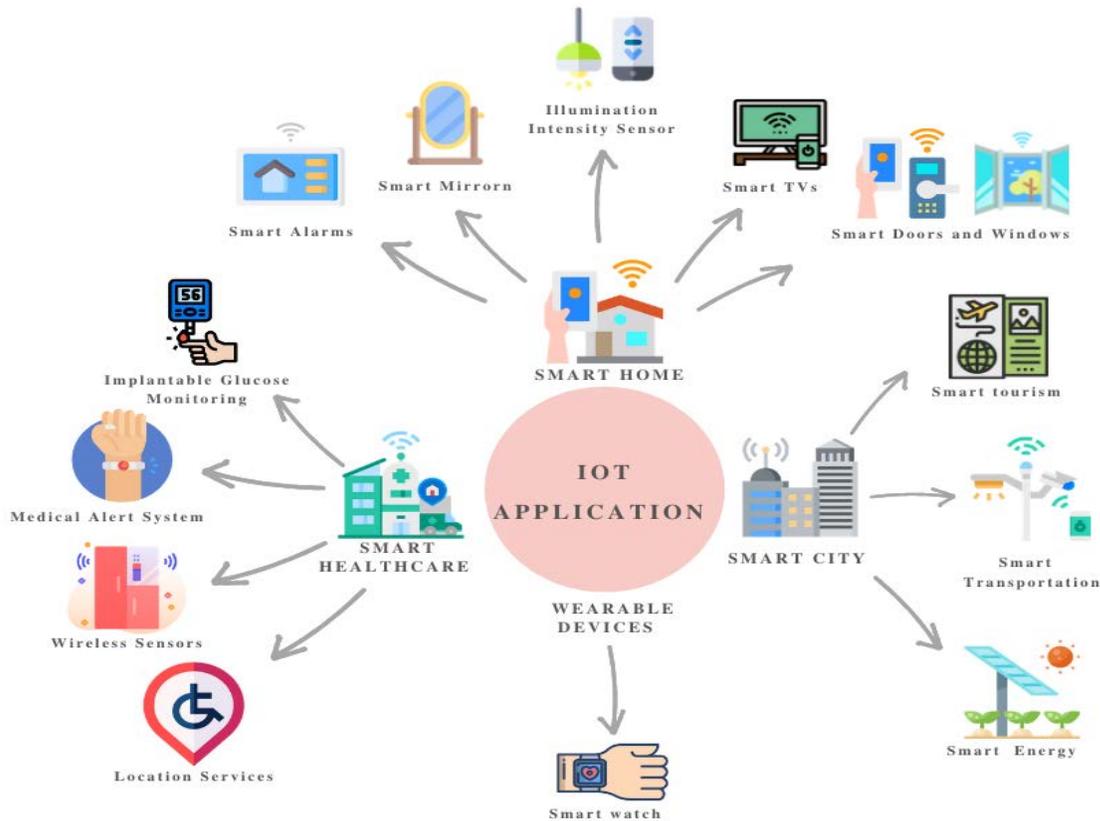


Fig. 1. IoT Application.

In this review, we select smart cities, smart healthcare, and smart homes as the main application fields of IoT, taking into consideration their corresponding use cases and security challenges. Fig. 1 illustrates these use cases.

The remainder of this paper is structured as follows: Section II: Related works, Section III: IoT definition and value, Section IV: IoT architecture, Section V: IoT features, Section VI: IoT security requirements, Section VII: IoT security protocols, Section VIII: IoT applications, Section IX: IoT security challenge, Section X: Categorization of the security issue, Section XI: Security mechanism, Section XII: IoT security solution, Section XIII: Findings, Section XIV: Discussion solution, Section XV: Future works, Section XVI: Conclusion and recommendation.

## II. RELATED WORKS

This section will discuss several studies related to the security of IoT-based technologies.

In one study [2], the authors propose a solution to secure the IoT system with machine learning techniques. In the study, the researchers used artificial neural networks (ANNs) to analyse the data and discover anomalies. They used R programming tools to create an ANN and selected a neural net package that makes it possible to construct a neural network for forecasts. The result shows that the use of neural networks

in the protection of an IoT device can be rigged for intrusion detection.

In another study [3], the authors discuss different security challenges in IoT and develop security solutions for IoT systems. The primary technique applied in this study is EdgeSec, which is embedded at the edge layer. Moreover, the authors applied EdgeSec in multiple use cases in the Smart Home application. The result shows that EdgeSec tackles most of the significant challenges affecting IoT security.

In yet another study [4], the authors discuss security issues and consider the problems of the large-scale, heterogeneous, resource-constrained IoT devices. They offer a list of cases, in which, different designs cover these low-capacity devices. The first case is to consider IoT end devices as conventional computing devices and to directly deploy specific protection solutions to those devices. Then, the correct protocols and algorithms should be considered; the end devices can assist with that. The second case is to gain assistance from edge devices and the cloud so that security-related activities can be moved to layers with large processing and storage capacities. The research shows that the security can be enhanced by the distribution of security information storage.

Another research paper [5] discusses IoT security, where the author focused on IoT technology's security aspects and the most prominent threats it faced as well as the security risks. Furthermore, the ability to effectively benefit from the

available opportunities by providing balance and security control is discussed, as are the rapid improvement of IoT technology and its ability to provide different types of growing services, impacting social life and work environments. Many innovations such as IoT, M2M, and artificial intelligence (AI) bring many cyber threats and solutions available to provide security. An excellent way to prevent these risks is the development of policies and strong controls. The author concludes that connecting more devices provides an opportunity to share more important personal information. However, the large number of devices that are connected causes some security problems. Thus, as technology rapidly evolves, its vulnerabilities also increase, which raises the chance for security crimes. This necessitates the ability to confront security threats.

In another study [6], researchers focused on the widespread use of IoT devices, which requires the development of security and privacy, to help implement better security, identify weaknesses in IoT devices, and promote low-cost IoT security methods. Their research mentioned the use of IoT devices in the commercial and industrial fields. The companies must increase security solutions to mitigate potential damage from this technology. Furthermore, they mention that deploying IoT devices at risk in the field led to safety complications. Due to the services provided by these units, an attacker could use these devices to cause physical sabotage. For example, industrial IoT-embedded devices can use the CENTRON CL200 Smart Meter to damage cyber-physical systems, such as the power grid. Excess consumption of uncensored energy can lead to an overload of the network, resulting in power outages and, in extreme cases, device malfunctions. Besides, it can lead to damage or loss, the attacker from hijacking the functionality of the devices the device performs intending to detect and attack the local network. For example, the Haier SmartCare device is used to deploy services in local networks and offers the user an operating system that is rich in capabilities. This device also enables participation in Address Resolution Protocol (ARP) and masquerades as a router, allowing targeted computer network traffic to be captured. Industrial devices pose a more significant threat if exposed to danger, as infrastructure may be corrupted, energy consumption information may be sabotaged by changing the smart identity, thus consuming energy while masquerading as a different device. Through the programming and debugging interfaces, the attacker can change the energy bill data. Thus, the power supply will not bill customers efficiently because the values recorded in the electricity meter's capacity calculations are incorrect.

Different research papers discuss the security of IoT. In one study [7], the researcher discusses some uses of IoT in manufacturing; for instance, the Walmart Corporation has already invested a lot into implementing IoT in its supply chain, retail, healthcare, and home services. The authors of the study point out security issues in IoT environments. Due to the volume of data, the primary security problems that are included are IoT default passwords and low-level devices on the transport layer with weak encryption. Additional issues include vulnerabilities in a web browser or mobile platform, which could grant access through IoT to gather and transfer

private information without protection over the network, and unsecure code practices. All of these problems present as incredible security risks. In the aforementioned paper, the researchers state that there is no preventive solution to IoT attacks unless security is implemented in its production lifecycle. Moreover, they mention some measures and solutions, such as secure network traffic, code reviews, and device platform, to reduce threats.

In another study [8], the researchers mention some background IoT security methods and techniques by researchers and organizations. The proposed security architectures have simple protection measures that cannot be automatically copied to construct IoT security systems due to the unique attributes of IoT. Standard network security models may be used for guidance through a dynamic approach to IoT security. Moreover, they suggest an approach where immune concepts and frameworks are applied to model IoT protection as an immune system in a real defence environment. This alters its security protection techniques along with the IoT's changing security environment, making the suggested solution adaptable to actual IoT devices. In the experiments, the authors used simulation tools and equipment to simulate attacks using AIS concepts and frameworks to identify security threats and protect IoT devices.

According to a further study [9], the concept of IoT includes defining the structure that controls the three basic elements of this technology: embedded devices, the cloud, and end users. It contains a set of protocols that regulate the procedure of data processing, and encrypt the transmitted messages to ensure data privacy. The IoT's final implementation should also support the masking of complex infrastructure protocols to build a user-friendly IoT framework.

### III. IOT: DEFINITION AND VALUE

A wide variety of different objects, such as lamps, cameras, mobile systems, alarm clocks, and locks, which can connect to the Internet and share data, is referred to as the Internet of Things. The network link function allows managing things remotely by structuring the network architecture, which contributes to alignment with the real world. Through the use of emerging technology such as cloud storage, networking capabilities, internet protocols, and applications, IoT transforms products from their classic state into smart devices [10].

IoT makes different smart devices communicate over the Internet Protocol, using wireless sensor networks (WSN) and RFID technology, by sending and receiving data without human intervention infrastructure for physical structures. IoT devices include tools, sensors, and various AI tools [10].

IoT's importance is determined by enabling the user to monitor his computer when he/she is away from it. Today, it is possible to connect things that are used in our daily life to the Internet, such as cars, washing machines, fridges, alarm clocks, TVs, sensors, and many others. The process of exchanging data between smart devices may affect the privacy and privacy of individuals and their personal information. Among these issues, failure to properly monitor devices that

contain sensors as well as deliberately jamming operations, which some people perform with the aim of disrupting the communication between these smart devices in an illegal manner and with the motives of sabotage [10].

#### IV. ARCHITECTURE OF IOT

The structure of IoT comprises physical devices, detectors, network computing, designers' motors, and protocols. Researchers divide the IoT architecture into three layers, namely, the layers of perception, network, and application. There are comparable protection concerns to each IoT layer. The layers are outlined below [11].

##### A. Perception Layer

In IoT, the layer of perception is also known as the "sensors" layer. With the assistance of sensors and actuators, this layer has the purpose of gathering environmental data. The sensors layer processes the data and then transfers it to the network layer.

##### B. Network Layer

The network layer performs data routing and transmission to multiple IoT hubs and devices over the network. This layer is composed of cloud servers, Internet gateways, switching devices, and routing devices. It operates by using some of the latest innovations, such as Wi-Fi, LTE, Ethernet, 3G, and Zigbee. The network gateways serve as intermediaries among different IoT nodes by collating, sorting, and transmitting data from different sensors.

##### C. Application Layer

In order to deliver services, the application layer ensures that the data is reliable, complete, and confidential. The main purpose of IoT, which is establishing an intelligent environment, is accomplished by this layer.

The architecture of the three layers represents the core concept of IoT. More layered structures are classified by other researchers, namely five layers: perception, transport, processing, application, and business layers. As in the three-layered architecture mentioned before, the perception and application layers have a similar role. The remaining three layers are described below [12].

##### D. Transport Layer

This layer aims to transmit data from the perception layer to the processing layer, such as the wireless network, LAN, RFID, and Ethernet.

##### E. Processing Layer

Collecting, inspecting, and analysing all the data from the transport layer is the critical feature of this layer. It can accommodate the lower layers and offer various services by utilizing numerous innovations, such as servers, cloud computing, and big data processing.

##### F. Business Layer

This layer is concerned with meeting business requirements that focus on providing added value to businesses and end users. It is also concerned with promoting interconnected IoT applications in the business area.

#### V. IOT FEATURES

IoT is a dynamic system with a multitude of features. Some of the main and general IOT characteristics are as follows [13].

##### A. Interconnectivity

With regards to IoT, the global information and communication infrastructure can interconnect anything.

##### B. Things-Related Services

IoT is designed to provide thing-related functionality within the limitations of things, such as privacy and semantic consistency of physical things and their corresponding virtual things. The distribution of things-related resources within the limitations of things would impact both the technology of the physical world and the world of knowledge.

##### C. Heterogeneity

IoT systems are heterogeneous as they rely on the various configurations of the hardware and network. They can connect with other systems or service channels over different networks.

##### D. Dynamic Changes

Dynamically, unit states vary, for example, modes of sleeping/operating and connected/disconnected, along with machine conditions such as location and speed. In addition, there could be rapid changes in the number of devices.

##### E. Enormous Scale

The data can be synchronized between a large number of devices according to the needs of the end user. Therefore, the data is managed and analysed in a comprehensive way, which can contribute to making decisions.

##### F. Security

One of the most important features that must be available in Internet technology is user safety. This includes all user data transferred over the network.

##### G. Connectivity

Connectivity allows accessibility and compatibility to networks. On a system, accessibility becomes usable, while compatibility provides the standardized ability to use and generate data.

#### VI. SECURITY REQUIREMENTS FOR IOT

There seems to be a security problem with IoT devices from being hacked or used for large-scale attacks. For safe IoT implementation, various methods and requirements must be dealt with as listed below [14].

##### A. Data Privacy, Confidentiality and Integrity

Given that IoT data moves through multiple hops on a network, maintaining data protection by a reliable encryption mechanism is required. The data stored on a computer is susceptible to privacy breaches through the nodes in an IoT system due to the dynamic integration of services, applications, and networks. By modifying the data stored for illegal reasons, IoT devices will allow an attacker to affect data integrity.

### B. Authentication, Authorization, and Accounting

Authentication is required when two devices are communicating with each other to secure interaction in IoT. Due to the increasing heterogeneous systemic structures and ecosystems that sustain IoT schemes, a spectrum of IoT authentication mechanisms exists. Such environments raise a challenge in the identification of standard global authentication protocols of IoT-based devices. Additionally, the authorization processes ensure that access to systems or data is granted to those who are authorized. Successful integration of authorization and authentication assists in securing the communication environment. In addition, accounting and auditing, and monitoring of resource utilization provide a robust method for secure network management.

### C. Availability of Services

It is essential to have a sustainable structure for the IoT. Information procured in real-time that help add quality to the lives of end user, such as predicting the future, are provided by IoT services.

### D. Energy Efficiency

Generally, IoT systems are resource-constrained and feature limited power and capacity. Attacks on IoT networks may cause an increase in energy consumption by compromising the network and consuming IoT properties via redundant or fake service demands.

### E. Single Points of Failure

The exponential growth of IoT networks may contribute to the degradation of IoT services due to a heterogeneous structure. It involves creating a tamper-proof framework for a large number of IoT networks and the implementation of alternative strategies for a fault-tolerant network.

## VII. MAJOR SECURITY PROTOCOLS FOR IOT

Since there are many devices that connect different objects or items to each other intelligently, IoT still needs to integrate these tools, which use multiple communication protocols. The only way these smart devices can exchange data among themselves is through interaction. Protocols are important to define the spoken language of the IoT devices in terms of coordinating the messages exchanged between the linked devices, and to determine the correct limits that correspond to the different functions of each device. The popular features in all of modern IoT protocols and structural requirements are as follows.

### A. CoAP Protocol

CoAP is used to carry messages and transfer lost packets with high privacy. CoAP is designed to be light in both applications and in the network's use, making it more suitable for small and large devices in the IoT. CoAP and HTTP share the REST architecture and use methods to protect interconnected devices. CoAP protocol transmits data via IoT. It is designed to work on devices with limited resources. CoAP's goal is to find a way to transfer data safely and reliably. It is also designed to be simple, and the devices can use it as an alternative to the HTTP protocol, which makes it

an important protocol in IoT security. The four specific CoAP security modes are as follows [15]:

- 1) *NoSec*: Assumes that security was not provided in this mode or in the transferred CoAP message.
- 2) *PreSharedKey*: Enabled by pre-programmed hardware sensing using symmetric cipher keys.
- 3) *RawPublicKey*: Mandatory mode for devices requiring authentication. The devices are programmed with the list of keys previously available.
- 4) *Certificates*: Supports authentication and assumes security infrastructure is available. Hardware that has an asymmetric key can be validated and provides reliable keys.

### B. Message Queuing Telemetry Transport

Message Queuing Telemetry Transport (MQTT) is one of the most popular IoT protocols and is a convenient solution for embedded devices with limited and unlimited resources in the area of processing and storage capacity. It is a secure message transport protocol between the client and server in publish/subscribe mode. Light, open, and easy for implementation, it was designed specifically for the context of IoT applications in limited resource environments in the areas of energy, data exchange, and storage. The protocol offers benefits that reduce power consumption and bandwidth, both of which are very important factors in IoT devices. MQTT has three main parts, which are as follows [16]:

- 1) *The broker*: Responsible for managing the network from clients who are a mix of publishers and subscribers.
- 2) *The publisher*: The device that sends messages (posted) to the broker.
- 3) *A subscriber*: The device that listens to a specific topic.

There is no direct contact between the subscriber and the publisher. Rather, the subscriber simply informs the server that he is interested in specific topics and the broker will then send messages to the subscribers when they become available [18].

### C. IEEE 802.15.4

It is one of the protocols that define the operation of low-priced wireless personal networks. IEEE 802.15.4 protocol includes several advantages, such as offering support for securing communications in an integrated manner and for applications to handle sensitive data while ensuring their ability to work, in addition to real-time compatibility. IEEE 802.15.4-compliant devices use one of three operational frequency bands (868/915/2450 MHz) [17].

### D. 6LoWPAN

It combines Internet Protocol (IPv6) and Low Energy Personal Area Networks (LoWPAN). 6LoWPAN allows small devices with limited processors to transmit information wirelessly using the Internet Protocol [15].

### E. TLS Protocol

Transport Layer Security (TLS) is a protocol used to encrypt and provide a secure communication channel between two parties on the network during the exchange of data so that the data is encrypted to prevent any third party from disclosing

it or gaining unauthorized access within the IoT devices. This protocol is used to communicate over the network in a manner designed to prevent eavesdropping or tampering with the data being exchanged, as data is sent and received between the client and the server in conditions that prevent any party on the network from revealing what that data is or even tampering with it, since the software usually uses ports specially for safe communication [18].

TLS relies on trusted third-party certificate authorities. These are a group of entities that are considered authoritative references for issuing and authenticating protection certificates. These entities certify the protection certificates that TLS uses to encrypt data, which are distributed to IoT devices [18].

#### F. HomeKit Accessory Protocol

In 2014, Apple developed the HomeKit platform for iPhone and iPad users. Using the HomeKit Accessory Protocol (HAP) which was designed for Apple devices, things can be interconnected to wirelessly operate with voice commands using Apple's virtual assistant Siri. With HAP, lights, amplifiers, air conditioning, and other devices can be connected to IoT and managed through a single interface that works with voice commands; as soon as a voice command like "Sleep" is issued, dim lighting will be turned on, turning off the TVs, and locking the doors of the house [15].

HomeKit is a closed platform that is not open-source, so it is well-protected. Apple works with several companies to provide IoT solutions such as August, which produces smart door locks, and Philips, which makes lighting devices that can communicate with each other via IoT technology [18].

#### G. Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) aims to improve security on WEP. The standard that is currently used to ensure the protection of the IoT is WPA2. WPA2 uses a more robust encryption device to encrypt the IoT network. The length of the IoT code is an improvement of security over WEP. Organizations often enforce security by using a certificate-based system to authenticate the communication device using the 802.1X protocol [19].

#### H. RPL Protocol

Also known as the network layer protocol, the RPL protocol supports distance-vector routing for low-power networks using IPv6. Connected RPL internet network devices that support data transmission security and integrity. Link-layer mechanisms can be used in three basic safety modes [20]:

- 1) *Unsafe*: Allows RPL control messages to be sent without additional security.
- 2) *Pre-installed*: Applied by the device using identical keys that are pre-set to join the RPL protocol. The keys support integration, data authentication, and confidentiality.
- 3) *Authentication*: Compatible with routers associated with Internet devices. When a new device can join the IoT network, the key will authenticate and license the devices,

which can then join the rest of the connected devices in the network.

RPL is used in IoT systems to check the consistency of messages and the effectiveness of the response production in order to provide security against attacks by adding the version number and to route the data authentication system.

#### I. Thread Protocol

Thread provides a solution to the complexities of IoT technology in terms of operation and security. It is one of the low-power wireless protocols based on the IP.

Google, in cooperation with Samsung and other companies, introduced the Thread protocol to connect home appliances with limited resources to the IoT network. Thread works perfectly with Bluetooth and Zigbee to connect 250 home devices to one home network. The homeowner is then granted the ability to control these home appliances remotely via the IoT network. The Thread protocol also provides a high level of security by encrypting communication between devices by AES encryption, as well as being energy efficient. [21]

### VIII. IOT APPLICATIONS

Many applications work with IoT technology, the most important of which is the smartphone. This device acts as a connection point for many machines connected to the Internet; it is, hence, considered an IoT device. Additionally, wearable sports trackers are widely used by athletes and health-conscious individuals. Processing equipment, sensing, and communication processes have been added to many devices. Smart thermostats, smoke detectors, and security cameras can monitor human behaviour and help them accomplish their daily tasks.

#### A. Smart Home

The deployment of smart home technologies has been in widespread use in recent years. IoT technology controls smart home devices using wireless technology through the power supply system and the access control system. Smart homes are based on several devices inside a home connected via IP. This technology enables the control of any device in the house remotely and quickly via the Internet, which makes life more comfortable for people. This technology allows the collection and sharing of data between them at the same time. For example, AI devices that depend on capturing sound will know the music an individual prefers at a particular time of the day and play them automatically, such as quiet music at bedtime. The individual's watch will also check his/her daily task schedule and reset the alarm daily accordingly. Furthermore, when an individual wakes up from his/her sleep, the bathtub is prepared and filled with water that suits the person's body temperature, in accordance with reading taken from the smartwatch that the individual wears. Some examples of devices that support IoT technology in a smart home are listed below [22].

- 1) *Smart mirror*: A smart mirror consists of a transparent mirror and a screen behind the mirror connected via the internet. It displays essential updates such as the weather, the

calendar, news, social media notifications, and more, depending on the homeowner's lifestyle.

2) *Smart TVs*: These devices help the home owner monitor their home in their absence, which increases security against thieves. If the individual switches off the TV, it will fold up automatically to save space.

3) *Illumination intensity sensor*: It works by pre-setting its connection to the Internet and other devices through IoT technology. It balances the sun's natural lighting during the day from the weather application, calculates the intensity of the lighting, and automatically creates the appropriate lighting for the user according to the user's preferences.

4) *Smart alarms*: It works in conjunction with all devices that operate on the security and safety principle in the smart home, so it issues a high-frequency alarm and sends a text message to the user through the application to inform him/her of emergencies.

5) *Smart doors and windows*: A burglar alarm keeps doors, windows, and cupboard doors safe when homeowners are away. Furthermore, if a stranger opened it, a warning sound would be triggered, in addition to an alert message being sent to the user's phone.

**IoT security challenges in smart homes:** Despite the presence of smart home features, there are many security and privacy concerns. If this technology is exposed to a security breach by hackers, the entire house may be vulnerable to sabotage, leading to disruption of the system and the loss of personal information and items.

There are two main threats to smart homes: The first threat is that of hackers being able to access information and controlling home appliances remotely or stopping their functioning. The second is that the data on these devices can be stolen and used for unethical purposes. If pirates succeed in accessing home cameras or surveillance devices, they will be able to know when the houses are vacant and use this knowledge to conduct a robbery [23].

Smart home privacy are a sensitive issue, and is one of the highest priorities in the protection of IoT-based smart homes. Cyber-physical systems (CPSs) are used to protect these smart homes. These are engineering systems that include interaction between physical and computational components, which intersect with IoT-based technology by creating a complex network of devices. Consequently, the common denominator between CPS and IoT is that user privacy is the main issue. Both systems are concerned with creating a smart and secure home. Since both systems (CPS/IoT) are in widespread use, they attract many attackers and hackers [23].

ISPC is an essential technology for the protection of smart homes security and provide a high advantage for IoT device privacy. It is a scheme that aims to protect personal information on connected smart home devices. It has four levels of privacy that are classified according to the degree of sensitivity: high, medium, low, and unclassified. Each provides different levels of data access. Usually, there are levels for each user account or family members present in the smart home. For example, parents can access all of their

children's information that are registered on IoT-based devices and determine children's validity. ISPC technology is responsible for protecting devices connected to the IoT network and allows users the freedom to choose between these levels of privacy.

Privacy has been divided into two types, namely, fixed privacy and dynamic privacy. The former describes the personal information of smart home residents and their properties, while the latter refers to the information that we create and grows automatically, such as text messages, phone calls, and banking transactions. A type of data called derivative data is created through a dynamic parameter analysis process to build a user profile.

## B. Smart Healthcare

Over the past several years, IoT has changed healthcare in several ways, and continue to do so in the coming years. Some examples of devices that support IoT technology in the healthcare industry are listed below [24].

1) *Implantable glucose monitoring systems*: Patients with diabetes may have devices with sensors inserted in them, just under their skin. The sensors in the devices will transmit information to a patient's smartphone if their glucose levels become too low, along with prior documented data. In this way, patients will be able to determine when they are most likely to be in danger of low glucose levels.

2) *Medical alert system*: Users can wear objects that seem like jewellery, but are used to alert them of an emergency. For example, if an individual wears a medical alarm band and falls out of bed at night-time, whoever the users appoint to assist in an emergency would immediately be informed on their smartphones that the user needs their help.

3) *Wireless sensors*: In laboratories and hospital refrigerators, wireless sensors are used to confirm that blood samples, frozen drugs, and other medicinal products are maintained at the required temperatures.

4) *Location services*: Items such as wheelchairs, scales, defibrillators, nebulizers, pumps, or monitoring devices can be identified with IoT sensors and quickly located by healthcare personnel. Physical devices can be lost many times, and are challenging to trace, but with IoT-based technology, they can be located quickly and easily.

**IoT security challenges in smart healthcare:** There are growing problems, often intertwined, related to the regulatory structure in which healthcare technologies are manufactured. Most security problems are related to the nature of use. Although they are not unique to healthcare, they rely on three elements: data availability, maintaining reliable communication, and service access. Interruption of the network's operation and denial of service attacks can seriously affect healthcare delivery. It can also impact the protection of patients when connections are essential. Besides, a common defence-in-depth security measure is replication (replication of equipment, ready to be switched into a network). However, this replication is not generally realistic in healthcare, especially when devices are life-critical monitors or embedded devices [24, 25].

### C. Smart Cities

Smart cities could be considered a series of fields in city management like public lighting, city transportation, wastewater management, emergency services, and traffic control. However, new smart cities are likely to emerge as the available technologies become more widely accepted and more oriented toward unique use case requirements [25]. This paper will describe the IoT traffic camera.

1) *Smart transportation*: This smart service provides many benefits to the population. For example, smart transportation services enable people to avoid traffic congestion and accidents in the streets by collecting information about roads and traffic conditions using sensors and cameras on the roads and GPS technology. The control centre captures these signals and sends notifications to travellers on smartphones, radio channels, or map applications. This system helps the police to automatically regulate traffic by managing traffic lights as well as bus and bicycle routes [26].

2) *Smart energy*: This technology leverages power usage, electric car charging, smart grids, etc., by using broadly distributed sensors to track electricity supply storage, transmission, and consumption. It can reduce electricity usage, chances of power supply failure, and loss of individual electricity consumption [26].

3) *Smart tourism*: This feature helps to individuals obtain information about tourist cities. The system relies on cities' tourism infrastructure that is connected to the IoT network in order to implement tourism solutions. Furthermore, the system provides tourism management services such as customer relations management, operational city control, and local tourist market development using tourism information and development expectations. Smart tourism integrates with government agencies and the private sector to provide integrated data to enhance tourism [27].

**IoT security challenges in smart cities:** As cities aim to become "smarter", smart city technologies pose security and privacy challenges. As a model for information and networking, the smart city must protect the data engaged from unauthorized access, adjustment, examination, and destruction. The information, interaction, and physical environments should fulfil underlying security and privacy specifications like reliability, honesty, efficiency, and privacy. In addition to these general criteria, there are several other unique challenges with regards to the security of a smart city. A smart city collects sensitive private data, such as the habits and behaviours of citizens. Due to these particular features, security and privacy challenges are becoming difficult and preventing the smart city from being adequately attractive to facilitate greater use [28].

### D. Wearable Devices

IoT provides wearable technologies and devices that support activities and performance. This section seeks to define wearable Internet of Things (WIoT) and to discuss these systems' potential. Wearable body-area sensors (WBAS) are front-end components of WIoT and envelop the body to

capture central body data. WBASs are responsible for the following [29]:

- Utilizing sensors that capture user data and providing specialized data on the user's situation, preferences, and health status.
- Preparing data and sending it to the related devices through IoT technology to support analysis and decision-making.

One of the most common wearable devices is the smartwatch. A smartwatch offers many features to save time, such as receiving notifications and speedily controlling audio. It also operates independently from smartphones. Users can monitor their health, fitness status, and heart rate. Health metrics such as amount of burned calories, pulse rate, and heart rate can also be assessed. There are portable devices associated with motion sensors, which operate through algorithms and power control to measure activity and enable individuals to perform healthier activities.

These wearable devices represent opportunities for users to increase efficiency. However, the main challenges faced by WIoT devices are security concerns. Many wearable devices store data on the local device without encryption, which is considered a real problem. There is no biometric security, and there is no strong authentication to protect users' data. If the wrong hands fall into the data, security and privacy threats could be raised. Some third-party applications neglect basic security standards and send or store unencrypted information, which is the type of data that is automatically collected by wearables via the IoT technology.

During synchronization and data replication on cloud servers, there are security concerns. Wearable devices remain a priority for hackers. It is, therefore, important to prevent security flaws on these devices [30].

## IX. CHALLENGES IN IOT SECURITY

IoT networks face several challenges. These challenges are broadly divided into two: technology and security challenges. Key IoT security issues are from the complexity and the large scale of things. The researchers will address these security issues in more detail in this section [31].

### A. Security Challenges

Initially, companies focused on financial returns, so they rushed to keep pace with the market by deploying smart devices connected to the IoT network without providing adequate attention to security issues. Therefore, collection of user information was prioritized to raise the efficiency of devices to match their needs [31].

1) *Object identification*: One of the challenges in using data integration in naming architectures is the identification of objects. DNS provides a translation service for users of IoT. However, one of the disadvantages of DNS is that it is an insecure naming system. In contrast, it may be subject to multiple types of attacks, such as poisoning and man-in-the-middle attacks, which affect the determination of the accuracy between the naming structure and the addressing structure. A

botulism attack inserts fake DNS records into the victim's memory, and as such, the entire naming structure is insecure without data integrity protection. When sending a Domain Name Security Service Extension (DNSSEC, IETF RFC4033) as DNS security extensions, DNSSEC will ensure the trustworthiness and reliability of the Resource Record (RR). Thus, public cryptographic keys will be published. While DNSSEC is a naming service solution, proper implementation of DNSSEC in IoT is challenging due to the aspects of high data and communication processing costs.

2) *Authentication and authorization*: Public key cryptography is one of the essential features in building authentication or licensing schemes. The lack of a Global Root Certificate Authority (CA) prevents specific, potentially feasible systems from being implemented. It is becoming increasingly challenging to model an IoT authentication system without the Global Root CA. It could be difficult to issue a license to an IoT object since the total number of objects is indeed huge. Consequently, the concept of delegated verification and delegated approval must be taken into account for IoT.

3) *Privacy*: This type of issues can be categorized into two: data collection policy and data anonymization.

The data collection policy enforces the form of data to be obtained and the regulation of access to the data by IoT. The form and amount of information gathered during the data collection phase are limited through the data collection policy. Given that collection of private information and storage is restricted, privacy protection can be assured.

Anonymity is the other challenge in this categorization. To ensure data confidentiality, both, encryption protection and anonymization, of data relationships are used. Due to the variety of things, several cryptographic schemes may be implemented. For instance, lightweight cryptographic schemes are more suitable for resource-constrained devices. The dissimulation of a data relationship examines the elimination of direct data relationships with its user. Data encryption can be used to implement this approach. Nevertheless, information needs to be spread in IoT; thus, encrypted computing data is another barrier to data anonymization. Some research work in homomorphic encryption may be applied to address the problem. [31]

4) *Security protocols and lightweight cryptography*: Public-key cryptosystems offer greater security features than symmetric-key cryptosystems. However, it leads to high computational overload. Moreover, it often requires data authenticity to encrypt the public key. Therefore, among the major challenges in IoT security are the decrease in overhead computing systems relying on public-key cryptography and the complexity of security protocols.

5) *Software vulnerability and backdoor assessment*: Dynamic analysis is used to discover security vulnerabilities before the software is released. Dynamic research might be inefficient to implement in an IoT system due to resource constraints. Simulation can be used to duplicate machine

action in a database with more computational power to make dynamic analysis feasible. Nevertheless, a significant issue to address is the semantic distance between the actual computer and the replicated system. It is hard to avoid the inconsistency between computer and replicated systems. Various elements, including GPS and sensor in a system, make it even harder to narrow the distance. Many analysis methods are strongly reliant on the system underlying it, such as taint analysis and symbolic execution. An analytics program must be versatile enough to consider different frameworks with highly diversified conditions. In addition, a good interface and the intermediate layer must be established to split system dependence. Therefore, to adopt a range of systems, extensibility can be obtained. The dynamic analytics approach is also a successful way to remove backdoors. However, it is not just a technical problem. It also plays an essential role in both management and policies. Multilevel analysis to reduce system flaws, reverse engineering discovery of backdoors, and system auditing helps prevent backdoor use.

6) *Malware in IoT*: As already mentioned, due to the limited assets of IoT systems, the threat of IoT-targeted malware is high. Furthermore, traditional malware security mechanisms can be impossible when moving straight from the standard x86 architecture systems to the IoT system. For example, antiviruses are considered one of the most effective security tools in the real-time model for identifying known malware. However, unlike the x86-architecture PC, the IoT systems have relatively little computing power. Antivirus's real-time scanning feature can lead to an inexpensive overhead for IoT systems. Meanwhile, malware developers will develop their malware into the separate downloader and the main body, given IoT's processing power concerns. The downloader has a small software body as a pioneer in infecting all IoT networks, thereby humiliating the retrieval of its unique, dangerous signature. Besides the above case, other problems exist, such as the differentiation of physical frameworks between different devices. Without a current IoT malware specification, existing approaches and strategies can be ad-hoc and impossible to enforce [31].

7) *Unsecured public cloud infrastructure & untrusted cloud service provider*: It is the integration of most information security areas such as network security, systems security, and application security related to the IoT network and the devices linked to each other. The protection of user data that is available on the cloud service provider involves protecting and separating the data is from mixing between users and storing safely. The data should be able to move securely from one location to another. Further, the data must be encrypted according to the best encryption technology [20].

8) *Data leak in transmission*: Data leakage in IoT technology occurs when sensitive data is accidentally exposed on the Internet. This means that cybercriminals can gain unauthorized access to sensitive data and personal devices associated with the IoT. Data leaks stem from bad data security practices or individual failure [16].

## B. Technological Challenges

Due to the various methods for running IoT systems, technology difficulties emerge, and security issues are linked to innovations and features applied to achieve safe internet connectivity. Wireless networks, distributed devices, and nature are frequently correlated with technological problems [11].

## X. CATEGORIZATION OF SECURITY ISSUES

Since IoT architecture involves a wide variety of devices and hardware, from small, embedded processing to massive high-end databases, it is essential to fix security vulnerabilities at different levels. The classification of the security risks to the IoT installation architecture are listed below [32].

### A. Low-Level Security Issues

As described below, the first level of security concern is at the interaction layers of physical and data connections [31].

1) *Enemy jamming*: Jamming attacks on smart devices target network failure by sending radio frequency signals without adopting a specific protocol.

2) *Low-level sybil and spoofing attacks*: Sybil attacks are triggered by fraudulent Sybil nodes in a wireless network that use fake names to compromise IoT features. A Sybil node may use randomly fabricated MAC values on the physical layer to masquerade as a different device, thus minimizing network resources. Legitimate nodes may ultimately be refused access to resources.

3) *Insecure physical interface*: Many physical factors intensify threats to IoT functions. The protection ratio of the IoT application can be manipulated and access to physical hardware systems can be controlled via software interfaces to overcome this problem.

4) *Sleep deprivation attack*: The danger of this attack is that the sensor nodes remain awake. This causes battery depletion when running a large number of functions to be executed in the 6LoWPAN environment, thus shortening battery life.

### B. Intermediate-Level Security Issues

Mid-level IoT security issues relate to the communications, transport and network layer, as mentioned below [29].

1) *Transport level end-to-end security*: Provides a secure approach to efficiently receiving data from the sender node by the desired endpoint node. This approach requires authentication mechanisms that ensure secure communication of encrypted messages in complete privacy, with minimal overhead.

2) *Buffer reservation attack*: Since a receiving node needs reserving buffer storage to reassemble arriving packets, it may be abused by an attacker, who may send unfinished parcels to it. Discarding of other fracture packets are discarded due to the space being filled up by the incomplete packets from the intruder results in denial of service.

3) *Privacy violation in cloud-based IoT*: Multiple attacks that may infringe identification and position security could be conducted on a cloud-based or delay-tolerant IoT network. Similarly, a fraudulent cloud service company focused on IoT implementation can control sensitive information forwarded to the desired location.

4) *Replay or duplication attacks due to fragmentation*: For devices that conform to the IEEE 802.15.4 standard, which is defined with small frame sizes, fragmentation of IPv6 packets is necessary. A rebuilding of the packet fragment areas at the 6LoW- PAN layer can lead to resource depletion, buffer overflows, and devices restarting. The duplicate fragments sent by malicious nodes impact the packet's reassembly and thus impede the processing of other legal packets.

### C. High-Level Security Issues

High-level security issues are associated with IoT applications, as mentioned below [32].

1) *Insecure interfaces*: To access IoT resources, device and cloud-based interfaces are subject to various attacks that can seriously affect data protection.

2) *Insecure software/firmware*: Numerous IoT vulnerabilities include those generated by unsafe firmware/software. Careful testing of code with languages such as JSON, XML, SQLi, and XSS is required. Likewise, operating system/firmware updates must be executed securely.

3) *Middleware security*: The IoT middleware built to make communication between IoT model heterogeneous entities sufficiently safe for service delivery. To ensure secure communication, various interfaces and environments must be integrated using middleware.

## XI. DIFFERENT MECHANISMS FOR ENSURING IoT SECURITY

Different methods can be adopted to ensure the security of IoT devices, as listed below [33]:

- For authorized users, the applications in all computers connected to the IoT network must be authorized for permitted users.
- When operating the IoT device, it must authenticate the network data before sending the data over to the devices.
- The use of a firewall is essential in applying IoT technology to ensure packets' integrity from attacks and penetration.
- Updates must be installed in the devices through secure protocols to secure communication between users, programs, things, and related processes.

## XII. IoT SECURITY SOLUTIONS

Business investment in IoT-based security has increased in recent years. Table II shows some security tools and solutions offered by different companies for IoT networks [34].

TABLE II. SECURITY SOLUTIONS

Company	Description
Cisco	Provides security solutions for IoT. Collects & automates data management with IoT. Cisco engineers have been the leaders in developing networking technologies based on the IP.
Bitdefender BOX	Provides protection for the whole home network and for all IoT devices. It also deactivates viruses, stolen keys, identity theft, and hacker attacks on all networked computers that are used in a VPN, even those that do not have a local anti-virus built into them.
ZingBox	A cloud-based cost-efficient IoT solution that provides IoT networks with secure infrastructure. Provides applications to solve the complexity of the IoT.
Subex	Covering real-time reaction and monitoring recovery. It is a leading supplier of software solutions, working through its security offerings on the IoT, including an IoT security solution, VAPT, managed services, and advisory services, to ensure a stable digital business future. Helps secure companies' systems reliably to protect them from security threats.
Kaspersky	Due to the need to protect IoT-based technologies, Kaspersky Lab initiated a trusted release of its Kaspersky Internet of Things Threat Data Feed that provides detailed data on IoT threats that affect security.

#### A. Solutions Provided by Edge Computing to Overcome IoT Security Risks

Edge computing serves or may provide solutions to IoT security risks, as discussed below.

**The threat of the man-in-the-middle:** The edge acts as a security layer between the end user and the cloud or the IoT platform. Any risks or attacks on the IoT system must pass the fog layer in between. This layer will detect and prevent suspicious activities before they are forwarded over the device.

**Incident response services:** Edge devices can be configured in order to provide incident response services in real-time. As soon as unusual data or queries are observed, fog nodes will trigger a flag for the IoT device or end users. Edge computing facilitates the identification of malware and problem-solving in transit. It might not be necessary to interrupt the whole device to address malware incidents in specific sensitive applications. Edge devices will assist in such solutions when the device is fully operational [35].

#### B. Solutions Provided by Blockchain to Overcome IoT Security

The industry and the academic community have anticipated blockchain technology as a promising technology capable of playing an essential role in managing, controlling, and critically protecting IoT systems. This section explains how blockchain could be an essential tool in enabling the delivery of possible solutions for IoT security issues. Some of blockchain's essential functions that are of enormous use to

IoT in general and IoT security in particular are outlined and addressed in this section as well [32].

1) *Address space:* Compared to the IPv6 address space, which has an address space of 128 bits, blockchain has 160 bits. A 20-byte blockchain address is a 160-bit public key hash created by Elliptic Curve Digital Signature Algorithm (ECDSA). For roughly  $1.46 \times 10^{48}$  IoT devices with 160-bit addresses, blockchain will attract and delegate disconnected addresses. An address crash risk is around 1048, which is assumed to be sufficiently secure to obtain a Global Unique Identifier (GUID) while assigning and allocating an address to an IoT system that does not require registration or recognition of uniqueness. Unified authority and leadership were eliminated with blockchain, such as that of the Internet Assigned Numbers Authority (IANA). Currently, IANA handles worldwide IPv4 and IPv6 address delivery. In addition, blockchain provides 4.3 billion additional addresses more than IPv6, making blockchain an IoT solution that is more scalable than IPv6. Finally, it is necessary to note that many IoT systems are restricted in terms of memory and processing capacity and are not ideal for operating an IPv6 stack [32].

2) *Authentication and data integrity:* The data sent by IoT connected devices to the blockchain system are always proved to be cryptographically and agreed to be signed by the real sender, which has a unique key and GUID, thereby guaranteeing the authentication and validity of the transmitted data. Additionally, all operations performed on or through an IoT machine are documented on the blockchain and monitored securely [20].

3) *Secure communications:* Protocols for IoT communication, such as HTTP, MQTT, CoAP, XMPP, and routing protocols, such as RPL and 6LoWPAN, have not designed securely. These need to be covered in other security protocols, such as DTLS or TLS, to ensure safe interaction. Similarly, for RPL and 6LoWPAN protocols, IPSec generally provides protection. In processing and memory requirements, DTLS, TLS, IPSec, or the lightweight TinyTLS protocols are weighty, difficult, and complicated with unified key control and management and transmission using the standard PKI protocol.

Key control and distribution are omitted for the blockchain. Once enabled and linked to the blockchain network, each IoT device will have its unique guide and asymmetric key pair. This results in significant simplification of other security protocols such as DTLS, without the need for handshake-handling and PKI-sharing for DTLS or TLS (or IKE in IPSec). and for the main and session keys to be configured. Lightweight security protocols that would fit the specifications and memory properties of IoT devices are, therefore, possible [32].

4) *Authentication, authorization, and privacy:* Blockchain smart networks can provide single and multi-party authentication for an IoT device with de-centralized authentication principles and logic.

Involving far less complexity than standard authorization protocols such as OAuth 2.0, OpenID, RBAC, LWM2M, and OMA-DM, intelligent networks can provide more effective authorization controls for IoT systems. As a result, intelligent protocols are widely used for the authentication, authorization, and control of IoT systems. In conjunction, data protection can also be maintained by using smart networks that set standards, limitations, and time limits for access to allow certain groups or individual users to own, track, or access data while resting or traveling [36]. The smart network can also determine who is allowed to upgrade, update, patch the IoT hardware/software, restore the IoT device, include new key pairs, trigger a service or maintenance request, change ownership, and supply or replenish the device [32].

5) *Blockchain vulnerabilities*: Although the blockchain systems have robust frameworks for protecting IoT networks, some vulnerabilities still exist.

It is possible to manipulate private keys with limited randomness to breach blockchain records. Effective systems also need to be developed to assure the security of transactions and the elimination of various attacks [32].

### XIII. FINDINGS

The current Internet of Things systems have shown their effectiveness through their ability to communicate with connected devices, which makes life more efficient. However, connecting multiple devices via the Internet poses a tremendous security challenge, as it has become a significant target for hackers. The wide field of the Internet of Things poses a greater risk on users' privacy. Also, the similarity in the protocols used on identical IoT devices increases security vulnerabilities. This calls for looking at tools and technologies associated with IoT security.

With the advancement of cyberattacks, research into security risks that change over time must be continued to create security solutions commensurate with the security problem's size. Companies must continuously update their applications because continuous updates help reduce changes in the systems, and thus the chances of cyber-attacks are reduced. The development of awareness guides contributes to raising the percentage of security awareness, as organizations can establish training and awareness programs to enhance security awareness. Some research papers suggested developing tools for monitoring devices. The monitoring tools detect unusual or harmful activities and assess the risks. All of these technologies contribute to developing the security of Internet of things applications.

### XIV. DISCUSSIONS

Most people own devices associated with the technology of the IoT. For example, mobile devices in their smart homes and blood sugar monitoring devices in smart healthcare. It has become easy to distribute and publish information via IoT devices.

This review illustrates one of the most critical problems facing the application of IoT with regards to data privacy and security. These devices show some security weaknesses

caused by specific threats such as unauthorized access, privacy breaches, and systems sabotage.

The increase in the usage of the Internet has helped organizations stay up-to-date with new developments and with essential support to run their business, and efficiently and rapidly acquire information. However, at the same time, this distributed information has made it easy to obtain, infiltrate, and manipulate and misuse. It also enables the likelihood of security incidents with IoT. An enhanced understanding of the current value of information security may reduce the rate of such incidents. Therefore, raising security awareness is an important aspect of the solution for these issue [37].

The security of IoT devices is part of emergency management. Security systems function by detecting the most critical vulnerabilities in the IoT device and the areas where the users are exposed, such as malware, extraction of user information, and destruction of networks. Unfortunately, there is the concern of not implementing security policies to the Internet of Things usage because some businesses did not identify their devices' information security policies from the beginning. That further puts them in many difficulties when enforcing these security policies to minimize the negative actions. The value of information security policies is often overlooked by users, which leads to formulating security policies without actually applying them to practice.

Business investment in IoT devices will continue to grow in the future as the advanced technology sector advances, consequently increasing business opportunities and making life easier for individuals. IoT security will experience a great deal of development, such as control of unauthorized access, trust management, and the implementation of specific policies and global standards, by better defining the authorized user's identity when accessing wireless devices and software.

This research has shown that leaders of information technology organizations who support the security of the IoT are trying to increase security and reduce vulnerabilities by making various efforts.

### XV. FUTURE WORKS

In this section, some of the promising future research directions will be discussed.

The possibilities for integrating different security approaches within IoT-based applications, including privacy-preservation machine learning (PPML) techniques, should be explored. Therefore, more research should be conducted on PPML techniques within IoT-based devices, which would provide a high degree of protection and ease of use at the same time.

We must aspire to develop a dynamic framework to support security and adapt to new IoT technologies' continuous research changes in the future.

### XVI. CONCLUSION

IoT poses many challenges that must be considered and addressed before widespread implementation. Security and privacy challenges are among the most critical problems for

IoT devices, which must necessarily be addressed to ensure the safety and integrity user information.

This study primarily focused on IoT security due to the vast developments in IoT of late. The research was extended to include industries, such as the healthcare sector, which requires strong privacy protection.

This paper focused on the applications that used IoT technology the most, namely, smart cities, smart homes, and smart healthcare, along with their security challenges. Furthermore, an overview of the various security tools and solutions to the IoT was provided. In addition, IoT security along with its more comprehensive and varied aspects was discussed by providing an overview of common issues and different security solutions. The IoT's hierarchical structure, the value and advantages of IoT-based technology, and the most important protection protocols used to secure data were covered. Blockchain and edge computing technology's role in providing modern solutions to IoT security was also highlighted.

Through this review, several recommendations can be made that contribute to developing IoT security.

Users' IoT security awareness must be increased to minimize security breaches. Users must also be responsible for protecting their own devices by following several steps, such as adopting protection systems for the home network, constantly updating systems, avoiding phishing sites, and continually changing the passwords for the devices connected to other devices through IoT-based technology.

When purchasing IoT devices, users should choose reliable and expert sellers. Even though devices from these sellers are expensive, they support the best protection systems. The user must also verify the protection protocols that the device supports and the manufacturer's privacy policy.

Governments must provide advanced IoT security solutions, develop security policies to counter security threats, and apply penalties for hackers of IoT-based devices.

In future studies, the researchers recommend using modern tools and algorithms to develop an IoT environment equipped with more secure technologies through the participation of information technology security professionals and to study the effectiveness of new technologies and their ability to maintain data confidentiality.

At the end of the research, it can be concluded that IoT networks are vulnerable to many attacks. Accordingly, many security requirements must be applied. IoT technologies facilitate our life. Therefore, achieving security and confidentiality is an issue of critical importance.

#### REFERENCES

- [1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010, doi: 10.1016/j.comnet.2010.05.010.
- [2] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," 2016 14th Annu. Conf. Privacy, Secur. Trust. PST 2016, pp. 219–222, 2016, doi: 10.1109/PST.2016.7906930.
- [3] K. Sha, R. Errabelly, W. Wei, T. A. Yang, and Z. Wang, "EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security," *Proc. - 2017 IEEE 1st Int. Conf. Fog Edge Comput. IC FEC 2017*, pp. 81–88, 2017, doi: 10.1109/ICFEC.2017.7.
- [4] W. Wei, A. T. Yang, and W. Shi, "Security in Internet of Things: Opportunities and Challenges," *Proc. - 2016 Int. Conf. Identification, Inf. Knowl. Internet Things, IIKI 2016*, vol. 2018-Janua, pp. 512–518, 2018, doi: 10.1109/IKI.2016.35.
- [5] E. Sahinaslan, "On the internet of things: Security, threat and control," *AIP Conf. Proc.*, vol. 2086, no. April, 2019, doi: 10.1063/1.5095120.
- [6] J. Wurm, K. Hoang, O. Arias, A. R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," *Proc. Asia South Pacific Des. Autom. Conf. ASP-DAC*, vol. 25-28-Janu, pp. 519–524, 2016, doi: 10.1109/ASP-DAC.2016.7428064.
- [7] A. K. Pathak, "Security Challenges in Internet of Things (IoT)," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 6, pp. 648–652, 2017, doi: 10.23956/ijarsse/v7i6/0185.
- [8] C. Liu, Y. Zhang, and H. Zhang, "A novel approach to IoT security based on immunology," *Proc. - 9th Int. Conf. Comput. Intell. Secur. CIS 2013*, pp. 771–775, 2013, doi: 10.1109/CIS.2013.168.
- [9] H. Derhamy, J. Eliasson, J. Delsing, and P. Priller, "A survey of commercial frameworks for the Internet of Things," *IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA*, vol. 2015-October, 2015, doi: 10.1109/ETFA.2015.7301661.
- [10] E. Fleisch, "What is the Internet of Things? An Economic Perspective What is the Internet of Things - An Economic Perspective," *Econ. Manag. Financ. Mark.*, vol. 5, no. 2, pp. 125–157, 2010, [Online]. Available: [www.autoidlabs.org](http://www.autoidlabs.org).
- [11] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015, pp. 336–341, 2016, doi: 10.1109/ICITST.2015.7412116.
- [12] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/9324035.
- [13] K. Patel and Keyur, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges..," *Univ. Iberoam. Ciudad México*, no. May, 2016, [Online]. Available: <http://ijesc.org/>.
- [14] V. K. B., S. L. Joshi, and S. H. Barshikar, "SURVEY ON INTERNET OF THINGS (IOT) SECURITY ISSUES & SOLUTIONS," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 12, pp. 492–496, 2018, doi: 10.26438/ijcse/v6i12.492496.
- [15] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," 2016 3rd MEC Int. Conf. Big Data Smart City, ICBDS-C 2016, pp. 172–178, 2016, doi: 10.1109/ICBDSC.2016.7460363.
- [16] M. Kashyap, V. Sharma, and N. Gupta, "Taking MQTT and NodeMcu to IOT: Communication in Internet of Things," *Procedia Comput. Sci.*, vol. 132, no. Iccids, pp. 1611–1618, 2018, doi: 10.1016/j.procs.2018.05.126.
- [17] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, 2017, doi: 10.1109/JIOT.2017.2683200.
- [18] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015, doi: 10.1109/COMST.2015.2388550.
- [19] Y. R. Li and G. Y. Wei, "A research on IPv6 address auto-configuration for IoT," *ACM Int. Conf. Proceeding Ser.*, pp. 11–15, 2018, doi: 10.1145/3291842.3291901.
- [20] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors (Switzerland)*, vol. 20, no. 13, pp. 1–20, 2020, doi: 10.3390/s20133625.
- [21] M. R. Palatella et al., "Standardized protocol stack for the internet of (important) things," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013, doi: 10.1109/SURV.2012.111412.00158.

- [22] H. Ning and Z. Wang, "Future IoT Architecture - Like Mankind Neural System or Social Organizaition Framework.pdf," *Ieee Commun. Lett.*, vol. 15, no. 4, pp. 461–463, 2011.
- [23] K. Aloufi, A. Alharbi, A. Redwan, and Y. Abutarboush, "Web Based Access Control of Smart Home Security System," no. December, 2019.
- [24] G. J. Joyia, R. M. Liaqat, A. Farooq, and S. Rehman, "Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain," *J. Commun.*, vol. 12, no. 4, pp. 240–247, 2017, doi: 10.12720/jcm.12.4.240-247.
- [25] P. A. H. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," 2016 IEEE 3rd World Forum Internet Things, WF-IoT 2016, pp. 30–35, 2017, doi: 10.1109/WF-IoT.2016.7845455.
- [26] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, 2017, doi: 10.1109/MCOM.2017.1600267CM.
- [27] K. Su, J. Li, and H. Fu, "Smart city and the applications," 2011 Int. Conf. Electron. Commun. Control. ICECC 2011 - Proc., pp. 1028–1031, 2011, doi: 10.1109/ICECC.2011.6066743.
- [28] D. Eckhoff and I. Wagner, "Privacy in the Smart City - Applications, Technologies, Challenges, and Solutions," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 489–516, 2018, doi: 10.1109/COMST.2017.2748998.
- [29] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, 2018, doi: 10.1016/j.jisa.2017.11.002.
- [30] S. Hiremath, G. Yang, and K. Mankodiya, "Wearable Internet of Things: Concept, Architectural Components and Promises for Person-Centered Healthcare," pp. 1–4, 2014, doi: 10.4108/icst.mobihealth.2014.257440.
- [31] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," *Proc. - IEEE 7th Int. Conf. Serv. Comput. Appl. SOCA 2014*, pp. 230–234, 2014, doi: 10.1109/SOCA.2014.58.
- [32] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.
- [33] M. Ganzha, M. Paprzycki, W. Pawlowski, P. Szmaja, and K. Wasielewska, "Semantic technologies for the IoT - An Inter-IoT perspective," *Proc. - 2016 IEEE 1st Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2016*, pp. 271–276, 2016, doi: 10.1109/IoTDI.2015.22.
- [34] M. Yamashita, H. Ishihara, M. Kudo, A. Matsuki, and T. Oyama, "A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches," *Acta Anaesthesiol. Scand.*, vol. 28, no. 3, pp. 331–333, 1984, doi: 10.1111/j.1399-6576.1984.tb02071.x.
- [35] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
- [36] N. Tyler, "Securing the internet of things," *New Electron.*, vol. 48, no. 6, pp. 30–31, 2015.
- [37] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.
- [38] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012, doi: 10.1109/ICCSEE.2012.373.
- [39] M. A. Burhanuddin, A. A. J. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, "A review on security challenges and features in wireless sensor networks: IoT perspective," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, no. 1–7, pp. 17–21, 2018.
- [40] Y. Perwej, F. Parwej, M. M. Mohamed Hassan, and N. Akhtar, "The Internet-of-Things (IoT) Security: A Technological Perspective and Review," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 5, no. 1, pp. 462–482, 2019, doi: 10.32628/cseit195193.
- [41] A. Sultan, M. A. Mushtaq, and M. Abubakar, "IoT security issues via blockchain: A review paper," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1481, pp. 60–65, 2019, doi: 10.1145/3320154.3320163.
- [42] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–6, 2019, doi: 10.1109/CAIS.2019.8769560.

# Customer Retention: Detecting Churners in Telecoms Industry using Data Mining Techniques

Mahmoud Ewieda<sup>1</sup>  
Business Information Systems  
Helwan University  
Helwan, Egypt

Essam M Shaaban<sup>2</sup>  
Business Technology Department  
Canadian International College School  
of Business Technology Department  
Cairo, Egypt

Mohamed Roushdy<sup>3</sup>  
Faculty of Computers and Information  
Technology, Future University in Egypt  
New Cairo, Cairo, Egypt

**Abstract**—Customers are more concerned with the quality of services that companies can provide. Customer churn is the percentage of service for subscribers, who stop their subscriptions or the proportion of customers, who discontinue using the product of the firm or service within a given time frame. Services by various service providers or sellers are not very distinct that raise rivalry between firms to maintain the quality of their services and upgrade them. This paper aims at manifesting the service quality effect on customer satisfaction and churn prediction to reveal customers who have meant to leave a service. Predictive models can give the extent of the service quality effect on customer satisfaction for the correct determination of possible churners shortly for the provision of a retention solution. This paper analyses the impact of service quality and prediction models that depend on data mining (DM) techniques. The present model contains five steps: data-pre-processing, feature selection, sampling of data, training our classifier, testing for prediction, and output of prediction. A data set with 17 attributes and 5000 records used - which consist of 75% training the model and 25% testing- are randomly selected. The DM techniques applied in this paper are Boruta algorithm, C5.0, Neural Network, Support Vector Machine, and random forest via open-source software R and WEKA.

**Keywords**—Quality of service; churn prediction; classification; data mining; prediction model; customer retention

## I. INTRODUCTION

In the world of works, customers are the source of gain and revenue for the service of organizations and improvements in QoS that lead to customer loyalty. Organizations become increasingly customer-focused and meet their requirements. QoS is a very effective factor as it becomes equal difficult to please and preserve customers. Research indicates that both QoS and customer satisfaction are distinctive structures but effectively related. This is especially true for companies' service where a higher level of customer satisfaction leads to higher profits [1]. Those facts eventually focus on predicting customer churn as a necessary part of the Communication firms' procedures and decisions, which are the major goal of customer relationship management (CRM) also. The increasing of importance of this tool has led to the enhancement of many predicting tools that reinforce some pivotal tasks in the predictive modeling and operations of classification [2]. Identifying a predicted churn is a beneficial tool to predict a customer in danger of churn. In general, service providers are blamed for poor quality, but the real

problem is the design of the service system. Predicting the level of service, good service planning, and knowing customer behavior and desires are way to improve the QoS [1]. The purpose of churn management is to decrease the loss of subscribers generally since subscribers raise profits by handing over a stable and profitable customer basis. [3]. Most Data Mining (DM) techniques play a very substantial role in telecom firms to enhance their marketing efforts, identify a scam, manage their telecom networks, demographic data, behavioral data, and many disciplines [4]. DM techniques are set in telecoms for CRM due to the fast growth of the huge quantity of data, high speed in the market rivalry, and rise in the churn rate. DM techniques can be used in the classification, clustering of customer data to predict churners. And have affected Genetic Algorithms (GA), Fuzzy Logic (FL), Random Forest (RF), Decision Tree (DT), Support Vector Machine (SVM), and Neural Networks (NN) [5].

This paper is organized as follows: Section 2 demonstrates the definition of the impact of service quality on customer satisfaction. This section presents, also, the concept of churn prediction, and shows the types of churners. Section 3 gives an overview of DM techniques and used algorithms. While Section 4 describes the proposed model for churn prediction; in addition to the results proceed of a case study. Finally; the conclusion and future work.

## II. IMPACT OF SERVICE QUALITY ON CUSTOMER SATISFACTION

1) *Quality of services and Customer Satisfaction*: QoS can be explained as superiority, measuring the ability of the service that reaches the customer and corresponds to his expectations. Also, it means that the organization's designs deliver the service correctly. Moreover, it enjoys competitive advantages. Perfect QoS leads to the retention of current customers, reduced costs, in addition to reinforcing customers 'loyalty' [6]. Customer satisfaction is a measure of the range of products and services that a company provides to meet customer expectations. Noticed, noticeable emergence of the term customer satisfaction, especially the increasing numbers of business organizations operating in the same sector with the expansion of local and global markets [7], [1].

2) *Churn prediction and customer retention*: Churn's prediction is used to identify potential churners, before they

leave the firm. This helps CRM to prevent potential customers from leaving the company, in the future, via retention policies. Thus, the loss possibility of the firm can be averting [8]. In telecoms-based industries, companies supply customers with rewards to tempt them into switching to their services. Toward off this, the firm must grasp the reasons why the customer decides to depart to another telecom firm [9].

Customer retention is the primary goal of the CRM. It is taken to ensure customer loyalty and reduce churn to move to serve supporters for higher quality, better offers, or more advantages. For this target, churn prediction is an essential part of a proactive scheme to retain a customer [8], [9].

3) *Type of churners there are two types of churners:* voluntary and involuntary churners. Voluntary churn happens as a result of a customer's resolution to moving into another service provider or another company. Involuntary churn happens because of conditions, as a customer moving to longtime care, death, or moving to a remote place. Involuntary churners are considered the easiest type of churners to determine. The company can decide to exclude them from the subscribers' list. This denomination includes people, who are churned for the scam, not paying, not using the phone [3]. Voluntary churn can be split into two primary classes: "incidental" and "deliberate" churn. Incidental churn happens not for the customers' intention but the actual reason lies in something that has happened in their lifetimes. For example, Change in the financial situation, location. Deliberate change occurring technological reasons; customers wanting new or better technology, economy, price fluctuation, dissatisfaction with the QoS factors, too high prices, no rewarding for customer loyalty, bad support, Social or psychological elements, and/or amenities. Deliberate churn is the issue that the churn department tries to get for solutions (Fig. 1) [3]-[10].

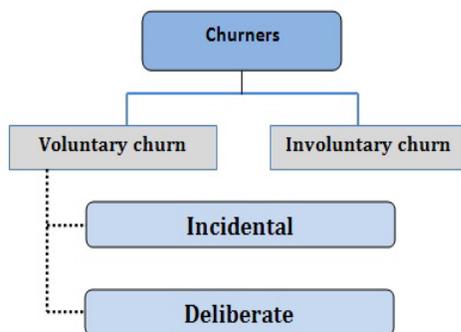


Fig. 1. Churn Classification.

### III. DATA MINING TECHNIQUES

Data mining looks for hidden and unexpected information, such as the optimum classification for customers. DM looks, also, unimportant trends and beneficial patterns in large data sets. DM relates to discovering unexpected or previously-unknown relationships between data. It is a multidisciplinary skill that uses machine learning, statistics, artificial intelligence technology, and database. Numerous main data

mining technologies are enhanced and used in recent DM projects, such as association, classification, clustering, prediction, sequential patterns, and decision tree [10], [11].

1) *The neural network:* The neural network is a group of connected (I /O) input/output units and each communicates with a weight. Through the learning stage, the net learns by tuning weights even predicts correct row classifications for input groups. The NN has a noteworthy ability to extract meaning from complex or inaccurate data and can be used to extract patterns and reveal very complex directions that cannot be observed by humans, or computer technologies e.g., computer training to vocalize English text after reorganizing handwritten letters [9].

2) *Random forest:* Random forest is considered to be one of the most powerful techniques of machine learning, it almost does not need any data preparation or any modeling experiences, and it is, also, considered as a tool that embodies the power of decision trees in addition to wise randomness and collective learning to produce accurate predictive models, insightful classifications of the values of lost, and new divisions, to help understand the deepest data [11].

3) *Support vector machine:* Support vector machine is a powerful supervised learning method for regression and classification problems that makes expectations via a linear combination of kernel basis functions. SVM is an implementation of the structural risk minimization (SRM) principles which attempt to minimize an upper bound of the generalization error instead of minimizing the empirical error. Depending on these transformations to find the optimum border between the possible outputs; simply, they perform some very complex data conversions, then they reveal how data is separated based on the labels or outputs that are specified [12].

4) *The decision tree:* The decision tree is the technique of the most communally DM techniques where its model is very easy to grasp and realize for users. DT is a model that breeds a structure as the shape of a tree that exemplifies a group of decisions. The DT root is an easy question or status that has various answers. All answers lead to a set of questions or situations that help determine the data to be able to make the final decision. The decision trees are created by the C5.0 algorithm work almost well, but are easy to understand and spread [13].

### IV. PROPOSED MODEL

The suggested model consists of many steps: the first step is to define the problem and data selection, the next step is data pre-processing (data transformation, data cleaning), the next step is feature selection. Feature selection methods are used to eject the iterative and not relevant features that do not contribute significantly to predict performance. The next step sampling stage, represented in the training set, is applied to train our classifier; Moreover, a predicting model builds to be ripe for testing. The last step is the performance and accuracy evaluation, the prediction Outputs and Results. Fig. 2 shows the proposed churn prediction model.

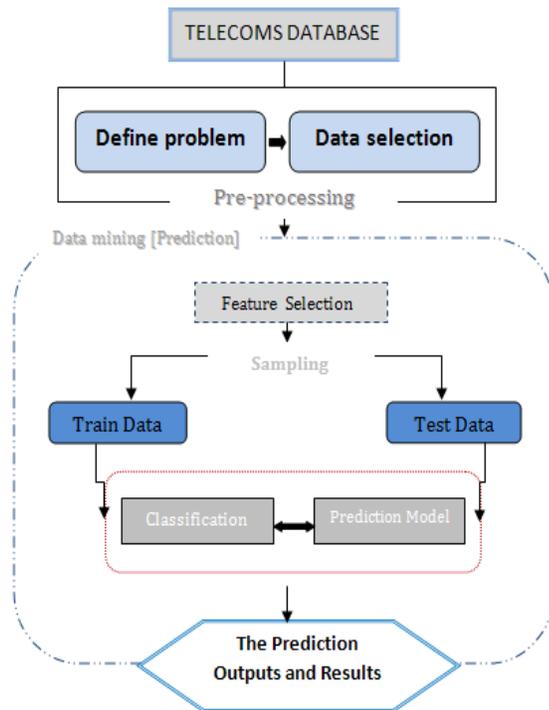


Fig. 2. The Proposed Churn Prediction Model.

1) *The initial stride:* Prior to applying specific analytical models to the data, which is previously prepared to be more appropriate for the analysis, by defining the problem, data selection, and analyzing data explicatory?

2) *Preparing data:* The data, used in this study, is a telecom company database containing a set of statistical data for customers that are 17 illustrative features regarding the use of customers' service daytime, Intl-calls, and customer-service-calls 14.14% of notes have a variable target of "true", and 85.86% of notes have a "false" value. Viewing data set variables of "customer transactions", and their characterization

is manifested in Fig. 3, and Table I demonstrates the distribution of every feature and describing a set of data.

Description of the quantiles of a data set is the numbers whose percentiles are the quarter marks of the data set. Specifically, they are the values in the data set that are at 1%, 25%, 50%, 75%, and 90% these are also known as a quartile, mean usually what one means by an average - the sum of dataset, mean usually what one means by an average - the sum of dataset. Standard Deviation (sd) contains percentiles of the measurements, mad = the median absolute deviation (from the median), trimmed = a trimmed mean (by default in this function, this removes the top and bottom 10% from the data, then computes the mean of the remaining values - the middle 80% of the full data set), The range of a quantitative variable is interpreted as the difference between the (maximum (max)and the minimum(min)), a measure of skew, which refers to how much asymmetry is present in the shape of the distribution. a measure of excess kurtosis, which refers to how outlier-prone, or heavy-tailed the shape of the distribution is, as compared to a Normal distribution, se = the standard error of the sample mean, equal to the sample (sd) divided by the square root of the sample size.as show in Fig. 3.

a) *Data Transformation:* Converting the explicatory variables (Intl-plan, voicemail-plan) to a binary form to be more appropriate (yes = 1 /no = 0) in a specific model.

b) *Data clean:* This stage involves processing /calculating lost data: Some specified algorithms cannot handle lost data like SVM. For this reason, the lost value can be alternated with average or (0). Yet, it is better option to replace the lost data by the calculated statistical value (computation option), including the data set utilized to the lost values in several variables numerical (total-day-charge, total-evening-minutes, total Intl-calls, total Intl-charges, and total nighttime-charges), and nominal variables (Voicemail-plan, Intl-plan). Numerical data is alternated using various RF techniques. Bilateral values are calculated via techniques [13], [14].

	vars	n	mean	sd	median	trimmed	mad	min	max	range	skew	kurtosis	se	Q0.1	Q0.25	Q0.5	Q0.75	Q0.9
account_length	1	5000	100.26	39.69	100.00	99.90	40.03	1	243.00	242.00	0.11	-0.10	0.56	49.00	73.00	100.00	127.00	151.10
international_plan	2	5000	0.09	0.29	0.00	0.00	0.00	0	1.00	1.00	2.77	5.67	0.00	0.00	0.00	0.00	0.00	0.00
voice_mail_plan	3	5000	0.26	0.44	0.00	0.21	0.00	0	1.00	1.00	1.07	-0.86	0.01	0.00	0.00	0.00	1.00	1.00
number_vmail_messages	4	5000	7.76	13.55	0.00	5.04	0.00	0	52.00	52.00	1.35	0.20	0.19	0.00	0.00	0.00	17.00	32.00
total_day_minutes	5	5000	180.29	53.89	180.10	180.26	53.82	0	351.50	351.50	-0.01	-0.02	0.76	111.89	143.70	180.10	216.20	248.81
total_day_calls	6	5000	100.03	19.83	100.00	100.14	19.27	0	165.00	165.00	-0.08	0.18	0.28	75.00	87.00	100.00	113.00	125.00
total_day_charge	7	5000	30.65	9.16	30.62	30.64	9.15	0	59.76	59.76	-0.01	-0.02	0.13	19.02	24.43	30.62	36.75	42.30
total_eve_minutes	8	5000	200.64	50.55	201.00	200.61	50.41	0	363.70	363.70	-0.01	0.05	0.71	136.70	166.38	201.00	234.10	265.32
total_eve_calls	9	5000	100.19	19.83	100.00	100.21	19.27	0	170.00	170.00	-0.02	0.11	0.28	75.00	87.00	100.00	114.00	125.00
total_eve_charge	10	5000	17.05	4.30	17.09	17.05	4.28	0	30.91	30.91	-0.01	0.05	0.06	11.62	14.14	17.09	19.90	22.55
total_night_minutes	11	5000	200.39	50.53	200.40	200.35	50.11	0	395.00	395.00	0.02	0.08	0.71	135.90	166.90	200.40	234.70	263.90
total_night_calls	12	5000	99.92	19.96	100.00	99.90	19.27	0	175.00	175.00	0.00	0.14	0.28	74.00	87.00	100.00	113.00	125.00
total_night_charge	13	5000	9.02	2.27	9.02	9.02	2.25	0	17.77	17.77	0.02	0.08	0.03	6.12	7.51	9.02	10.56	11.88
total_intl_minutes	14	5000	10.26	2.76	10.30	10.30	2.67	0	20.00	20.00	-0.21	0.65	0.04	6.80	8.50	10.30	12.00	13.70
total_intl_calls	15	5000	4.44	2.46	4.00	4.16	1.48	0	20.00	20.00	1.36	3.26	0.03	2.00	3.00	4.00	6.00	8.00
total_intl_charge	16	5000	2.77	0.75	2.78	2.78	0.71	0	5.40	5.40	-0.21	0.65	0.01	1.84	2.30	2.78	3.24	3.70
number_customer_service_calls	17	5000	1.57	1.31	1.00	1.43	1.48	0	9.00	9.00	1.04	1.48	0.02	0.00	1.00	1.00	2.00	3.00
churn	18	5000	0.14	0.35	0.00	0.05	0.00	0	1.00	1.00	2.06	2.23	0.00	0.00	0.00	0.00	0.00	1.00

Fig. 3. Description of the Data Set (Data Set Variables of Customer Transactions).

TABLE I. ATTRIBUTES OF THE DATA SET

Data Type	Description	Variable
Account Length	Customer subscription period by weeks	Integer
International plan	participation in the international plan (yes, no)	Categorical
Voice. Mail plan	participation voicemail plan (yes, no)	Categorical
Vmail. messages	No. of voicemails	Integer
Total. Day. minutes	Total daily minutes	Integer
Total. Day. calls	Total of calls that was during the day	Integer
Total. Day. charge	Total daily charge	Integer
Total. Eve. minutes	Total eve minutes used	Integer
Total. Eve. calls	Total calls in the evening used	Integer
Total. Eve. charge	Total evening call charges	Integer
Total.night.minutes	Total nighttime minutes used	Integer
Total.night.calls	Total nighttime calls used	Integer
Total.night.charge	Total nightly calls charges	Integer
Total.intl.minutes	total International minutes usage	Integer
Total.intl.calls	Total International calling used	Integer
Total.intl.charge	Total invoice international charges	Integer
Customer.service.calls	No. of calls used serving of customers	Integer
Churn	Customer's case (True = churn, False = no churn)	Categorical

3) *Feature selection*: Feature selection is one of the most vital elements that can influence model performance. It is also, the operation in which actions are performed automatically or manually, and features that contribute most to the variable or the prediction result. Inappropriate data features can reduce

the accuracy of forms and make the model based on irrelevant features. The selection feature helps to give a clearer understanding of the data by identifying the important features of the data and their relationship to each other. In this study, to assess the relationship between each input variable and the target variable, these scores are applied as a basis for selecting (filtering) and arranging the most important variables and reducing dimensions. The RF technique that is used in selection the feature using the average accuracy decrease. Average deficiency means that each feature affects the accuracy of the model. The model allows the values of every feature and estimates the model's accuracy change. Features that have a high effect on accuracy are only important [15], [16]. Technique known as "Boruta" is used for other feature selection. It is amelioration on RF, in which all the features have to be linked to the target variable, while most technologies are following the minimum optimization method interplay among features. Both techniques are used to rank predictors depending on the mean significance of Boruta, and the average decreasing error calculated by RF. The results, indicated in Table II, clarify that the initial three variables correspond to the identical rank (customer-serve-calls, Intl-plan, total-day-minutes). Models agreement is the following ten features of various ranks: (total day-charges, Total-Intl-calls, Total-Int'l-minutes, Total-Int'l-charges, voicemail-plan, total-evening-charges, total-evening-minutes, v-mail-messages, total-nighttime-minutes, and total-nighttime-charges). Models show a low ranking for the remaining variables (total-day-calls, total-nighttime-calls, total-evening-calls, and account-length). Outcomes are indicated in Table II and Fig. 4. Where 13 variables were confirmed and 4 variables rejected.

TABLE II. FEATURES MEAN IMPORTANCE (DESCRIPTION STATISTICS OF NUMERICAL VARIABLES IN THE DATABASE)

Feature	Mean Import	Median Import	Min Import	Max Import	Norm Hits	Decision
customer_service_calls	79.7030451	79.8658717	76.297333	82.8529157	1	Confirmed
international_plan	65.5254351	66.0630689	62.212469	68.7058141	1	Confirmed
total_day_minutes	39.9455885	40.0260729	36.90489	42.4116863	1	Confirmed
total_day_charge	38.8683454	39.0927738	36.539083	40.806327	1	Confirmed
total_intl_calls	37.9153817	37.3873506	35.874353	41.182217	1	Confirmed
total_intl_minutes	22.8759486	22.7362083	22.02165	24.0693349	1	Confirmed
total_intl_charge	22.7810105	22.9715311	20.817315	24.2876061	1	Confirmed
voice_mail_plan	22.6492168	22.8422342	20.877226	23.6341128	1	Confirmed
total_eve_charge	22.1410863	21.8842483	20.407409	23.6509283	1	Confirmed
total_eve_minutes	21.8988284	21.8339512	20.498661	23.4987201	1	Confirmed
number_vmail_messages	21.8944202	21.3996754	21.096311	24.4659916	1	Confirmed
total_night_minutes	13.4130025	13.4427115	12.759512	14.3821655	1	Confirmed
total_night_charge	13.0082163	12.924208	12.121582	14.3744161	1	Confirmed
total_day_calls	-0.5188858	-0.4468013	-1.95245	0.6344864	0	Rejected
total_night_calls	-0.6262422	-0.3491468	-2.672444	0.874702	0	Rejected
total_eve_calls	-1.3878873	-1.1726735	-2.787194	-0.175634	0	Rejected
account length	-1.0827182	-1.1550063	-2.631888	0.9322869	0	Rejected

Features Importance processing of finding and specifying the most beneficial features in a data set. The top essential variables are from the top tier of boruta's selections and features for RF models. In Fig. 4 show in mean decrease accuracy, it indicates that the right of the blue line is the number of customer service calls, international plan, and total daily minutes.

This means that these are the most important factors in determining customer churn, it is logical the customer, who has to receive many customer service calls to resolve a problem, may become disappointed and leave his business with the company [16] shown in Table II and Fig. 4, is also illustrated cases in Fig. 5.

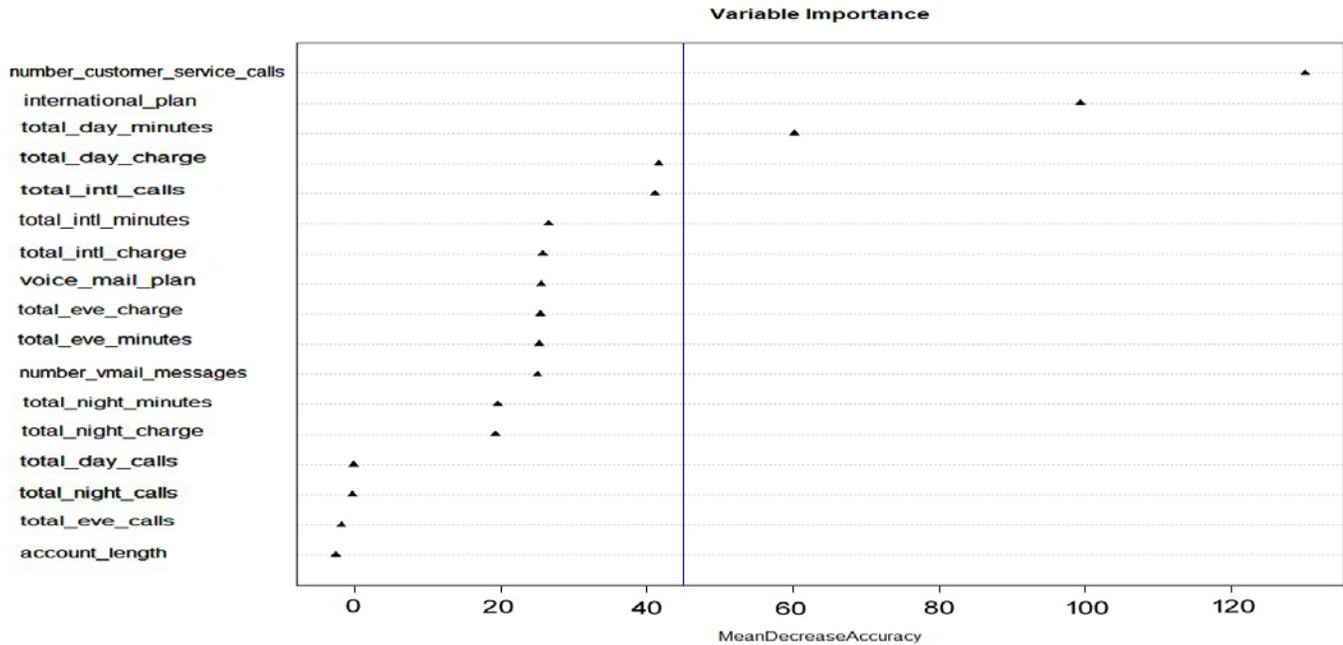


Fig. 4. Features mean Importance (Mean Decrease Accuracy).

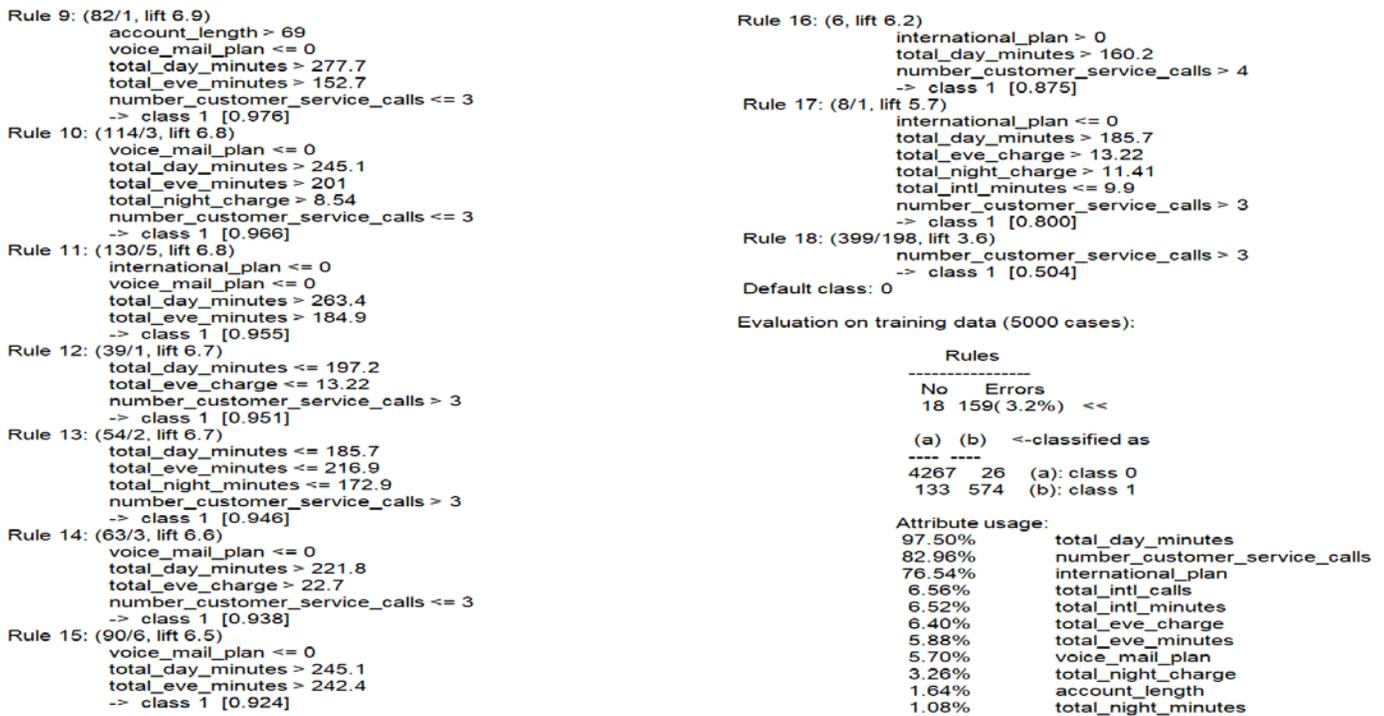


Fig. 5. The Result of Chumers.

4) *Calculation of variable importance*: This step for sampling training and testing through this stage predicts uses the dataset containing 5000 records. A data set with 17 attributes 75% is used to train the model and 25% are applied as testing. Training is used to explore data and build models, while testing will be used to measure model performance. For significance grades generated from varImp.train, the drawing method can be used to visualize results. Variable importance is only 5 of the 17 features are utilized by “rpart”. The tree structure shown here provides a neat and easy-to-follow description of the problem under consideration and its solution. Note that the implementation of R for the CART algorithm is called RPART (Recursive Partitioning and Regression Trees). Dataset and constructing an algorithm, used in the training, can be used to calculate the variable importance (varImp), model. The varImp is, then, used to value the different importance, which is plotted. It shows that the number of customer-service-calls, international-plan, total-day-minutes, total-day-charger, and voicemail-plan attributes are the top 5 most essential attributes. Ranks of features variable importance is shown in Fig. 6 and 7.

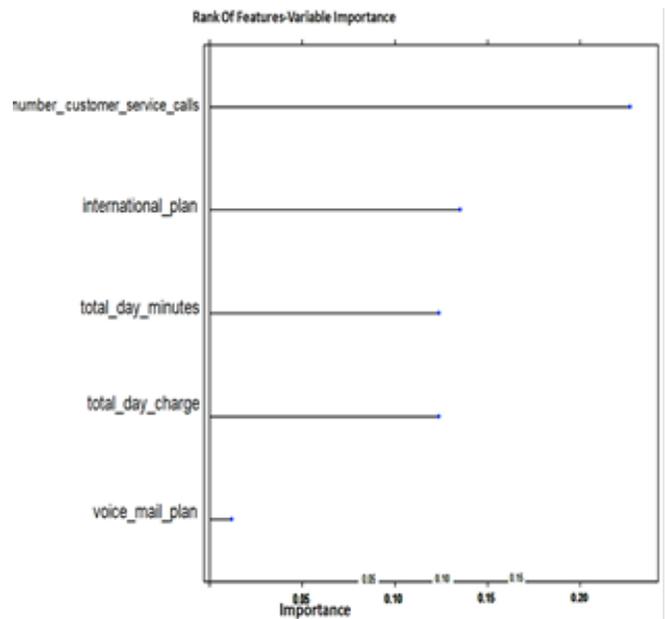


Fig. 6. The Rank of Features Variable Importance.

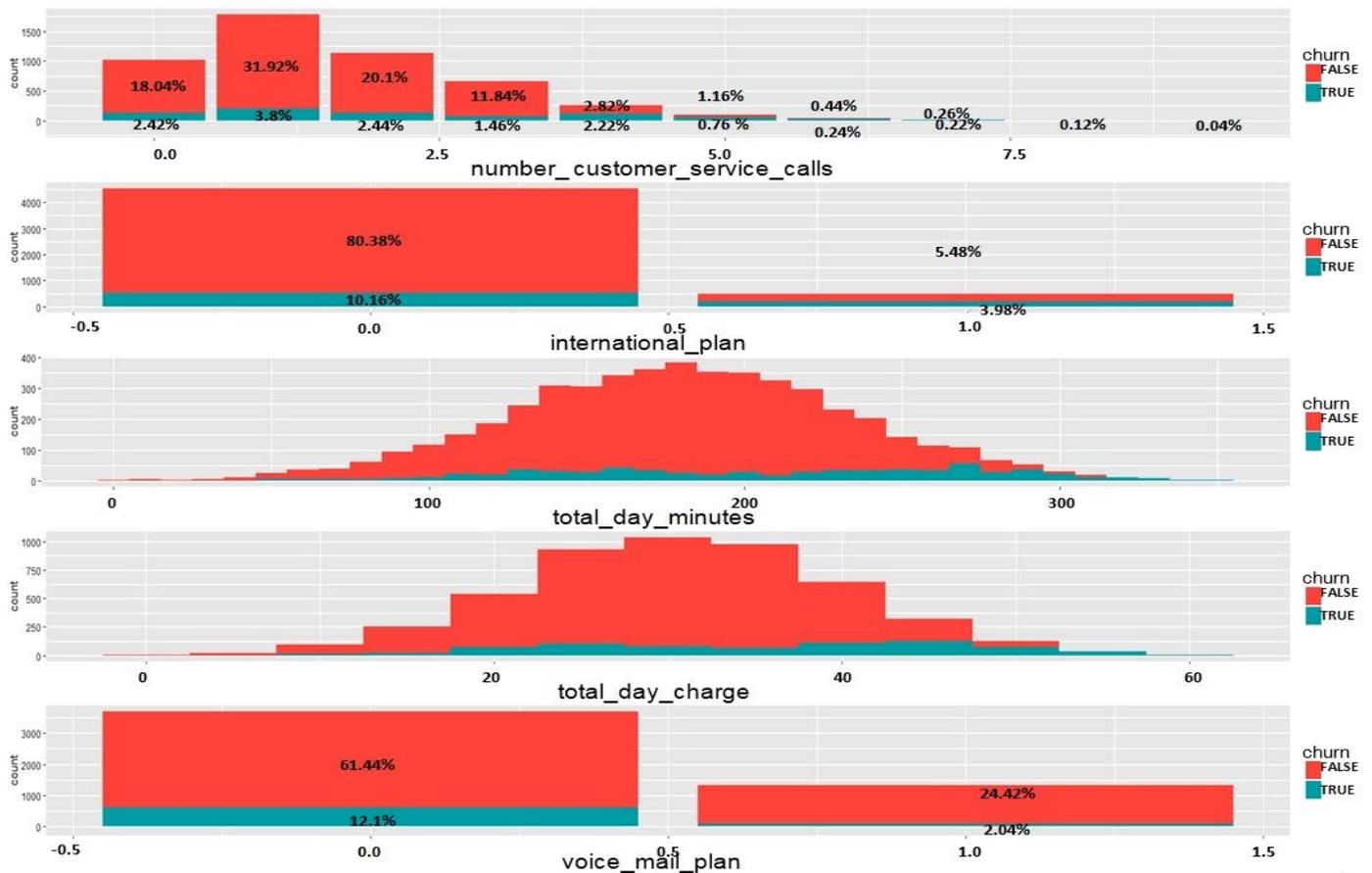


Fig. 7. Variables Importance Distribution (Ranks of Features Variables Distribution).

b) *Data visualization of descriptive statistics:* After taking various steps including calculating variable importance, descriptive statistics for data are examined under some simple plots, which define several important predictive variables for the model and which represent the five variables shown in Fig. 6. Fig. 7 shows illustrates the distribution of this feature concerning the churn class, the churn rate via the categorical predictors (red = false) and (blue = true). While the percentage of change for customers, who do not use voicemail plans, seems higher, the rate of change in the international plan is 4 times the average, and there is a higher increase in the rate of calls with the increase of customer calls exceeding 4 customer calls. Many churning customers use more "minutes of the time of day" while charges are high. It also shows (increases and decreases) between churners' factors, find an increase in the number of calls to customer of service and a rise in using international plan, increases charge process daily, daily contact ,and Less use on voicemail.

c) *Neural Networks:* Neural networks are built via 17 inputs, 2 outputs, and 1 hidden layer with 6 neurons. The algorithm that is used in neural net by default is based on the resilient back-propagation without weight backtracking, to perform a classification (linear. Output = FALSE) in this case.

d) *Support Vector Machine:* Support vector machine builds and specifies a type for c-classification, in addition to using two extra parameters: gamma and cost. Gamma is the argument used by the function kernel= radial "the default". Test with various gamma and cost values to find better classification accuracy. Whereas, actual support offer1018 detects the model support vectors dispenser in the categories (false for 585 and 433 for true).

e) *Random forest:* Forests of 500 DT are built by using RF 100 trees; they do not decrease in the error. Besides, the parameter is metric, which refers to the number of predictors that are sampled to divide by every node. Optimum performance at metric Mtry= 5.

f) *Results and discussion:* A dataset of 5,000 customers dissected, included 707 churning. The results reveal that there are five correlations between customers' behavior and variables that affect the QoS, which affects customer loyalty. A dataset was applied to an available dataset of publicly, obtained from the KDD library. The data is acquired from a wireless communications operator. For a complete description of the dataset, one can refer to D.Larose (2014) [17].

1) *Number customer service calls:* About 50% of customers who contact the company more than 3 times are classified as "Churn" while only 5 % of "non-churners" Called for service more than three times, this reveals that 27 % of churners have done so. The company must monitor the QoS in its call centers in an attempt to solve technical problems in less than three calls. Besides, customers who call more than three times should be noteworthy. As shown in Fig. 3 and 7.

2) *International plan:* It reveals that customers who have an international plan quadruple their odds to be churn. The company should examine its Intl plan and its suitability for customer needs. For every unit of increase in international

fees, there is an 18% increase in the possibility of high rate (leaving the company) 10% of those without an international plan are classified "Churn" and 8% of those who own an international plan is churn. A high rate of churn among customers has international plans. The count of customer service calls, the international plan, and the total of international calls. This means that it is the most important factor that determines churn. The customer who has to receive many customer service calls to solve a problem is likely to become frustrated. And leave his dealings with the company. This is shown in Fig. 3 and 7.

3) *Total day minutes and total day charge:* Total day minutes & Total day charge: Apparent that many churn customers use more "daytime minutes", and as an outcome for paying high invoices. They are "the significant use". These are the company's most values customers because of the high fees they pay. Higher charges may push these customers to find a cheaper plan or other providers. Targeting these higher in-use customers by promoting the best prices may be an incentive for them to remain as customers. This is shown in Fig. 3 and 7.

4) *Total day minutes and total eve minutes:* If the whole minutes per day exceed 277.7, and the total evening minutes are 152.7, the customer is probable to depart the company. This is shown in rule 9 in Fig. 5. High churn rate among intense time users today, it is probably customers who pay high bills and some of these customers seek to find cheaper options. Show in Fig. 5.

5) *Voice- mail- plan:* customers who have a voicemail plan are less probable to "churn" than customers without a voicemail plan. This is shown in Fig. 3 and 7.

The proposed model categorizes churn customer data by using classification algorithms to identify the root causes of amplification [18]. By knowing the important churners factors from customer the data. CRM can improve productivity; recommend related promotions to set of potential churners [19], [20] Results have been discussed based on the performance of three classifiers; NN, SVM, and RF were evaluated as confusion matrix mentioned in the basic abbreviations used in confusion matrix (Table III).

Accuracy defines the percentage of rightly classified cases from test assigned by the classifier [11] - [13].

$$\text{Accuracy} = \frac{tp+tn}{tp+tn+fp+fn} \quad (1)$$

(TP) Are statuses where predicted churners by correctly "churn"

(FP) Are statuses where the predicted churners by incorrectly "churn"

(TN) Are statuses where the predicted churners by correctly "non-churn"

(FN) Are statuses where the predicted churners by incorrectly "non-churn"

The results performed by the tool R, considering the NN, SVM, and RF techniques, are shown in Table IV. The results performed by the WEKA tool considering the NN, SVM, and RF techniques are shown in table 5. The summary of the total results of tools and techniques are shown in Table VI.

Table VI compares the accuracy of the R and WEKA tools considering the NN, SVM, and RF techniques. For the NN technique, the accuracy of the R tool is 96.9%, which shows better results than the WEKA tool that is 95.92%. Considering the SVM technique, the accuracies of the WEKA and R tools are 94.8% and 92.1%, respectively. That means the WEKA tool outperforms the R tool in such a case. For the RF technique, the accuracy of the R tool is 96.4%, which shows better results than that of the WEKA tool that is 95.44%.

TABLE III. CONFUSION MATRIX

Confusion matrix	Predicted value	Predicted value
Actual	True	False
True	TP	FP
False	FN	TN

TABLE IV. CONFUSION MATRIX R TOOL

Tool and Techniques using		Actual Class	Actual Prediction	
			Non-churners	Churners
R Tool	NN	Non- churners	1405	11
		Churners	39	211
	SVM	Non- churners	1417	79
		Churners	20	150
	RF	Non- churners	1078	35
		Churners	10	127

TABLE V. CONFUSION MATRIX WEKA TOOL

Tool and Techniques using		Actual Class	Actual Prediction	
			Non-churners	Churners
Weka Tool	NN	Non- churners	1059	11
		Churners	40	140
	SVM	Non- churners	1403	20
		Churners	65	178
	RF	Non- churners	1063	7
		Churners	50	130

TABLE VI. ACCURACY, ERROR RATES COMPARISON FOR R TOOL AND WEKA TOOL OF TECHNIQUES

Tool	Technique	Accuracy	Error rate
R	NN	96.9%	3.1 %
	SVM	92.1%	7.9%
	RF	96.4%	3.6%
WEKA	NN	95.92	4.08 %
	SVM	94.8%	5.2%
	RF	95.44	4.56%

## V. CONCLUSIONS AND FUTURE WORK

This study manifests an effective methodology to expect fluctuations in industries depending on customer service; the customer is affected by the quality of service, and that the QoS is one of the most important factors affecting the survival and continuation of the customer. Besides, the higher costs, associated with purchasing new customers, highlight the need for telecom operators to identify the churn to reduce costs, increase revenue, and analyze case types of churners. The model depending on DM techniques is offered to aid in the CRM management tracking its customers and their conduct versus disturbances Using 3 various techniques predicting NN, SVM, and RF for classification results hint that the best output for the data set used is the NN technique. In the future, the present methodology can be used to modern data sources such as flowing data in real-time to obtain a prediction of churn in real-time and would be more fit for data-based industries. The idea of churn prediction can be expanded to include other areas such as employee churn, drop-out customers' expectations. Customers can also learn about the best services suitable for them through a detailed stride-by-stride guide without communicating with the service providers.

## REFERENCES

- [1] Qadeer, Sara, "Service Quality & Customer Satisfaction: A case study in Banking Sector," pp.1-101, 2014.
- [2] Amin, A., Anwar, S., Adnan, A., Nawaz, M., Alawfi, K., Hussain, A., & Huang, K., "Customer churn prediction in the telecommunication sector using a rough set approach," Neurocomputing, 237, pp. 242-254, 2017.
- [3] E. Shaaban, Y. Helmy, A. Khedr, and M. Nasr, "A proposed churn prediction model," International Journal of Engineering Research and Applications, Vol. 2, No. 4, pp. 693 - 697, 2012.
- [4] K. Kaur and S. Vashisht, "Enhanced Boosted Trees Technique for Customer Churn Prediction Model," IOSR Journal of Engineering (IOSRJEN), Vol. 04, Issue 03, pp 41-45, 2014.
- [5] KiranDahiya ,Surbhi Bhatia "Customer Churn Analysis in Telecom Industry," 4th InternationalConference on Reliability, InfocomTechnologies and Optimization (ICRITO) (Trends and Future Directions), pp. 1-6,2015.
- [6] Oghojafor , Benjamin &Bakarea , Rasaki&Omoera, Charles &Adeleke, I.A, "Discriminant Analysis of Factors Affecting Telecoms Customer Churn," International Journal of Business Administration 3(2),pp.59-67, 2012.
- [7] Sidra Ansar, co authorSamreenLodhi, "the impact of service quality on customer satisfaction in telecom sector of Pakistan. An empirical study of Pakistan," International Journal of Scientific & Engineering Research, Volume 6, Issue 10, pp.1639-1645, 2015.
- [8] ManpreetKaur, Dr. PrernaMahajan, "Churn Prediction in Telecom Industry Using R," International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-5, pp.46-53, 2015.
- [9] Bharati, M. &Ramageri, "data mining technique applications," Indian Journal of Computer Science and Engineering, Vol. 1 No. 4, pp. 301-305, 2010.
- [10] Mamčenko, J. &Gasimov, J., "Customer churn prediction in mobile operator using combined model," ICEIS 2014 - Proceedings of the 16th International Conference on Enterprise Information Systems. 1, pp. 233-240, 2014.
- [11] Jayaswal, Pretam& Prasad, Bakshi&Tomar, Divya&Agarwal, Sonali. , "An Ensemble Approach for Efficient Churn Prediction in Telecom Industry," International Journal of Database Theory and Application. 9, pp. 211-232, 2016.

- [12] Brandusoiu, Ionut&Todorean, G., "Churn Prediction in the Telecommunications Sector Using Support Vector Machines," Annals of the Oradea University. Fascicle of Management and Technological Engineering. XXII (XII), pp.19-22, 2013.
- [13] I. I. Ullah, B. Raza, A. K. Malik, M. Imran, S. U. Islam and S. W. Kim, "A Churn Prediction Model Using Random Forest: Analysis of Machine Learning Techniques for Churn Prediction and Factor Identification in Telecom Sector," in *IEEE Access*, vol. 7, pp. 60134-60149, 2019.
- [14] Shah AD, Bartlett JW, Carpenter J, Nicholas O, Hemingway H., "Comparison of random forest and parametric imputation models for imputing missing data using MICE: a CALIBER study," *Am J Epidemiol.* 15; 179(6):764-74, 2014.
- [15] Oralhan, Burcu&Uyar, Kumru& ORALHAN, Zeki, "Customer Satisfaction Using Data Mining Approach," *International Journal of Intelligent Systems and Applications in Engineering.* 4. 63-63, 2016.
- [16] F., Sahar. "Machine-Learning Techniques for Customer Retention: A Comparative Study," *International Journal of Advanced Computer Science and Applications.* Vol. 9, No. 2, pp.273-281, 2018.
- [17] Daniel T. Larose and Chantal D. Larose "Discovering Knowledge in Data: An Introduction to Data Mining, Second Edition",pp.1-366,2014
- [18] Ahmad, A.K., Jafar, A. &Aljoumaa, K., "Customer churn prediction in telecom using machine learning in big data platform," *Journal of Big Data*, 6(1), pp.1-24, 2019.
- [19] Abdulrahman, S. A., Khalifa, W., Roushdy, M., & Salem, A.-B. M., "Comparative study for 8 computational intelligence algorithms for human identification. *Computer Science Review*," 36, 100237, pp.1-11, 2020.
- [20] HomaMeghyasi and AbasRad, "Customer Churn Prediction in Irancell Company Using Data Mining Methods," *EasyChair Preprint No. 2422*, pp.1-6, 2020.

# Speech-to-Text Conversion in Indonesian Language Using a Deep Bidirectional Long Short-Term Memory Algorithm

Suci Dwijayanti<sup>1</sup>, Muhammad Abid Tami<sup>2</sup>, Bhakti Yudho Suprpto<sup>3</sup>  
Department of Electrical Engineering, Universitas Sriwijaya, Indralaya, Indonesia

**Abstract**—Now-a-days, speech is used also for communication between humans and computers, which requires conversion from speech to text. Nevertheless, few studies have been performed on speech-to-text conversion in Indonesian language, and most studies on speech-to-text conversion were limited to the conversion of speech datasets with incomplete sentences. In this study, speech-to-text conversion of complete sentences in Indonesian language is performed using the deep bidirectional long short-term memory (LSTM) algorithm. Spectrograms and Mel frequency cepstral coefficients (MFCCs) were utilized as features of a total of 5000 speech data spoken by ten subjects (five males and five females). The results showed that the deep bidirectional LSTM algorithm successfully converted speech to text in Indonesian. The accuracy achieved by the MFCC features was higher than that achieved with the spectrograms; the MFCC obtained the best accuracy with a word error rate value of 0.2745% while the spectrograms were 2.0784%. Thus, MFCCs are more suitable than spectrograms as feature for speech-to-text conversion in Indonesian. The results of this study will help in the implementation of communication tools in Indonesian and other languages.

**Keywords**—Speech-to-text; Deep Bidirectional Long Short-Term Memory (LSTM); spectrogram; Mel frequency cepstral coefficients (MFCC); word error rate

## I. INTRODUCTION

Speech is a longitudinal wave that propagated through a medium, which can be solid, liquid, or gaseous [1]. Humans utilize speech as a primary component of communication to exchange information. Today, humans communicate also with computers; generally, this communication requires the conversion of speech into text [2]. This process involves various stages of conversion and outputs data consisting of numbers that can be processed by a computer into text [3]. Speech-to-text conversion can be implemented in various applications, such as communication tools for deaf people [2], smart homes [4], and translators [5].

Some studies have investigated speech-to-text conversion in various languages. Ahmed et al. utilized a hidden Markov model (HMM) for English and Arabic speech recognition [6]. Hotta [7] and Othman [8] performed speech-to-text conversion using neural networks in Japanese and Jawi, respectively. Kumar et al [9] used a recurrent neural network (RNN) for speech-to-text conversion in Hindi, and Laksono et al. [10] used connectionist temporal classification (CTC), which is usually applied on top of an RNN, for speech-to-text

conversion in Indonesian and Javanese. Abidin et al. presented an approach to obtain Indonesian voice-to-text data set using Time Delay Neural Network Factorization (TDNNF) [11].

Mon and Tun [12] proposed the HMM method, which uses Mel frequency cepstral coefficients (MFCCs) as features. Because they used a large dataset of English words, the HMM was ineffective owing to the high probability of similarity between words. Zhang [13] used a combination of the deep neural network (DNN) and HMM model for English speech recognition and showed that DNN-HMM was superior to the traditional Gaussian mixture model (GMM)-HMM method. Nevertheless, it still had low accuracy. Liu et al. [14] had shown that the RNN together with Long Short Term Memory (LSTM) improved the performance of speech recognition on the ChiME-5 dataset. Meanwhile, Wu et al. [15] and He [16] utilized RNN-LSTM for Chinese dataset, and the accuracy of speech recognition was improved.

Most studies on speech-to-text conversion were limited to the conversion of words or incomplete sentences from a dataset, and very few studies considered speech-to-text conversion in Indonesian. Laksono et al. [10] used DNN and CTC with MFCCs as the features for speech-to-text conversion in Indonesian and Javanese with a small number of Indonesian and Javanese words. However, the result showed low accuracy for both Indonesian and Javanese; thus, they might not be suitable for speech-to-text conversion.

In this study, we perform speech-to-text conversion in Indonesian using a deep bidirectional long short-term memory (LSTM) algorithm. We determine the features suitable for the deep bidirectional LSTM and consider complete sentences consisting of subject, predicate, object, and adverb spoken by some respondents.

The rest of this paper is organized as follows. In Section 2, the research method used in this study is presented. Section 3 reports and discusses the results. Finally, the paper is concluded in Section 4.

## II. MATERIALS AND METHODS

### A. Data Collection

The speech data were obtained from ten speakers (five males and five females). Every speaker uttered ten sentences in Indonesian consisting of a subject, predicate, object, and adverb, as presented in Table I. Each sentence was uttered 50 times; thus, a total of 5000 sentences were recorded. Data

were manually divided as follows: 70% for training, 20% for validation, and 10% for testing. Thus, 3500 training, 1000 validations, and 500 testing data were obtained. The data were recorded in the Control and Robotics Laboratory, Universitas Sriwijaya.

### B. Proposed Speech-to-Text Conversion Process

Fig. 1 shows a block diagram of the proposed speech-to-text conversion process. The speech is recorded using a FIFINE K669B microphone with a sampling frequency of 16 kHz. Speech data undergo the preprocessing stage, which involves normalization, silence removal, and pre-emphasis, to correct the speech signal by reducing noise and removing the silence area on the speech signal. Then, the speech features are extracted into spectrograms and MFCCs. The features are fed to the deep bidirectional LSTM to determine the probability of each label. In the deep bidirectional LSTM training process, CTC is used to determine the loss. Subsequently, the network performs the decoding for the process of labeling from the output of the deep bidirectional LSTM network and language model obtained from the Kompas newspaper. Finally, text is obtained as the output.

TABLE I. SENTENCES UTTERED BY THE SPEAKERS

No.	Sentence
1	saya bermain bola di lapangan
2	ayah membaca buku di ruang tamu
3	nenek memasak sayur di dapur.
4	kakak bermain sepeda di halaman
5	paman menggembala sapi di kebun.
6	bibi mengantar tas ke sekolah.
7	dia membaca buku di rumah.
8	adik memakai sepeda ke sekolah
9	kakek menanam padi di sawah
10	ibu menonton tv di kamar

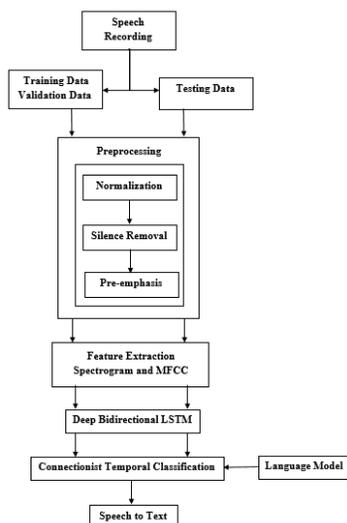


Fig. 1. Block Diagram of Speech-to-Text Conversion Process.

### C. Evaluation

The word error rate (WER) is used to determine the percentage of success of speech-to-text conversion. It is determined by calculating the number of insertions, subtractions, and substitutions of the word used to convert speech into text as follows:

$$WER = \frac{1}{z} \sum ED(h(x)) \quad (1)$$

where  $ED(h(x))$  is the number of insertions, subtractions, and substitutions of the word in the target sentence and  $z$  represents the total words in the reference which were actually said [17].

## III. RESULTS AND DISCUSSION

### A. Preprocessing Signal

The preprocessing stage involved normalization, silence removal, and pre-emphasis, which were performed using the Python library Pyrus. Normalization is performed by dividing the data in the speech signal by the maximum value of the amplitude to equate the amplitude of the speech signals. Owing to the recording process, the speech signal may have different intensities and consequently, different amplitude values. Silence removal is performed to determine the silence area to be erased on the speech signal. Finally, pre-emphasis is important to remove the noise while maintaining the frequency of the speech signal.

Fig. 2(a) and (b) show the speech signal before and after the preprocessing stage, respectively, displayed using the audacity software. From the figure, it can be seen that before preprocessing, the speech signal has an amplitude of less than 0.5 and silence areas are at the beginning and end of the speech. On the other hand, after preprocessing (Fig. 2(b)), the amplitude of the signal is approximately 0.5, which is the ideal value for speech signals [18], and the silence areas are smaller than those before the preprocessing stage; the duration of the speech signal changes from 3 to 2.4 s. Furthermore, the noise in the speech signal was reduced by using a high pass filter to eliminate speech signals with frequency below 250 Hz.

### B. Feature Extraction

Using the contrib audio library of TensorFlow, we extracted the log power spectra, i.e., spectrograms, and MFCCs as features and determined which is more suitable as input to the deep bidirectional LSTM.

To obtain the spectrograms, the preprocessed speech signal was divided into sections with window lengths of 32 ms and window steps of 16 ms. A fast Fourier transform (FFT) was performed to convert the speech signal from the time domain to the frequency domain. 512 frequency bins were used, and only half of the frequency bins plus one (257 bins) were used. Then, the log power spectra, which were the density of the FFT spectra, were used as input for the training process. The visual representation of log power spectra is known as spectrogram. Fig. 3 shows an example spectrogram. As shown in the figure, an x-axis shows the time length and a y-axis is the power spectrum of the speech signals.

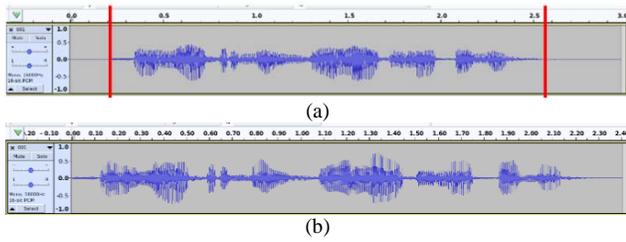


Fig. 2. Speech Signal (a) before and (b) after Preprocessing.

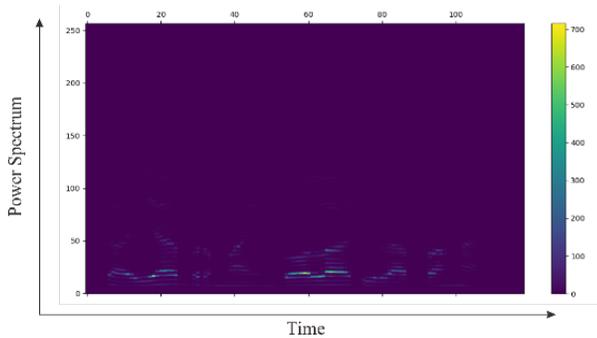


Fig. 3. Example of a Spectrogram.

The MFCCs are generated using the result of the spectral density, which is filtered with a Mel scale and filter bank to obtain the energy at each point. The resolution of the Mel filter bank was 40 with lowest and highest frequencies of 0 Hz and 8 kHz, respectively. The Mel spectrum, which is the output from the Mel filter bank, is converted into the time domain using a discrete cosine transform (DCT) with a coefficient of 13. The output from the DCT process is called an MFCC plot. Fig. 4 shows an example MFCC plot.

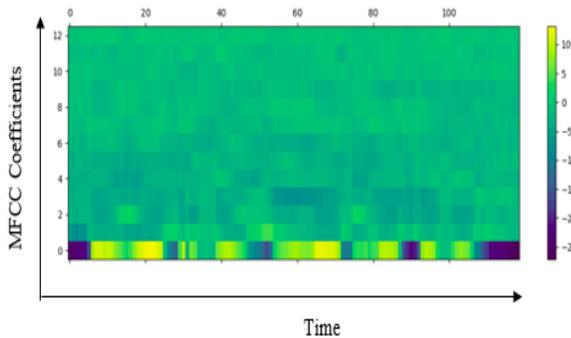


Fig. 4. Example MFCC Plot.

### C. Language Model

A language model is used to perform the decoding process on the network output for the speech-to-text conversion process. The decoding process is performed by calculating the probability of appearance of each word based on the exact word order [19]. This probability is calculated from the word chunks based on word order in the N-grams model. The language model can be built using Corpus text with a large amount of data, e.g., words and sentences in a newspaper. Accordingly, in this study, Corpus text in .txt format derived from the Kompas newspaper [20] was used. The Kompas newspaper has published more than 5000 articles, which were merged to create the language model. Before using, the

Corpus text is sorted in alphabetical order from A to Z, and invalid data such as space and blank () are removed.

A 5-gram language model was built with outputs in lm.arpa format using the KENLM library. The lm.arpa output was transformed into binary format to be processed and read by the computer. Then, a trie that works by tracking the minimum probability for the word prefix was created as a data structure to assist in using the memory to construct the language model.

### D. Training Dataset

The DeepSpeech library was used in the training process of the deep bidirectional LSTM algorithm. This algorithm consists of a combination of bidirectional RNN and LSTM, commonly known as bidirectional LSTM. The bidirectional LSTM exploits long-range context dependencies in the past ( $t - 1$ ) steps and future ( $t + 1$ ) steps. This algorithm has a deep architecture, which can perform high-level representations of acoustic data [21]. The DeepSpeech architecture consists of the input layer derived from the extracted features, i.e., spectrograms and MFCCs. Then, there are five stacked hidden layers: three linear hidden layers, one LSTM hidden layer, and one linear hidden layer. The last layer is an output layer that uses the Softmax activation function to determine the probability of a transcript label. Fig. 5 shows a schematic of the DeepSpeech architecture.

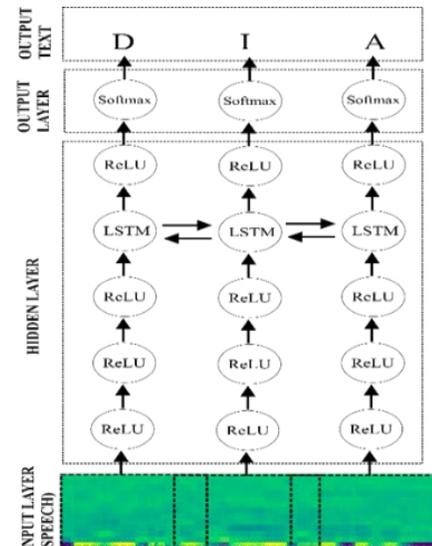


Fig. 5. Schematic of DeepSpeech Architecture.

The training performance can be determined from the loss values on the network. To prevent overfitting on the network, we use the early stopping technique, which involves the comparison of the loss value of the network during validation. The output of the network will be processed by CTC to perform the decoding process with the prefix beam search method according to the probability generated by the SoftMax layer and language model. CTC is used to model the training results obtained by a network. Because it can classify labels without having to know the alignment given, it is suitable for the deep bidirectional LSTM [22]. The CTC value decreased as the number of layers used increased, a phenomenon known as the CTC loss. The CTC loss value is a representation of the

accuracy of the training results; a smaller CTC loss value indicates a higher accuracy. Nevertheless, an excessively small CTC loss value leads to overfitting. In the training, we used five scenarios denoted as A, B, C, D, and E, as presented in Table II, to find the most suitable parameters.

In scenarios B, D, and E, the training process is continued until the epoch is ended, while in scenarios A and C, it is stopped early. We used 3500 speech data for training and a batch size of 70; thus, the number of steps in each epoch was 50. These steps were repeated for all data in each epoch. The training process resulted in a model called output graph, which could be stored and used to transcribe the data. Table III presents the results of each training scenario.

From Table III, it can be seen that when spectrograms were used as the input to the deep bidirectional LSTM and early stopping was activated (scenario A), training ended after 12 epochs within 5 h, 13 min, and 23 s with training and validation loss values of 0.746044 and 4.590043, respectively. When MFCC were used as the input and early stopping was activated (scenario C), training ended after 9 epochs within 2 h, 53 min, and 5 s with training and validation loss values of 0.424811 and 0.914198, respectively. These results indicate that MFCCs are more suitable as input to the deep bidirectional LSTM than spectrograms. These results may also imply that the MFCC features are better in terms of the computation time and loss value, and provide more useful information for the classifier.

On the other hand, when spectrograms were used as the input to the deep bidirectional LSTM and early stopping was not activated (scenario B), the loss values were lower than in scenario A. Furthermore, when MFCCs were used without early stopping (training scenario D), the loss values were lower than in scenarios A, B, and C. In particular, in scenario B, the training and validation loss values were 0.084932 and 2.765626, respectively, and training was completed within 16 h, 6 min, and 40 s; in scenario D, the training and validation loss values were 0.016846 and 0.505358, respectively, and training was completed within 15 h, 13 min, and 14 s. Therefore, when MFCCs are inputted, the training and validation loss values are smaller than when spectrograms are inputted. Although overfitting occurred in training scenario D, the training process could be re-adapted as shown in Fig. 6. Overfitting may have occurred owing to the presence of noise.

To prevent overfitting, we reduced the number of epochs before the occurrence of overfitting (scenario E). The process of training in scenario E is performed to determine the best training results before overfitting. Training ended at epoch of 24 within 7 h and 23 min with training and validation loss values of 0.077836 and 0.494393, respectively. Fig. 7 shows the plot of the loss values in scenario E. Compared to training scenario D, scenario E has higher training loss value but lower validation loss value. In scenario E, the training process took only 24 epochs, which is less than in scenario D.

**E. Testing Model**

The model obtained from the training results was tested. The test involved speech-to-text conversion of 500 speech data samples not included in the training process. As a

measure of the accuracy, we considered the WER, which has a range of 0–1; a smaller WER value indicates a higher testing accuracy. Table IV shows the results obtained from a different model of training scenarios.

TABLE II. SCENARIOS USED FOR TRAINING

Parameter	Spectrogram		MFCC		
	A	B	C	D	E
Training scenario	A	B	C	D	E
Train Batch Size	70	70	70	70	70
Validation Batch Size	4	4	4	4	4
Test Batch Size	1	1	1	1	1
Learning Rate	10 <sup>-4</sup>	10 <sup>-4</sup>	10 <sup>-4</sup>	10 <sup>-4</sup>	10 <sup>-4</sup>
Epoch	50	50	50	50	24
Early Stopping	Yes	No	Yes	No	No

TABLE III. RESULTS OF THE TRAINING SCENARIOS

Parameter	Spectrogram		MFCC		
	A	B	C	D	E
Training Scenario	A	B	C	D	E
Actual Epoch	12	50	9	50	24
Time (h)	5:13:23	16:06:40	2:53:05	15:13:14	7:23:00
Training Loss	0.746044	0.084932	0.424811	0.016846	0.077836
Validation Loss	4.590043	2.765626	0.914198	0.505358	0.494393

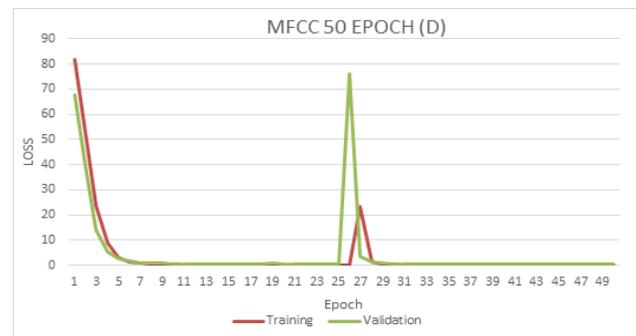


Fig. 6. Training and Validation Loss Values in Scenario D (using MFCC and 50 Epochs).

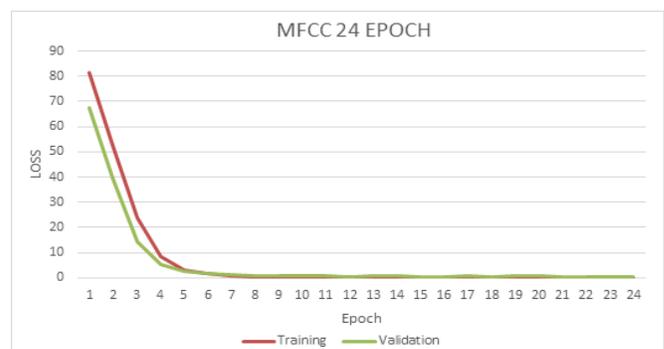


Fig. 7. Training and Validation Loss Values in Scenario E (using MFCCs and 24 Epochs).

TABLE IV. RESULTS OF TESTING USING DIFFERENT MODELS

Parameter	Spectrogram		MFCC		
	A	B	C	D	E
Training scenario	A	B	C	D	E
WER	0.035686	0.020784	0.004706	0.002745	0.002745
% WER	3.5686	2.0784	0.4706	0.2745	0.2745

From Table IV results with a WER of 2.0784% in training scenario B, testing with MFCCs yielded the best results with a WER of 0.2745% in training scenarios D and E. These results indicate that the MFCCs are more suitable than spectrograms for speech-to-text conversion with the deep bidirectional LSTM algorithm. Training with MFCCs can identify linguistic content and remove unimportant parts of speeches, which may contain noise. Furthermore, training with MFCCs can demonstrate the vocal tract of human speech in the form of a power spectrum. Fig. 8 shows the accuracy of each model.

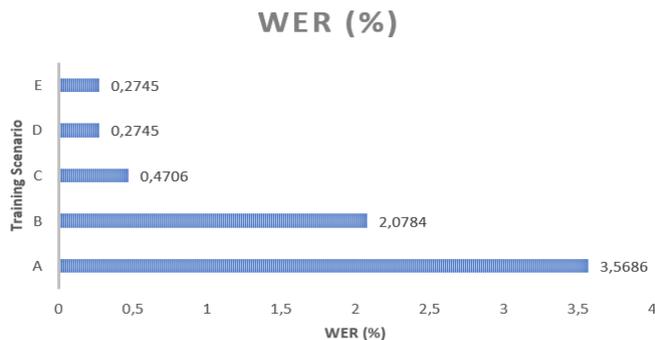


Fig. 8. WER Graph for each Training Scenario Model.

#### F. Testing Process using Speech Variations

Testing was also performed using five speech variations, namely regular (normal) conversation, speech with high intonation, speech with low intonation, speech with fast rhythm, and speech with slow rhythm. The test involved two speakers: a male and a female. The speakers uttered sentences 1–5 (see Table I) with the five styles listed in Table V. We tested the model obtained from training scenario E (using MFCCs as features) because it yielded the best results among the five training scenarios. Table V shows the WER obtained from the testing using different speech styles.

The results reported in Table V indicate that the model detected normal speech effectively. It can be seen that the intonation of the speech did not significantly affect the results. The model also detected the speech with fast rhythm well. However, the WER value obtained with the slow-rhythm speech is 40%, which indicates that many errors occurred during speech-to-text conversion. This may be due to the time-lapse between the words spoken and the large number of silence areas on the speech signal. These results indicate that the rhythm of the speech tends to affect the speech-to-text conversion process, while the intonation does not.

#### G. Testing Process with Secondary Datasets from TITML-IDN

The model obtained with training scenario E was also tested using five sentences obtained from the TITML-IDN dataset [23]. Table VI presents the results of speech-to-text conversion using speech corpus data for males and females.

TABLE V. RESULTS OF THE TESTING USING DIFFERENT SPEECH STYLES

Variation	WER (%)
Normal	0
High Intonation	9.3
Low Intonation	1.7
Fast Rhythm	6
Slow Rhythm	40

TABLE VI. RESULTS OF SPEECH-TO-TEXT CONVERSION USING THE TITML-IDN DATASET

No.	Target Transcript	Speech Detected from Male Speaker	Speech Detected from Female Speaker
1	dia tidak datang ke sekolah	diadi kakak ke sekolah	diadi eka ke sekolah eu
2	ketika kuatrianus hendak menelepon di wartel di halaman parkir bandara penjahat radin melarikan tas dengan mobil feroza.	kakak kakak muka selaku depkeu abu di halaman take pea asapa kakak di menanak ka sea budi rusun ke	kakak kakak sae aka di mana di halaman taeuk di aibak adi naik asean men sakka
3	kalian boleh lihat saya tidak apa apa padahal saya juga mengonsumsi produk transgenik	ada media saya ia kakak kakak saudi kamanan ke kekakuan	ayah menamai sa saya ie kakak kakak da sau iea bermasa ke sekaa sea edi
4	adi pandai bermain alat musik keyboard	aibak bermain skea babibu mena	adi aak benenain kaka aib mena
5	minggu depan ada main bola bareng anak kelas dua f	ibu mentan kakak main telapak kakak kakak	nenek kakak bermain bola aur aa seka

The results indicate that the model could detect the words in the TITML-IDN. For example, the target transcript “dia tidak datang ke sekolah” spoken by the male and female speakers is converted to “diadi kakak ke sekolah” and “diadi eka ke sekolah eu,” respectively. Therefore, the model successfully detected the word “ke sekolah” and it detected the word “dia” as “diadi.” However, the model did not recognize all words successfully because they were not in the transcript of the training data. Besides, the number of words in the model was much smaller (only 39 different words) than that in the TITML-IDN dataset. In addition, speech data from TITML-IDN have a different structure of sentences used in our primary data. TITML-IDN either contains complete sentences (subject-predicate-object-adverb) or non-complete sentences or only phrases, as these data were obtained from

the text corpus. Meanwhile, the speech in our primary data recorded from 10 respondents consists of complete sentences, as described in the section Data Collection.

#### IV. CONCLUSIONS

This study tested the performance of a deep bidirectional LSTM algorithm on speech-to-text conversion in Indonesian using MFCCs and spectrograms as features. The data used were complete sentences consisting of subject, predicate, object, and adverb spoken by some respondents. With the MFCCs and spectrograms, the algorithm achieved the highest WER of 0.2745% and 2.0784%, respectively, indicating the higher performance of the MFCCs on speech-to-text in the Indonesian language.

The algorithm was shown to successfully convert speech with different intonation and rhythm and achieved reasonable accuracy when applied to the TITML-IDN dataset.

However, the variation of words used in this study is still limited. Thus, in the future, the algorithm should be tested with speech with the higher variation of words and rhythms to increase its universality.

#### REFERENCES

- [1] B. Gold, N. Morgan, and D. Ellis, *Speech and Audio Signal Processing*. John Wiley & Sons, Inc., 2011.
- [2] P. Khilari and Bhope V. P., "A review on speech to text conversion," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 4, no. 7, pp. 3067–3072, 2015.
- [3] L. Deng et al., "Recent advances in deep learning for speech research at microsoft," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, vol. 26, no. 64, pp. 8604–8608.
- [4] A. Munir, S. Kashif Ehsan, S. M. Mohsin Raza, and M. Mudassir, "Face and speech recognition based smart home," in *2019 Int. Conf. Eng. Emerg. Technol. ICEET 2019*, pp. 1–5, 2019.
- [5] C. Jeyalakshmi, "Speech recognition of deaf and hard of hearing people using hybrid neural network," in *2010 2nd Int. Conf. Mech. Electron. Eng.*, vol. 1, pp. 83–87, 2010.
- [6] B. H. A. Ahmed and A. S. Ghabayen, "Arabic automatic speech recognition enhancement," in *Palest. Int. Conf. Inf. Commun. Technol. Arab.*, pp. 98–102, 2017.
- [7] H. Hotta, "Japanese speaker-independent homonyms speech recognition," *Procedia - Soc. Behav. Sci.*, vol. 27, pp. 306–313, 2011.
- [8] Z. A. Othman, Z. Razak, N. A. Abdullah, M. Yakub, and Z. Bin Zulkifli, "Jawi character speech-to-text engine using linear predictive and neural network for effective reading," *Proc. - 2009 3rd Asia Int. Conf. Model. Simulation, AMS 2009*, pp. 348–352, 2009.
- [9] A. Kumar, M. Dua, and T. Choudhary, "Continuous hindi speech recognition using monophone based acoustic modeling," in *Int. Conf. Adv. Comput. Eng. Appl.*, pp. 1–5, 2014.
- [10] T. P. Laksono, A. F. Hidayatullah, and C. I. Ratnasari, "Speech to text of patient complaints for Bahasa Indonesia," in *2018 International Conference on Asian Language Processing (IALP)*, pp. 79–84, 2018.
- [11] T. F. Abidin, A. Misbullah, R. Ferdhiana, M. Z. Aksana, and L. Farsiah, "Deep Neural Network for Automatic Speech Recognition from Indonesian Audio using Several Lexicon Types," *Proc. Int. Conf. Electr. Eng. Informatics*, vol. 2020–October, 2020.
- [12] S. M. Mon and H. M. Tun, "Speech-to-text conversion ( STT ) system using Hidden Markov Model ( HMM )," *Int. J. Sci. Technol. Res.*, vol. 4, no. 06, pp. 349–352, 2015.
- [13] L. Zhang, "An acoustic model for english speech recognition based on deep learning," *Proc. - 2019 11th Int. Conf. Meas. Technol. Mechatronics Autom. ICMTMA 2019*, pp. 610–614, 2019.
- [14] C. R. Liu, D. Qu, and X. K. Yang, "Long short term memory networks weighted prediction error for far-field speech recognition," *Proc. 2019 IEEE 8th Jt. Int. Inf. Technol. Artif. Intell. Conf. ITAIC 2019*, no. Itaic, pp. 200–203, 2019.
- [15] D. Wu, L. Ding, S. Deng, and S. Lu, "Research on speech recognition acceleration technology based on embedded platform," *Chinese Control Conf. CCC*, vol. 2019–July, no. 1, pp. 3663–3668, 2019.
- [16] Z. He, "Improving LSTM Based Acoustic Model with Dropout Method," *Proc. - 2019 Int. Conf. Artif. Intell. Adv. Manuf. AIAM 2019*, pp. 27–30, 2019.
- [17] A. Ahmed and S. Renals, "Word error rate estimation for speech recognition:e-WER, " In *Proc. of the 56th Annual Meeting of the Association for Computational Linguistics*, vol 2 short paper, pp. 20–24, 2018.
- [18] Audacity, *Guide to Using Audacity*. 2018.
- [19] M. Suzuki, N. Itoh, T. Nagano, G. Kurata, and S. Thomas, "Improvements To N -Gram Language Model Using Text Generated From Neural Language Model," *ICASSP 2019 - 2019 IEEE Int. Conf. Acoust. Speech Signal Process.*, pp. 7245–7249, 2019.
- [20] K. Kurniawan, "Indonesian NLP resources," 2018. [Online]. Available: <https://github.com/kmkurn/id-nlp-resource>. [Accessed: Feb 2020]
- [21] A. Graves and N. Jaitly, "Towards end-to-end speech recognition with transfer learning," *Int. Conf. Mach. Learn.*, vol. 32, 2014.
- [22] A. Graves, S. Fernández, F. Gomez, and J. Schmidhuber, "Connectionist temporal classification: labelling unsegmented sequence data with recurrent neural networks," *Proc. 23rd Int. Conf. Mach. Learn.*, pp. 369–376, 2006.
- [23] Speech Resources Consortium [Online] Available: <http://research.nii.ac.jp/src/en/TITML-IDN.html>.

# Smart Internet of Vehicles Architecture based on Deep Learning for Occlusion Detection

Shaya A. Alshaya

Department of Computer Science

College of Science and Humanities at alGhat, Majmaah University, Majmaah, 11952, Saudi Arabia

**Abstract**—In our days, the cyber world is developing due to the revolution of smart cities and machine learning technologies. The internet of Things constitutes the essential background of cyber technology. As a case study, the Internet of Vehicles is one of the leading applications which is developed quickly. Studies are focused on resolving issues related to real-time problems and privacy leakage. Uploading data from the cloud during the data collection step is the origin of delay issues. This process decreases the level of privacy. The objective of the present paper is to ensure a high level of privacy and accelerated data collection. During this study, we propose an advanced Internet of Vehicle architecture to conduct the data collection step. An occlusion detection application based on a deep learning technique is performed to evaluate the IoV architecture. Training data at Distributed Intelligent layer ensures not only the privacy of data but also reduces the delay.

**Keywords**—Internet of vehicle; deep learning; collaborative technologies; cloud; edge computing

## I. INTRODUCTION

The recent development of network technology gives birth to cyber intelligence technologies. The Internet of Vehicles (IoV) is a subfield of the Internet of Things (IoT) that has evolved a new generation of network technology [1].

The IoV case analyzes data based on artificial intelligence (AI) and Machine Learning (ML) methods. This field is still challenged by analyzing big data, privacy, and computational power limitation.

The IoV cooperates with the cloud platform to ensure permanent services. Two issues are faced with the IoV applications: (1) delay problem and (2) privacy violation [2].

We define an intermediate layer called edge computing to manage the vehicle network layer and cloud layer to overcome these problems. The edge computing layer is determined by the location information and the low latency. This is obtained because edge nodes are constituted by the Road Side Unit (RSU) [3].

The edge computing layer indeed solves the above problems, but other difficulties are bred as (1) increase in the amount of data, (2) an increase in the amount of data types, (3) difficult to adapt existing data collection related to embedded data, (4) need for intelligent methods to collect data, and (5) need for smart methods for the transmission [4].

Deep learning methods provide a solution for the above difficulty. They ensure the simulation of the data analysis to

avoid forged data based on interpretation mechanisms. Besides, deep learning methods reduce redundancy and provide high robustness of the system by following the inspection's high quality.

Therefore, moving from a centralized approach to edge computing reduces the unnecessary jumps to the network and improves latency [5]. Privacy is enhanced by adopting a Collaborative Learning (CL) technology. It manages data through multiple decentralized edge devices without exchanging them. It follows a training method different from the traditional cloud data center. The trained data were not collected directly from terminals [6]. The CL technology ensures privacy by gathering models and their updates from each RSU.

All RSU shares the model of the cloud data center. The CL performs the following steps: (1) the user provides data, (2) the local model trains the provided data, and (3) the trained model is uploaded to the cloud data center.

However, the CL mechanism provides more privacy and reduces delay by decreasing the training time of the sharing model in the cloud.

In light of this introduction, we can summarize contributions into three points:

- 1) Propose an advanced architecture at the edge computing layer for the IoV. The proposed ensures intelligent data collection.
- 2) Propose a deep learning method for the preprocessing step. The proposed reduces the delay.
- 3) Deploy the CL technology between the local model from the edge node and the cloud edge.

The next section presents the literature review. The proposed IoV architecture is introduced in Section III. The data preprocessing schemes designed according to a deep learning method and collaborative learning are described in Section IV. Results and analyzes are discussed in Section V. A conclusion is highlighted at the end of this article.

## II. LITERATURE REVIEW

This section attempts to summarize the latest research related to the Internet of Vehicles based on the following directives: (1) The assessment of the quality of services, (2) occlusion detection.

### A. Quality of Service Assessment

The safety of the road and the crowd's reduction is enhanced according to the evaluation of the QoS [7]. Van der Lee et al., [8] propose a scheduling method to evaluate the vehicle network QoS. This method was named a Time Synchronized Channel Hopping (TSCH). It introduces the interference diagram, which is dependent on internal interference and conflict. This attempt provides accurate analyzes of the network performance. The ratio of packet reception and latency compose the performance metrics.

Zhang et al., [9] introduce an open access geometry-based efficient propagation model. This model is composed of a connected vehicle in the traffic network that analyzes the QoS according to the principal component, multidimensional scaling, and variance. The QoS is carrying out for vehicle-infrastructure and vehicle-vehicle.

### B. Occlusion Detection in IoV Systems

Avoid occlusion in traffic is the subject of many related works. Determine the density of the crowded in urban is still challenged [10]. The process aims to detect vehicles and exploit the crowded density. This is ensured through preprocessing, motion detection, feature extraction, and classification steps [11]. There are many traditional and new techniques used for classification [12]. Deep learning is the kernel of these new approaches like CNN approaches.

In the traditional approaches, features are determined manually, and the classification step computes the similarity according to these predetermined features. For example, the authors in [24] applied HOG algorithm to detect humans. Hadjkacem et al. [13] used Gait-Appearance-based Multi-Scale Video Covariance (GAMS-ViCov) to detect a pedestrian. The estimation of a high-dense crowd through images is the main subject discussed in [14]. The author used Balanced Communication-Avoiding Support Vector Machine classifier for the detection. In [15], the authors are focused on the case of the detection of vehicles by applying Harr-like and Adaboost features. The limitation of representation is the main issue of the traditional approaches.

In the deep learning approach, features are determined automatically according to the provided dataset. This approach offers a broad representation ability [16]. We focus on related works based on CNN with two-stage because it enriches higher performance compared to the one-stage approach [17][18]. The CNN-two-stage includes a region-based convolutional neural network [19]. Martinez et al., [19] perform CNN as a selective search. The purpose is to detect two thousand candidate regions through a fixed-sized input image. The obtained result in terms of performance is higher than the traditional approach but this method is time-consuming. The authors in [20] and [21] attempt to reduce the time consuming. They used the selective once (SPP-Net method) to remove it (Fast R-CNN method) as described in [21]. This led to announce the region network method instead of selective search. The region network ensures convolutional operation and sharing computation. These advancements provide a higher accuracy at minimum time-consuming.

### III. PROPOSED IOV ARCHITECTURE SCHEME

We introduce the proposed IoV architecture for the collection and transmission of data on an edge computing layer during this section. This architecture is composed of four sub-layers, as described in Fig. 1.

**Data collection layer:** This layer is built based on nodes. RSUs collect data related to vehicles and roads as vehicle location and traffic information [22]. These data are sent continuously to the distributed intelligence layer through edge devices.

**Distributed intelligence layer:** This layer aims to ensure preprocessing and data analysis received from the data collection layer. This intermediate layer between RSU and centralized cloud computing provides a powerful step to increase storage capabilities, share communication resources, and improve computing. The distributed intelligence layer is responsible for data transfer methods and the network's evaluation [23].

**Data processing layer:** In this layer, the collecting sensing data are trained. Three functions are verified in this step: (1) Detect the data quality, (2) Detect data similarity, and (3) Detect relevant data. This step decreases the amount of data transmitted to the cloud. Only the training results are sent to the cloud instead of direct transmission to the centralized cloud. The data processing layer reduces delays related to communications and increases the privacy level [24].

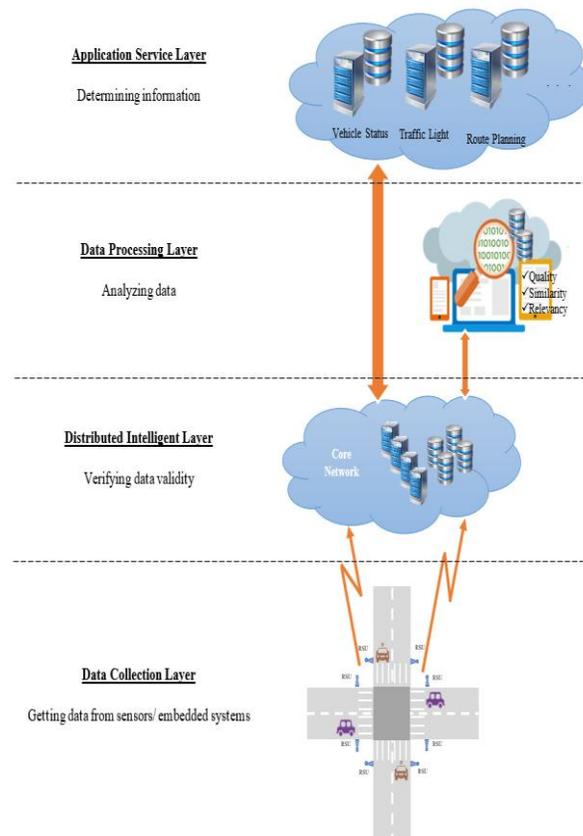


Fig. 1. Proposed IoV Architecture.

Application service layer: This layer offers information and helps make a decision based on the results obtained from sensing data. It monitors vehicle status, manages traffic lights, and updates route planning and directories.

Road sensors and systems embedded in vehicles transmit data to the RSU. The data collected by RSUs are moved to the core network. In this layer, data are conducted based on types. The data are verified according to the redundancy, quality, and relevancy at the data processing layer. When the verification is done, feedback is sent back to the distributed intelligent layer. Finally, the application service layer receives trained information. According to these results, the IoV systems are managed.

The proposed IoV architecture is built in terms of the network environment. The IoV model took into consideration network traffic and road environment. We carry out a strategy based on adaptive upload of the network bandwidth, environment, and transmission delay to enhance the collection data layer's performance.

The model divided the domain to ensure the Qos requirements. Divisions conditions are described by equation (1).

$$\begin{cases} D_i \in [x_i, y_i] \\ A_0 = \frac{x_0+y_0}{2} \\ A_i = \frac{x_i+y_i}{6} \\ H_e = Const \end{cases} \quad (1)$$

Therefore, building standards for the targeted network QoS evaluation was a necessity [25]. The Assessment standard is constructed by transforming qualitative data into quantitative data [26]. The network QoS is defined by the next parameters: namely, assessment indexes, bandwidth, delay, and rate of the lost packet.

Assessment indexes are composed of five levels of standard. Digital features are computed using the conditions presented in equation 1. Table I presents QoS features in the edge model.

TABLE I. DIGITAL FEATURES OF QOS ASSESSMENT IN EDGE MODEL

Assessment Level	Division	Digital features
Excellent	0.8-1	1.0,0.2 / 3,0.02
Good	0.65-1	0.78,0.15 / 5, 0.05
Average	0.5-0.65	0.64-0.1 / 5, 0.05
Poor	0.25-0.5	0.45-0.2 / 5,0.05
Very Poor	0.0.25	0,0.25 / 3,0.02

Then, we look for the optimal weight value. To achieve the target, we compute each secondary index's weight by applying the entropy method and the analytic hierarchy process. Then the square model is performed as described in equation 2.

$$\min g(w) = \sum_{i=1}^m \sum_{j=1}^n w [(s_j - w_j)p_{ij}]^2 + [(O_j - w_j)p_{ij}]^2 \quad (2)$$

Were  $s = [s_1 s_2 \dots s_n]^T$  is the computed weight through subjective analysis method,  $O = [O_1 O_2 \dots O_n]^T$  is the

computed weight through objective analysis method  $w = [w_1 w_2 \dots w_n]^T$  is the combined weight, the matrix  $P(p_{ij})^{m \times n}$  is the result of the standardized process of the measured data,  $m$  is the number of data, and  $n$  is the number of indicators.

The Lagrangian function is applied to reach the optimal weight, as mentioned in equations 3 and 4.

$$w = M^{-1} [B + \frac{1-E^T M^{-1} B}{I^T M^{-1} I} I] \quad (3)$$

Were

$$\begin{cases} M = diagonal [\sum_{i=1}^m p_{i1}^2, \sum_{i=1}^m p_{i2}^2, \dots, \sum_{i=1}^m p_{in}^2] \\ I = [1, 1, \dots, 1]^T \\ B = [\sum_{i=1}^m \frac{(s_1+v_1)p_{i1}^2}{2}, \sum_{i=1}^m \frac{(s_2+v_2)p_{i2}^2}{2}, \dots, \sum_{i=1}^m \frac{(s_n+v_n)p_{in}^2}{2}] \end{cases} \quad (4)$$

Then, digital features related to each level index are computed to determine the evaluation of the target layer edge using the entropy method (equation 5).

$$\begin{cases} E_i = \frac{E_{i1}E_{n1w1} + E_{i2}E_{n2w2} + \dots + E_{iq}E_{nqwq}}{E_n} \\ H_e = \frac{H_{e1}E_{n1w1} + H_{e2}E_{n2w2} + \dots + H_{eq}E_{nqwq}}{E_n} \\ E_n = E_{n1w1} + E_{n2w2} + \dots + E_{nqwq} \end{cases} \quad (5)$$

Were  $E_n$  measures the fuzziness and the probability of qualitative concept,  $E_i$  defines the qualitative concept in the number domain space,  $H_e$  is the doubt measure value of  $E_n$ .

The achieved digital features define precisely the adequate level of the edge model highlighted in Table I.

Table I applies many upload strategies based on selected network states. During this step, the scale of data is sent. The network congestion evaluation in this phase is composed of three levels: Good, Average, and Poor.

Results of the network status vary based on upload strategies. The network status is good when the RSU processes the image. The status moves to average when little videos are transmitted to the cloud. When the IoV uploads images and much video, the network status becomes poor.

#### IV. OCCLUSION DETECTION APPLICATION

The type of collected data is so crucial for the privacy and the amount of transmitted data. The proposed IoV architecture is evaluated via an occlusion detection application. Privacy is ensured by using a deep learning method to avoid the storage of the input data.

The detection of occlusion in urban traffic presents the main objective of each urban traffic surveillance video. This application is the most suitable to evaluate the proposed IoV architecture. The RSU applies the Convolutional Neural Network (CNN) for the input video to detect urban traffic status. The training is ensured at the distributed intelligent layer.

During this section, we focus on the detection of occlusion using the CNN method. The occlusion is considered based on global and local characteristics targets to detect precisely the vehicle position. Fig. 2 shows the occlusion detection framework.

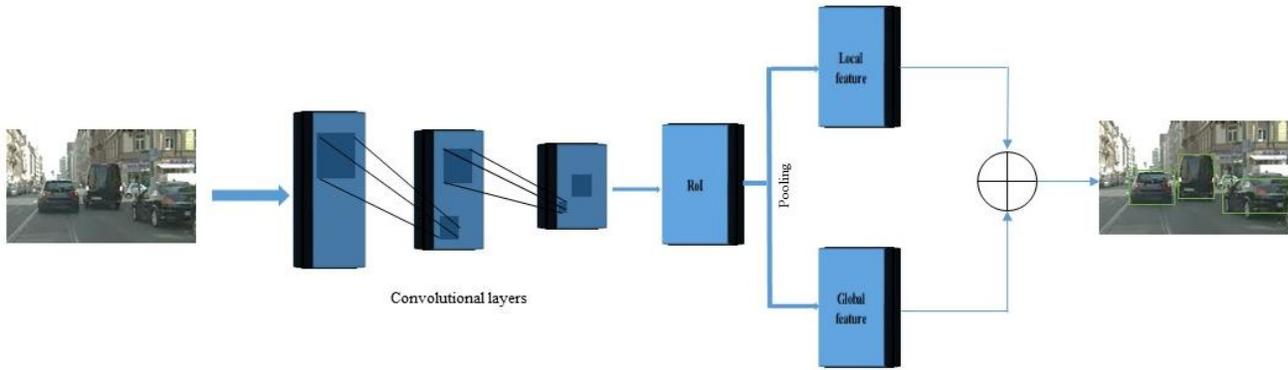


Fig. 2. Occlusion Detection Approach.

The local feature is extracted based on the position of the Region of Interest (RoI). A convolutional layer with size one and  $r^2 \times (C+1)$  channels are added to the last convolutional layer, where  $r$  defines the mask size, and  $C+1$  defines the background and the classes. The average of pooling related to the RoI indicates the probability of vehicle. Then, the bounding-box is labeled the same. Some channels are added to the bounding-box to compute the average pooling on the convolutional layer. The obtained result defines the values of bounding-box regression.

We consider the global feature of the video streaming of urban traffic enhances the accuracy of vehicle detection. The RoI pooling is used in this case to avoid errors related to the size of vehicles. Then, we apply  $1 \times 1$  convolutional layer to select the global feature.

The concatenation of these features provides accurate detection.

## V. EXPERIMENTATIONS

The proposed IoV architecture and the occlusion detection application are verified during this section. We start to display the achieved results related to the occlusion detection application.

The occlusion detection using a deep learning algorithm is tested based on UIUC dataset [27]. This dataset is composed of 550 grayscale image cars. Images are both single-scale and multi-scale. We use 400 images for training and the rest for testing.

The learning rate starts from 0.01, then changes to 0.001 after 18000 iterations. The training requires 302s to be performed. The training is characterized by momentum, which is about 0.92, and weight decay which is about 0.002.

In the complete evaluation of the proposed architecture, we use 150 images. We introduce two metrics: (1) True Positive Rate (TPR), and (2) False Positive Rate (FPR).

Fig. 3 shows the Receiver Operating Characteristics graph (ROC) of occlusion detection. The ROC is defined as the relationship between TPR and FPR. The ROC curve overgrows.

The best baseline highlighted in Fig. 3 is 0.8. In comparison with Shivani et al., in [27], we demonstrate that our method had the best baseline.

We drew also, the accuracy rate curve according to the baseline, as shown in Fig. 4. The curve is composed of one peak which is achieved at value 0.91. Then, the curve go-down and stabilizes under the accuracy rate value is 0.2. The baseline is selected at 0.9.

The processing requests 54.2 ms to be performed. The proposed architecture of data collection and transmission is evaluated according to the detection of occlusion in traffic.

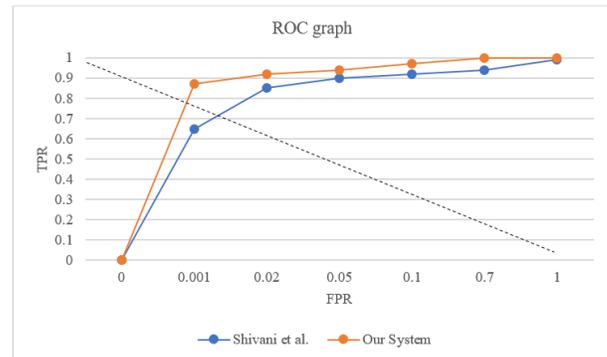


Fig. 3. ROC Curves.

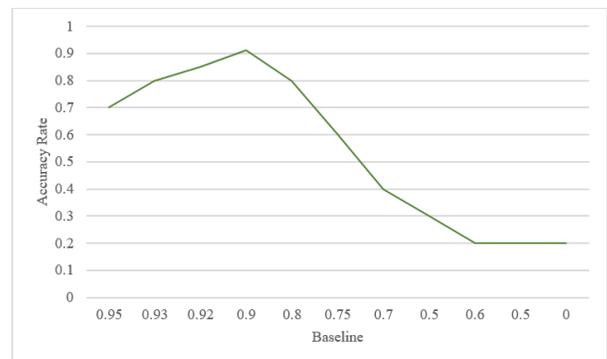


Fig. 4. Baseline and Accuracy of Image Traffic.

The recognition accuracy and latency is computed to study the performance in-depth. In our case, the evaluation is done through 550 images in which the number of cars per image varies between two and ten. The latency is computed using 2.4 G network environment. Its curve is reduced and did not exceed 6s, as shown in Fig. 5. In contrariwise, the recognition accuracy curve (Fig. 6) depends directly on the data size. The more the data bigger, is more the accuracy is improved. This is well justified due to the use of deep learning. The accuracy achieves a rare about 95%.

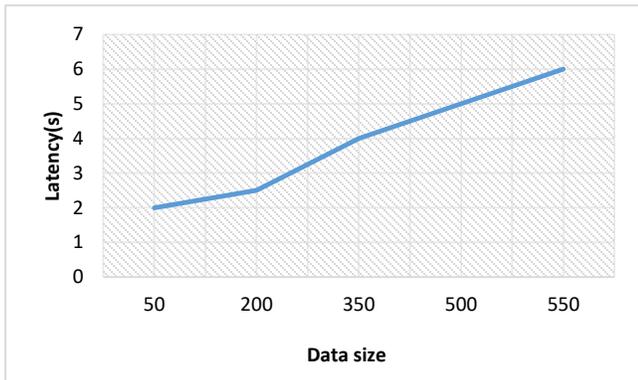


Fig. 5. Latency Curve.

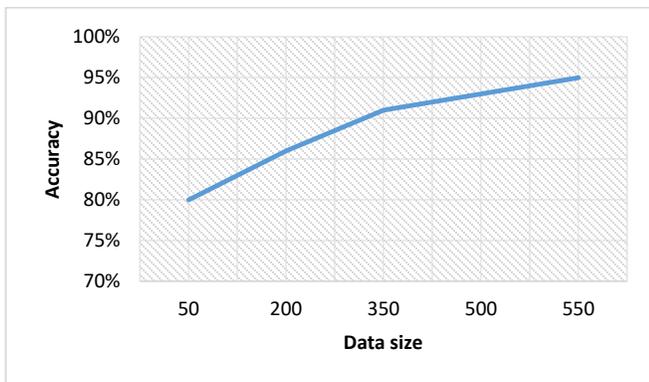


Fig. 6. Accuracy Curve.

The experimental results prove that the proposed IoV architecture obtains high performance in the detection of occlusions in decreasing delay and ensuring a high level of privacy.

## VI. CONCLUSION

The network intelligence technology is faced with the leakage of privacy problem. Provide a new preprocessing technique to detect redundant data is so important. Therefore, this paper uses deep learning and edge computation to design an accurate data collection and preprocessing scheme. The cloud data centers and edge devices are managed through collaborative learning technologies and deep learning models. The IoV architecture describes the enhancement of the adaptability and efficiency of data collection. Detection of occlusion is performed to verify the correlation of data. Achieved results highlight the reduction of data uploaded to the cloud and the safety of the user's privacy.

## ACKNOWLEDGMENT

The authors would like to thank Deanship of Scientific Research at Majmaah University for funding this project under the number R-2021-61.

## REFERENCES

- [1] T. Wang, H. Luo, X. Zheng, and M. Xie, "Crowdsourcing mechanism for trust evaluation in CPCS based on intelligent mobile edge computing," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1–19, 2019.
- [2] Y. Wu, H. Huang, Q. Wu, A. Liu, and T. Wang, "A risk defense method based on microscopic state prediction with partial information observations in social networks," *J. Parallel Distrib. Comput.*, vol. 131, pp. 189–199, 2019.
- [3] X. Liu, T. Wang, W. Jia, A. Liu, and K. Chi, "Quick convex hull-based rendezvous planning for delay-harsh mobile data gathering in disjoint sensor networks," *IEEE Trans. Syst. Man, Cybern. Syst.*, 2019.
- [4] T. Wang, Y. Mei, W. Jia, X. Zheng, G. Wang, and M. Xie, "Edge-based differential privacy computing for sensor–cloud systems," *J. Parallel Distrib. Comput.*, vol. 136, pp. 75–85, 2020.
- [5] B. Yin, Y. Wu, T. Hu, J. Dong, and Z. Jiang, "An Efficient Collaboration and Incentive Mechanism for Internet of Vehicles (IoV) With Secured Information Exchange Based on Blockchains," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1582–1593, 2019.
- [6] K. Yan, W. Shen, Q. Jin, and H. Lu, "Emerging privacy issues and solutions in cyber-enabled sharing services: From multiple perspectives," *IEEE Access*, vol. 7, pp. 26031–26059, 2019.
- [7] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things," *IEEE Trans. Ind. Informatics*, vol. 16, no. 3, pp. 2054–2062, 2019.
- [8] T. van der Lee, A. Liotta, and G. Exarchakos, "Time-scheduled network evaluation based on interference," in *2018 IEEE International Conference on Cloud Engineering (IC2E)*, 2018, pp. 323–332.
- [9] L. Zhang, Y. Liu, Z. Wang, J. Guo, and Y. Huo, "Mobility and QoS oriented 802.11 p MAC scheme for vehicle-to-infrastructure communications," *Telecommun. Syst.*, vol. 60, no. 1, pp. 107–117, 2015.
- [10] S. A. Alshaya, "Open Challenges for Crowd Density Estimation," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 1, 2020, doi: 10.14569/IJACSA.2020.01110123.
- [11] A. A. Yilmaz, M. S. Guzel, I. Askerbeyli, and E. Bostanci, "A vehicle detection approach using deep learning methodologies," *arXiv Prepr. arXiv1804.00429*, 2018.
- [12] S. Zhang, L. Wen, X. Bian, Z. Lei, and S. Z. Li, "Single-shot refinement neural network for object detection," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 4203–4212.
- [13] B. Hadjkacem, W. Ayedi, M. Ben Ayed, S. A. Alshaya, and M. Abid, "A novel Gait-Appearance-based Multi-Scale Video Covariance Approach for pedestrian (re)-identification," *Eng. Appl. Artif. Intell.*, vol. 91, p. 103566, 2020.
- [14] S. A. Alshaya, "Estimation of a high-dense crowd based on a Balanced Communication-Avoiding Support Vector Machine classifier," *Int. J. Comput. Sci. Netw. Secur.*, vol. 20, no. 6, pp. 195–201, Jun. 2020.
- [15] A. Tannouche, K. Sbai, M. Rahmoune, R. Agounoune, A. Rahmani, and A. Rahmani, "Real Time Weed Detection using a Boosted Cascade of Simple Features.," *Int. J. Electr. Comput. Eng.*, vol. 6, no. 6, 2016.
- [16] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural Comput.*, vol. 18, no. 7, pp. 1527–1554, 2006.
- [17] M. Everingham, S. M. A. Eslami, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman, "The pascal visual object classes challenge: A retrospective," *Int. J. Comput. Vis.*, vol. 111, no. 1, pp. 98–136, 2015.
- [18] T.-Y. Lin et al., "Microsoft coco: Common objects in context," in *European conference on computer vision*, 2014, pp. 740–755.

- [19] A. Alonso, M. Del Valle, J. A. Cecchini, and M. Izquierdo, "Asociación de la condición física saludable y los indicadores del estado de salud (II)," 2003.
- [20] K. He, X. Zhang, S. Ren, and J. Sun, "Spatial pyramid pooling in deep convolutional networks for visual recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 37, no. 9, pp. 1904–1916, 2015.
- [21] S. Ren, K. He, R. Girshick, and J. Sun, "Faster r-cnn: Towards real-time object detection with region proposal networks," in *Advances in neural information processing systems*, 2015, pp. 91–99.
- [22] T. Wang, L. Qiu, A. K. Sangaiah, G. Xu, and A. Liu, "Energy-efficient and trustworthy data collection protocol based on mobile fog computing in Internet of Things," *IEEE Trans. Ind. Informatics*, vol. 16, no. 5, pp. 3531–3539, 2019.
- [23] Z. Xia, Z. Hu, and J. Luo, "UPTP vehicle trajectory prediction based on user preference under complexity environment," *Wirel. Pers. Commun.*, vol. 97, no. 3, pp. 4651–4665, 2017.
- [24] Q. Tang, M. Xie, K. Yang, Y. Luo, D. Zhou, and Y. Song, "A decision function based smart charging and discharging strategy for electric vehicle in smart grid," *Mob. Networks Appl.*, vol. 24, no. 5, pp. 1722–1731, 2019.
- [25] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and T. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2679–2689, 2019.
- [26] B. Xiong, K. Yang, J. Zhao, and K. Li, "Robust dynamic network traffic partitioning against malicious attacks," *J. Netw. Comput. Appl.*, vol. 87, pp. 20–31, 2017.
- [27] S. Agarwal, A. Awan, and D. Roth, "Learning to detect objects in images via a sparse, part-based representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 26, no. 11, pp. 1475–1490, 2004.

#### AUTHOR'S PROFILE

Dr. Shaya Alshaya: Coming from the invaluable educational background in both under and postgraduate degrees from Saudi Arabia, USA, and Italy, Dr. Alshaya has put his knowledge into practicality as an international entrepreneur, his endeavors include education and research, ICT sector. He is a member of the National Association of Industrial Technology, the Institute of Electrical Engineers and the Sloan-C Online Association amongst others. Dr. Alshaya has a wealthy experience as Head of IT in Majmaah University, Saudi Arabia. His experience as a researcher, consultant, project manager and information technologist has allowed him to bring his extensive experience of technology planning, training and implementation to all of the projects he endeavors. The numerous national and international companies that utilize his expertise as a consultant evidence Dr. Alshaya's success. Dr. Alshaya's wealthy experience, vast knowledge is integral to his vision and future projects.

# Smart Home Energy Management System

## A Multi-agent Approach for Scheduling and Controlling Household Appliances

Yasser AL Sultan<sup>1</sup>

Department of IS  
King Abdul Aziz University  
Jeddah, Saudi Arabia

Ben Salma Sami<sup>2</sup>

Department of CIT  
King Abdul Aziz University  
Jeddah, Saudi Arabia

Bassam A. Zafar<sup>3</sup>

Information System Department  
FCIT, King Abdulaziz University  
Jeddah, Saudi Arabia

**Abstract**—Home energy management system has been selected as an attractive research issue due to its ability to enhance energy security by including devices, entertainment systems, security systems, environmental controls, etc. Home automation is incorporated as a potential technology to ensure efficient electricity performance without interruption, solve power demand problems and coordinate devices with innovative technologies. In this context, our proposal seeks to implement an accurate home energy management system. The proposed approach aims to improve uninterrupted electricity production and provide comfortable services to families. To implement correct system operations and meet each device's power demand, a Real Time Energy Management System (RT-EMS) will be implemented and discussed through some required tasks using the Multi-Agent System (MAS). Each agent will be determined according to some criteria to implement the appropriate design and meet each device's power demand. The obtained results will show that the proposed system meets the general objectives of RT-EMS.

**Keywords**—Home energy management; multi-agent system; real-time system; energy recovery

### I. INTRODUCTION

Home Energy Management System has been selected as a potential technology for connecting devices, sensors, etc., using communication technologies and platforms. Innovative home technologies are gradually integrated into our daily activities and our physical and emotional relationships with our communities [1] - [2]. This means that we are starting to create a separate structure with transparent social interaction. This concept is similar to that predicted by Mark Weiser in 1991 [3]. The authors suggest in [4] that the idea of home automation is designed to interfere with specific components, especially labels, air conditioning, light switches, default rates and many consumer activities. Simultaneously, the authors stated in [5] that this trend could be primarily justified by the lower cost and financial advantages of industrial manufacturing and technologies in academic research. In this context, the economic impact of improving knowledge will also have the potential to generate \$ 5-7 trillion in the economy during 2025. The authors mentioned in [6] that in the past, the smart home was limited to strategic sectors (engineering, infrastructure and satellites) but that it is now actively interested in domestic activities, for example, network control systems, intelligent park systems and smartphone applications.

In [7], innovative technologies are designed and incorporated to ensure comfort, enhance excellence and

improve safety and health. To achieve this goal, the automation house has developed a detection and management system capable of using the integrated data of various detectors and hierarchical sensors. While the authors have shown in [8] - [9] that the home automation environment will create a considerable amount of data, it helps to build new approaches and branches of research such as the Internet of Things (IoT), Big Data, artificial intelligence etc. In [10], the smart home's conception has changed due to different contexts (domestic platforms, innovative technologies, IoT, etc.). Besides, smart home technologies are aimed at identifying, monitoring and coordinating devices. The authors have shown in [11] that the intelligent home is chosen as an environment in which consumers are integrated into all these modern innovations, which are also appreciated. Software-defined network (SDN) has been seen as a good research question and has been explicitly used to replace older innovative home instruments [12]. The authors mention in [13] - [14] that SDN seems to offer new ways of proposing cross-platform concepts. The control and application of machine learning technology quickly update SDN capabilities. The authors reported in [15] - [16] that data from the QianJia.com survey show that smart homes' future growth in China is about 20%, to 357.6 billion yuan, from 2012 to 2020. Improving the age of smart homes will dramatically improve people's daily lifestyles. The authors report in [17] that at CES, the smart home continued to evolve aggressively two years later. Many new elements, including the Parrot flowerpot and the robot Soma bar, have attracted attention.

In [18], the smart home consists of an infrastructure that provides precise communication between devices and equipment using a combination of wired and wireless technologies. This combination allows for seamless integration that facilitates access to home systems and provides a personalized home environment. In [19], several methods were selected and implemented to coordinate, collect and process data between the two devices. The authors suggest in [20] that machine learning was chosen as an exciting research question because of their opportunities and their efficiency in processing the data collected between devices. Computing and data challenges in innovative home systems focus on effective ways to manage data sharing between devices [21]. In [22], several approaches including advanced measurement infrastructure (AMI), intelligent sensor technology, home energy storage system (HESS), intelligent home systems and local area network (HAN).

Home Energy Management (HEM) was seen as a potential solution due to its ability to manage appliances and control energy demand in a smart home. HEM refers to using energy management systems to monitor and collect data that includes generation, distribution, and transmission of electricity [23]. HEM is a monitoring and data collection application for energy management systems, covering power grid production and delivery, i.e. the idea of an intelligent grid. This definition has been widely supported to suggest a way forward for electricity supply [24]. In [25], HEM is the key to successful, intelligent grid management on the demand side for home system users. HEM works with real-time monitoring and regulation of various home appliances according to user needs through smart assistive devices controlled by human interfaces in intelligent homes to reduce electricity prices and improve energy efficiency. The authors have mentioned in [26] that due to growing concerns about the sustainability of renewable energies and environmental emissions, HEM was created to manage renewable energies locally (wind turbines, solar panels, etc.). The authors stated in [27] that according to the rapid developments in the field of advanced innovations in electricity and sustainable energy, these intelligent systems could be introduced in HEM. SHEM was faced with a crucial concern in a decentralized generation, demand reduction and peak periods to provide consumers or service providers with adequate solutions [28].

The smart home is a growing emerging technology continuously now. It incorporates many new technologies to improve the quality of human life. Indeed, Home automation devices often do not handle issues independently, as most are single-use tools. However, it is different when it comes to a home automation system connecting various devices and applications to all data. For this reason, households are also looking for forms and methods to change their lifestyle by taking advantage of newly accessible IoT technologies. Energy demand and measurement are considered the primary goal of householders. For this reason, this paper extends the ideas of previous studies by using:

(+) As we are convinced, an intelligent HEM is confident that the used energy management systems are still incapable of controlling and coordinating properly among sources.

(+) we tend to monitor and request power for each device, which will help us in the future to keep costs and electricity consumption under control and extend the life of appliances. We intend to make intelligent devices capable, through some agents of the predictive control system, to forecast, control and measure voltage, which can regulate power consumption. A HEM system will be implemented and discussed through many required tasks using MAS to implement correct system operations and meet each device's power demand.

(+) we introduce the Smart Home Device Scheduling (SHDS) issue that formalizes the MAS scheduling problem.

The remaining part of the paper is organized as follows: Section I introduces Introduction and related works. Section II provides a brief description of the whole system. Section III discusses in details the Hierarchical Home Energy management. Section IV discusses the obtained results "Finding and results". We conclude our work in Section V.

## II. DESCRIPTION OF THE WHOLE PROPOSED SCHEME

This sub-section describes the overall Home energy management system using MAS given by Fig. 1(a); the presented hierarchical scheme explains the relationship between appliances and Smart home blocks based on MAS. So, the proposed Smart Home agents tend to produce an enormous amount of data that can be calculated in the local server, limiting access to service requirements. Additionally, each agent will transfer data collected from a neighbor agent using intelligent devices, IoT applications, and wireless to perform tasks (see Fig. 1(b)). As we can see, the proposed scheme is composed of three main blocks, which are:

- 1) BLOCK-A: Home Devices and Data Management
- 2) BLOCK-B: Monitoring and Data Processing
- 3) BLOCK C: System Control for User Request

The Supervising agent is used to administer a new system control measure based on the updated BLOCK C data, ensuring:

- All (BLOCK A and BLOCK C) should be synchronized in decisions allowing each agent to minimize slow reaction response and increase performance speed during data processing.
- Send new control measures to alert agent devices to pre-stop those with a high peak using a fixed system parameter threshold, thereby minimizing power consumption levels.

Request: Send current energy consumption to Recovery Agent in real-time. The monitoring agent should verify and confirm the following tasks:

- Data is already broadcast in real-time per hour.
- The broadcast data is then compared appropriately controlled with the user's need to recover the energy demand.
- All decision functions of each agent are synchronized at the regional level.
- Any data change will be tracked after being compared and permitted by the alert outside the threshold.
- Rotate a new loop request for fresh input

Action: Send the updated household appliance consumption data to the supervisor agent to confirm the following tasks:

- According to its highest consumption level, data is collected in an orderly fashion, the lowest level in a recovery agent.
- Recovery agent compares data high/low peaks are measured between current and past.
- Check for simultaneous changes to update the system panel, informing the supervisor agent of the decisions to be involved in the coming hours.
- The changes determine the user's pre-request for the following hours, which devices should be chosen to minimize his operation during the daily routine.

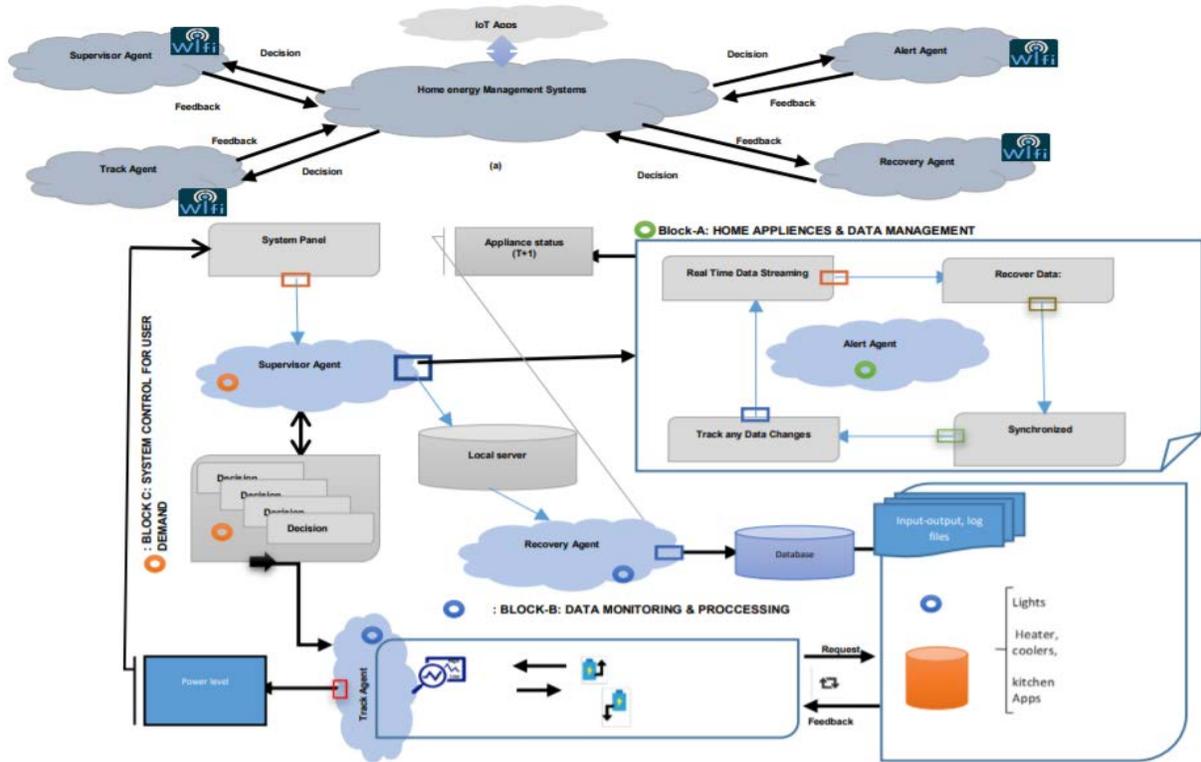


Fig. 1. Innovative Home Energy Management Design: (a) Descriptive Design; (b) Proposed Multi-Agent System Control Design.

To execute the proposed model in real-time, quick prototyping is used, providing that the quick concept checks with the versatility to produce acceptable outcomes is done with the right environment. Since the design will be evaluated on Python / Thread Simulator AOP (Fig. 2(a)), which has an interacting Toolbox dealing with real-time control diagrams, the algorithms established can quickly be loaded into a microcontroller STM32 Discovery F4. Thus, the coordination between the STM32F4 board and device can be carried out quickly without any problems with a Processor-in-the-Loop (PIL) simulation check. In reality, the design can be run in the discovery board of STM32F4 while holding a PIL block. The method can also be used in the STM32F4 discovery board via the development of the PIL block while keeping the simulation on the device connected to the on-board board via ST-LINK (see Fig. 2(b)). PIL verification allows loading and executing a hexadecimal output file launched on the goal microcontroller with understandable map generation from the software.

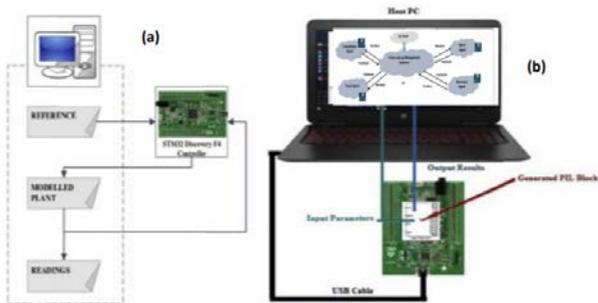


Fig. 2. Real-time Implementation Scheme.

Modelling system constraints is vital in achieving overall action arrangements, including interconnections and interaction with other agents and systems to automate and plan challenges (see Fig. 3). Our work evaluates four different types of residential loads, storage loads and moving non-moving and thermal loads. To exploit their complex behaviors for intelligent home automation, we consider several electrical devices representing each charged class (see Table I). Two periods ( $T_H$ ,  $T_L$ ) are considered to assess and control energy demand. Thus, these periods denote high and low peak hours.

$T_H$ : High Peak hours and Shoulder Peak hours

$T_L$ : Low Peak hours and Off-Peak hours

#### A. Device Schedule

We need to define the behavior of smart devices operating in Smart Home (SH) over the time horizon to monitor the energy needs [29]. The scheduling time horizon for household appliances is generally fragmented into an amount of times slots that are expressed by:

$$\phi(t) = d_{\text{Home-energy Management}} = \frac{v(t = 60 \text{ min} = 1h)}{s} \quad (1)$$

$$\begin{cases} \text{Load}(\text{Home - Appliances}) = \sum_{\text{Hour}=1}^{24} (\text{App}(H) * I_{\text{Rate}}^{\text{App}}) = [1, 0] \\ \sum_{j=1}^N \sum_{H=1}^{24} P_{\text{total}}^{\text{App}} \leq I_{\text{total Grid}} / R_{nE} \end{cases}$$

TABLE I. APPLIANCES CLASSIFICATION

Appliances Categories	Operational Time (Hours)	Power Ratings (KWh)	Appliances Class
Air Conditioner	14	1.5	Shiftable
Steam Iron	3	1.2	Shiftable
Oven	4	1.23	Fixed
Watching Machine	3	5	Non-shiftable
Blender	2	0.3	Fixed
Tumble Dryer	4	3.3	Non-shiftable
Water Pump	8	1	Shiftable
Electric Water Heater	8	2.6	Shiftable
Ceiling Fan	12	0.1	Fixed
Desktop PC	0.3	10	Fixed
Refrigerator	20	0.22	Shiftable

$d_{HEM}$  represents the length of the time slot, and  $s$  represents the time slot per hour, meaning the scheduling time horizon [30]. The time duration authorized for intelligent home Appliances (App1... App) scheduled is expressed by (3):

$$\phi(d_{HEMS}) = [d_{HEM} - 1, d_{HEM} - 2, d_{HEM} - 2, \dots, d_{HEM} - n] \quad (2)$$

The consumed power by equipment during time slots is shown as follows:

$$I_{Consumed}^{App} = \begin{bmatrix} I_1^1 & I_2^1 & I_3^1 & \dots & I_n^1 \\ I_1^2 & I_2^2 & I_3^2 & \dots & I_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ I_1^n & I_2^n & I_3^n & \dots & I_n^n \end{bmatrix}; \begin{pmatrix} \text{Power consumption} \\ \text{Calculation} \end{pmatrix} \quad (3)$$

### III. HOME ENERGY MANAGEMENT

Home Energy Management's main objective is to provide a smooth, continuous electrification operation in housing developments, with a demand rationalization that facilitates the reductions in energy product prices. Thus, a practical and intelligent supervisory approach may be used to preserve, on the one side, an equilibrium between demand and output and, therefore, regulating the allocation of household electricity to change the system stability. Furthermore, activating/deactivating household appliances, the data on each household appliance's power usage, the overall consumption, and the house's self-generated electricity through the provided power, carry out the monitoring. These intelligent devices can remotely process and evaluate all home appliances. Thus, using an appropriate communication protocol between smart devices becomes a necessity that must be partnered with the Energy Management Unit to achieve steady and optimal performance. More broadly, in automated systems management, multi-agent technology has proven its efficiency and sustainability. In this vein, the multi-agent system is based on the concept of agent interaction that can be integrated into hardware or software hardware. Thus, this proposal aims to develop an energy management unit based on hierarchical agents created to control the distribution of flows to provide a comfortable and intelligent electrification service for the household. The

proposed design methodology is defined through a state machine model that offers the opportunity to describe the system events encountered and the transitions from one state to another. Home Apps produces early large volumes of streaming data, the sensor is configured to extract that flow of data in hours frequently skips so it can to take benefit of this data, warn agent input the system a new data each time with the correct data intervals 24/7 (Fig. 3), and then track agent responds to changes from the real-time agent Simultaneously outputting the results throughout the pc simulations.

Fig. 4 describes the status of each appliance using agent coordinators. As seen, a supervisory agent's value is found by decision-making sent to each agent after obtaining its state of knowledge. The two primary system processes, "Total Energy" and "Energy Recovery," are outlined as noted. The diagram summarizes both previously mentioned states and transformations as well as the two apparent states (ST'4"/SR"4) "relevant total energy and recovery Agent, respectively. The state of SR "4" illustrates the system's response against incapability to provide energy demand. In this situation, the system controls the operation of household appliances to align the energy dues with the output of flows taking into consideration the following activities:

Task1: Set the number of home appliances on;

Task2: Check the threshold by comparing the levels, response time, and recovery rate via agent recovery;

Task3: Turn off household devices one by one considering operation priority until reaching the power balance between the production and demand;

State machine Control: Home appliances and energy demand and consumption are cited as below:

- Onset Storage Process (SS "1") : Time Ts= "1".
- Onset Recovery Process (SR "1") : Time TR= "1".
- Home Battery Storage process (SS "2") : Time Ts= "2".
- Home Battery Consumption process (SR "2") : Time TR= "2".
- Battery Charging Process (SS "3") : Time Ts= "3".
- Battery Discharging Process (SR "3") : Time TR= "3".
- Battery Charging (on/off) (SS "4") : Time Ts= "4".
- Appliances Operation Control (SR "4") : Time Ts= "4".

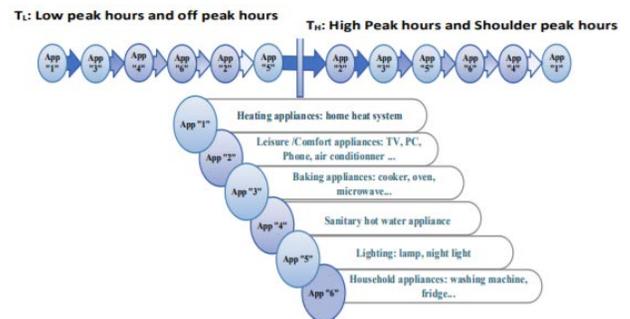


Fig. 3. Operation Priority of Home Appliances.

The home appliances control system aimed to equilibrate the energy efficiency dues with the flows, considering the following everyday household priority.

- Track 1: Set the lower and highest priority energy usage during Morning/Night of home appliances;
- Track 2: Check the high and regular peak updates of consumed power level thresholds from each appliance via recovery agent;
- Track 3: Switch off/on household appliances one by one consider the higher operation level consumption prioritized until reaching the stable power between the production, and demand which can be recovered from the recovery agent deficiency;

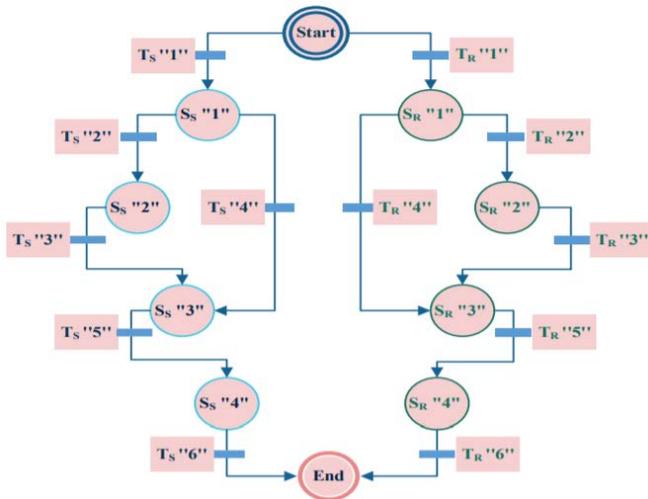


Fig. 4. State Machine Control Algorithm: Energy Consumption and Storage [31].

In the multi-agent system, the behavior is presented and discussed in Fig. 5. The Multi-Agent System presented four agents:

- A Supervisor Agent, which controls and synchronizes all system agents. The Supervisor Agent is also in charge of making data requests, triggering alerts for energy consumption outside the established thresholds and training a Machine Learning model capable of predicting the system's energy consumption.
- The Tracker Agent is the type of agent that monitors and controls each device, providing consumption data to the Supervisor Agent and the Alert Agent.
- The Alert Agent is the type of agent who receives the Supervisor Agent's alert requests when the Tracker Agent has notified energy consumption outside the established thresholds.
- The Recovery Agent is the type of agent in charge of data persistence in the system. The Recovery Agent also receives data request requests from the Supervisor Agent to train the Machine Learning model of power consumption.

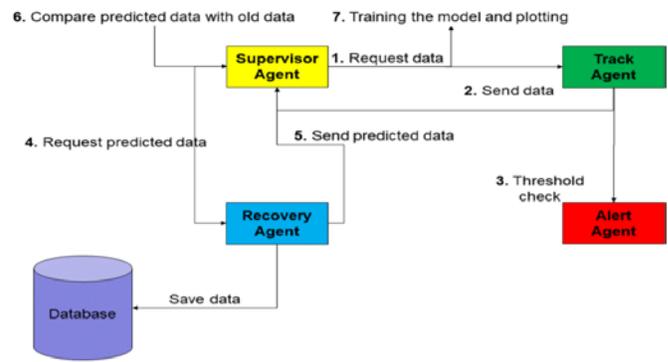


Fig. 5. The Proposed Multi-Agent System.

#### IV. FINDING RESULTS

To assess and demonstrate the feasibility of the developed system and the sophistication of the approach to energy management, a real-time prototype home energy design is tested, taking into account the regular use of various appliances in the Python AOP / Simulation real-time environment. The sustainable energy demand includes multiple electrical devices, the energy source, and energy recovery for the backup and storage unit. To perform the test simulation, a home energy database is used to collect the devices' actual energy profiles on four consecutive days during High Peak hours, Shoulder peak hours, and Low peak hours and off-peak hours. The calculated device profiles of different household appliances.

We have chosen the Matlab / Simulink environment to increase the feasibility of the proposed control approach, demonstrate the autonomous hybrid-electric system's capacity, and satisfy the load demand, whatever the instances. The analysis involves a variety of electric equipment, photovoltaics sources, and energy recovery and storage systems. For more than four days, the KSA forecast database offered advice on actual solar radiation and ambient temperature profiles, grouped into two successive periods:

$T_H$ : High Peak hours and Shoulder peak hours

$T_L$ : Low Peak hours and Off-Peak hours

We have often used a realistic load profile that is the most critical aspect for designing any electric power system. In reality, the load variance typically represents the electricity usage of various appliances, taking into account different household requirements. Fig. 6 and Fig. 7 Display measured household appliance consumption profiles during  $T_H$  and  $T_L$  periods.

According to the obtained results, solar energy supply generates less power in  $T_L$  than during  $T_H$ . This belongs to the irradiation change influenced by climate change. Low power consumption was reported due to the lack of frequent electricity systems (see Fig. 8). Both phase and deficit levels are observed simultaneously during winter and summer system operations. The transition between the states monitored by the original power management defines the flow of power distribution and the behavior of the system. The above requests to multiple control situations are to determine decision (Fig. 9) appropriately. To analyze system performance, Table II

summarizes the average distributed power flow over four consecutive days. The device achieves consumption peaks, evidenced by the intense activity of household appliances, for

the reported performance. The transported active flows are mainly affected by changing conditions.

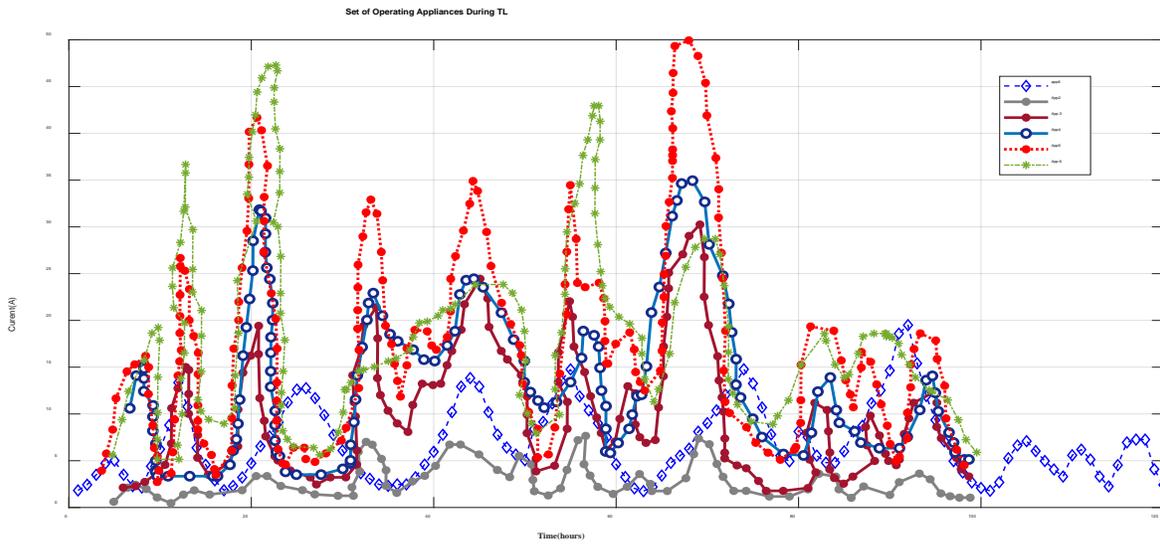


Fig. 6. Household Appliances: (a): Set of Operating Appliances during  $T_L$

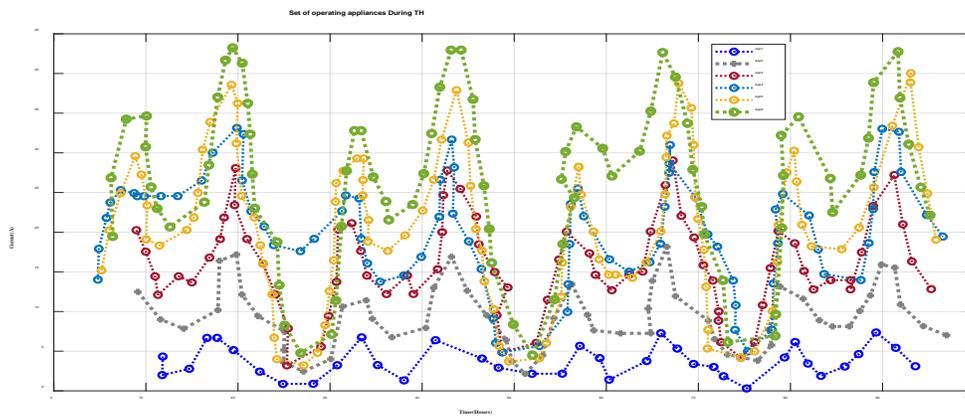


Fig. 7. Household Appliances: (a): Set of Operating Appliances during  $T_H$

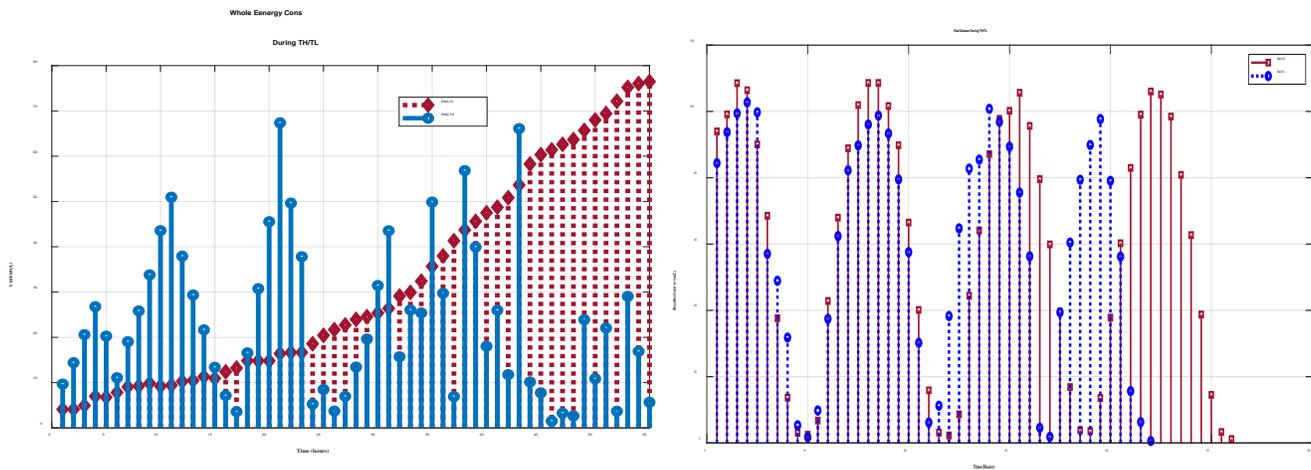


Fig. 8. RHES Specification Input Parameters during " $T_L, T_H$ ". (a) Overall Energy utilization. (b) Solar Radiation.

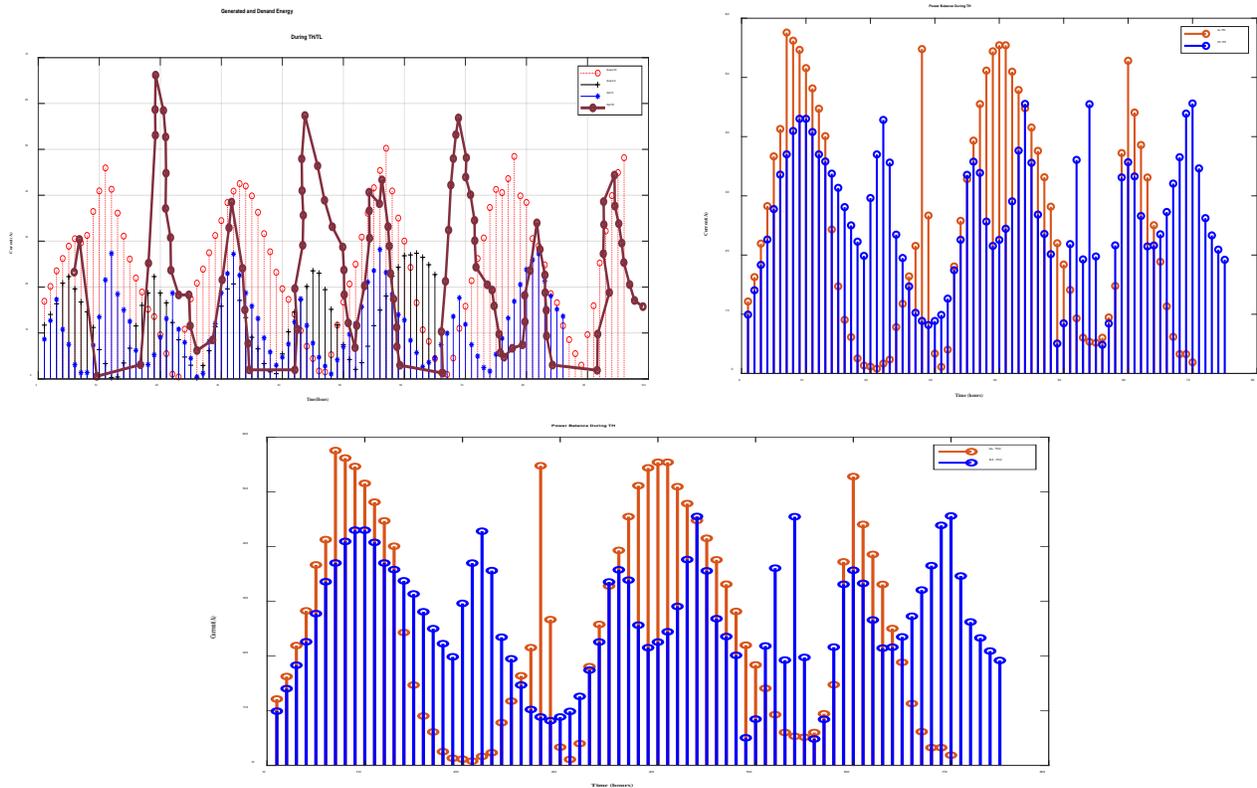


Fig. 9. RHEs Power Balance during "TL"; During "TH" (a, b): (c) Both Energy Demand and Generated.

TABLE II. AVERAGE OF ENERGY FLOWS DISTRIBUTION

Peak Hours		Generation Average (A)	Consumption Average (A)
High Peak Hours ( $T_H$ )	Day 1	11.10	11.71
	Day 2	11.50	15.57
	Day 3	11.25	17.95
	Day 4	10.59	7.93
Low Peak Hours ( $T_L$ )	Day 1	11.70	16.04
	Day 2	11.72	16.23
	Day 3	11.10	16.23
	Day 4	11.09	16.23

## V. CONCLUSION

The current research has been performed on a precise home energy management system (EMS). The proposed HEM is designed to control the power requirements between the home appliances and the power supply components meet to meet the MAS's Home load demand. The proposed system has been combined as a renewable source database and home appliances. The HEM approach, based on a multi-agent system, was implemented to control energy production and consumption. This approach aimed to improve system performance by speeding up response times and enhancing synchronization between all components during  $T_H$  and  $T_L$  periods.

## ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression "one of us (R. B. G.) Thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

## REFERENCES

- [1] D. C. Khedekar, A. C. Truco, D. A. Oteyza, and G. F. Huertas, "Home automation - A fast - Expanding market," *Thunderbird International Business Review*, vol. 59, no. 1, pp. 79–91, Jun. 2016, doi: 10.1002/tie.21829.
- [2] M. Zaki, A. Alquraini, and T. Sheltami, "Home automation using EMOTIV: Controlling TV by Brainwaves," *Journal of Ubiquitous Systems and Pervasive Networks*, vol. 10, no. 1, pp. 27–32, Mar. 2018, doi: 10.5383/jusp.n.10.01.004.
- [3] O. Krejcar, L. K. Cheng, and J. Dvorak, "Application of universal remote control of non-smart home appliances for smart home concepts," *International Journal of Digital Enterprise Technology*, vol. 1, no. 3, p. 276, 2019, doi: 10.1504/ijdet.2019.10019067.
- [4] Y. Amri and M. A. Setiawan, "Improving smart home concept with the internet of things concept using RaspberryPi and NodeMCU," *IOP Conference Series: Materials Science and Engineering*, vol. 325, pp. 1–11, Mar. 2018, doi: 10.1088/1757-899x/325/1/012021.
- [5] A. Ndolo, "Smart home monitoring," *Qeios*, Nov. 2019, doi: 10.32388/508747.
- [6] L. Katsinoulas, M. Papoutsidakis, and D. Tseles, "Smart home applications for energy saving and increased security," *International Journal of Computer Applications*, vol. 175, no. 8, pp. 38–44, Oct. 2017, doi: 10.5120/ijca2017915650.
- [7] Q. Liu, X. Yang, and L. Deng, "An iBeacon-based location system for smart home control," *Sensors*, vol. 18, no. 6, p. 1897, Jun. 2018, doi: 10.3390/s18061897.

- [8] P. Siano, I. Shahrour, and S. Vergura, "Introducing smart cities: A transdisciplinary journal on the science and technology of smart cities," *Smart Cities*, vol. 1, no. 1, pp. 1–3, Jul. 2018, doi: 10.3390/smartcities1010001.
- [9] A. Veiga and C. Abbas, "Proposal and application of bluetooth mesh profile for smart cities' services," *Smart Cities*, vol. 2, no. 1, pp. 1–19, Dec. 2018, doi: 10.3390/smartcities2010001.
- [10] A. Nag and S. C. Mukhopadhyaya, "Smart home: Recognition of activities of elderly for 24/7; Coverage issues," *International Journal on Smart Sensing and Intelligent Systems*, vol. 7, no. 5, pp. 1–10, 2020, doi: 10.21307/ijssis-2019-118.
- [11] T. Daum, H. Buchwald, A. Gerlicher, and R. Birner, "Times have changed: using a pictorial smartphone app to collect time–use data in rural Zambia," *Field Methods*, vol. 31, no. 1, pp. 3–22, Sep. 2018, doi: 10.1177/1525822x18797303.
- [12] P. Wang, F. Ye, and X. Chen, "Smart devices information extraction in home Wi-Fi networks," *Internet Technology Letters*, vol. 1, no. 3, pp. 1–6, Apr. 2018, doi: 10.1002/itl2.42.
- [13] S. Al-Fedaghi, "Design of home circulation: Application to smart homes," *International Journal of Smart Home*, vol. 10, no. 12, pp. 131–144, Dec. 2016, doi: 10.14257/ijsh.2016.10.12.13.
- [14] A. C. Jose, R. Malekian, and B. B. Letswamotse, "Improving smart home security; integrating behaviour prediction into smart home," *International Journal of Sensor Networks*, vol. 28, no. 4, pp. 253–269, 2018, doi: 10.1504/ijsn.2018.096464.
- [15] U. Saxena, J. S. Sodhi, and Y. Singh, "Software defined security architecture for a smart home networks using token sharing mechanism," Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019, pp. 2551–2559, doi: 10.2139/ssrn.3370160.
- [16] K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, "Software-defined networking (SDN): A survey," *Security and Communication Networks*, vol. 9, no. 18, pp. 5803–5833, Dec. 2016, doi: 10.1002/sec.1737.
- [17] A. M. Alshnta, M. F. Abdollah, and A. Al-Haiqi, "SDN in the home: A survey of home network solutions using Software Defined Networking," *Cogent Engineering*, vol. 5, no. 1, May 2018, doi: 10.1080/23311916.2018.1469949.
- [18] C. González García, D. Meana-Llorián, B. C. Pelayo G-Bustelo, J. M. Cueva Lovelle, and N. García-Fernandez, "Midgar: Detection of people through computer vision in the Internet of Things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes," *Future Generation Computer Systems*, vol. 76, pp. 301–313, Nov. 2017, doi: 10.1016/j.future.2016.12.033.
- [19] V. Plantevin, A. Bouzouane, and S. Gaboury, "The light node communication framework: A new way to communicate inside smart homes," *Sensors*, vol. 17, no. 10, p. 2397, Oct. 2017, doi: 10.3390/s17102397.
- [20] J. Sebastian and Y.-L. Hsu, "Talking to the home: IT infrastructure for a cloud-based robotic home smart-assistant," *Gerontechnology*, vol. 17, no. s, pp. 102–102, Apr. 2018, doi: 10.4017/gt.2018.17.s.099.00.
- [21] P. Purwanto, H. Hermawan, and S. Suherman, "Integration of Solar Energy Supply on the Smart Home Micro Grid to Support Efficient Electricity and Green Environment," *IOP Conference Series: Earth and Environmental Science*, vol. 239, pp. 1–8, Feb. 2019, doi: 10.1088/1755-1315/239/1/012032.
- [22] D. Liciotti, M. Bernardini, L. Romeo, and E. Frontoni, "A sequential deep learning application for recognising human activities in smart homes," *Neurocomputing*, vol. 396, pp. 501–513, Jul. 2020, doi: 10.1016/j.neucom.2018.10.104.
- [23] B. S. Sami, "An intelligent power management investigation for stand-alone hybrid system using short-time energy storage," *International Journal of Power Electronics and Drive Systems (IJPEDS)*, vol. 8, no. 1, pp. 367–375, Mar. 2017, doi: 10.11591/ijpeds.v8.i1.pp367-375.
- [24] H. Yamagishi, "Microbial contamination and countermeasures in home bathrooms and toilets," *Indoor Environment*, vol. 22, no. 1, pp. 73–79, 2019, doi: 10.7879/siej.22.73.
- [25] S. Kim, H. Christiaans, and J. S. Baek, "Smart homes as product-service systems: Two focal areas for developing competitive smart home appliances," *Service Science*, vol. 11, no. 4, pp. 292–310, Dec. 2019, doi: 10.1287/serv.2019.0248.
- [26] H. Mehrjerdi, "Peer-to-peer home energy management incorporating hydrogen storage system and solar generating units," *Renewable Energy*, vol. 156, pp. 183–192, Apr. 2020, doi: 10.1016/j.renene.2020.04.090.
- [27] J. Yoon, "Deep-learning approach to attack handling of IoT devices using IoT-enabled network services," *Internet of Things* [online], Jun. 2020, doi: 10.1016/j.iot.2020.100241.
- [28] J. Kim, "HEMS (Home Energy Management System) base on the IoT smart home," *Contemporary Engineering Sciences*, vol. 9, no. 1, pp. 21–28, 2016, doi: 10.12988/ces.2016.512316.
- [29] B. Sami, "A Survey of Hydrogen Energy and I-Energy Applications: Household Intelligent Electrical Power Systems", *IEEE Access*, vol. 8, pp. 55181–55203, 2020. Available: 10.1109/access.2020.2981349.
- [30] B. Sami, "Intelligent Energy Management for Off-Grid Renewable Hybrid System Using Multi-Agent Approach", *IEEE Access*, vol. 8, pp. 8681–8696, 2020. Available: 10.1109/access.2019.2963584.
- [31] B. Slama and Nasri S, "Design and implementation of an intelligent home energy management system: A realistic autonomous hybrid system using energy storage", *International Journal of Hydrogen Energy*, 43(42), pp. 19352–19365. 10.1016/j.ijhydene.2018.09.001.

# Trade-off between Energy Consumption and Transmission Rate in Mobile Ad-Hoc Network

Ashraf Al Sharah<sup>1</sup>, Mohammad Alhaj<sup>2</sup>

Computer Engineering Department  
Al-Ahliyya Amman University, Amman, Jordan

Firas Al Naimat<sup>3</sup>

Medical Engineering Department  
Al-Ahliyya Amman University, Amman, Jordan

**Abstract**—Mobile Ad-Hoc Networks are decentralized systems of mobile nodes where each node is responsible for computing and retaining the routing and topology details. The autonomous nature of the nodes stresses more on the way of handling power consumptions. This raises a concern about how to improve the power efficiency that leads to a better battery life of the mobile nodes. It is important to balance between power and transmission rates to improve the network lifetime and reduce the sudden failure of the nodes. In this paper, a new transmission power control-based scheme is proposed that allows the mobile nodes to achieve a tradeoff between balancing transmission rate and power consumption. Through defining and updating two tables for every node that contain the average transmission rate for the neighboring nodes and number of times the neighboring node is used for data transmission. We validate our proposed scheme using several test cases.

**Keywords**—Coalition; MANETs; power-aware routing; power consumption; transmission power control-based; transmission rate

## I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) are wireless networks where a group of mobile nodes operate independently in order to configure and hold their ad-hoc network routing and topology information. MANETs do not rely on present infrastructure, but instead each mobile node broadcast messages to the neighboring nodes. They are popular in different military and domestic applications such as ship-to-ship, law enforcement communications and ecological monitoring [1].

MANET provides a decentralized control with uncertain connections among nodes and a rapid mobility of hosts. The mobile nodes act as routers, monitors and decision makers. It has a limited availability of resources where the processing power, memory capacity, battery performance, and bandwidth relies on the mobile nodes of the network. MANET provides vulnerable and insecure operating environment; and it suffers from low transmission rate, data overhead according to not choosing the optimal bandwidth and power consumption. Since its topology varies dynamically and frequently, mobile nodes may appear and disappear abruptly.

Cooperation between mobile nodes in MANETs is important to assure the best performance and utilization. For that purpose, game theory is used to solve interactions between nodes in the network. Game theory is the best practice to study situations of mutual interest among mobile nodes, solve conflict between them and find the suitable

actions for an individual node [2]. There are two kinds of game theory: a) Non-cooperative game where the strategic choices of each node are chosen based his own interest without any commitment with the others; and b) Cooperative game where nodes have mutual interest with each other and can make binding commitments. All nodes in this paper are cooperative, have mutual interests and exchange transmission details between the neighboring nodes.

The efficient utilization of power is a major concern in MANETs where nodes in the network are constrained by power consumption and computational resource. The battery life time determines the mobility time of a node in a network. With the increasing of mobility time, the power consumption increases and the remaining node battery life decreases. The decision of route selection decision is becoming more challenging than just selecting the route with the lowest power consumption [3][4]. Using the power-aware routing to examine the power consumption of the nodes when making routing decisions improves the performance of routing in MANETs [5].

Transmission rate is another concern in optimizing the performance of routing in MANETs. The transmission rate in MANETs is normally unstable and keeps changing during the time. In order to assure the stability of transmission rates, it is important to select the right rate between the neighboring nodes for data exchanging and avoid data overhead or data loss in the transmission channel. A previous research in [6] proposes a mechanism called Hand-shake Rate Adaptation (HRA) that avoids wrong selections of transmission rate in MANET by specifying the average transmission rate between its mobile nodes. Mobile nodes can select the appropriate transmission rates to ensure that bandwidth requirements are met. The mechanism adopts a decentralized approach where nodes are involved in calculating transmission rate for the neighbors, therefor by knowing the neighbors' transmission rates, individual node is able to select the proper rates. Mobile nodes in MANETs also have different transmission power based on the amount of transmitted data. Choosing a wrong transmission rate increases the power consumption and affects the efficiency of its power utilization [7][8][9][10].

A literature survey in [11] summarizes 51 reviewed papers about power-efficient routing schemes in MANETs based on topology information and protocol operations. The survey categorizes the routing schemes into six approaches:

- 1) Link state-based where each node finds the shortest path through exchanging the routing table information with the neighbors.
- 2) Source initiated-based where the sending node perform the discovery procedure when it is necessary to find the path to the destination node.
- 3) Transition power control-based which focuses on adjusting the transmission power between the source node and the destination node.
- 4) Load balancing-based which focuses on balancing energy usage among all nodes by choosing a routing path that includes previously unused mobile nodes instead of choosing the shortest path.
- 5) Location-based which selects the routing path between the source and destination nodes using the geographic position techniques such as global positioning system GPS or location aided routing (LAR) [12].
- 6) Multicast-based which broadcasts the data from one source to all destinations within a multicast group.

In this paper, we propose a scheme based on transmission power control-based approach to provide a balance between the transmission rates and power consumption of mobile nodes. The scheme uses a cascaded single-hop to discover the utilization and the average transmission rate of the neighboring node. Each node maintains two tables: one contains number of times that a node utilizes the neighbor nodes in data transmission, and another table contains the assigned average transmission rate between each node. Based on the two tables, nodes can select the suitable neighbor node in transmitting data. The scheme increases the life time of the network and reduces the rate of failing nodes.

The paper is organized as follows, Section II presents the background and related work; Section III presents the proposed model; Section IV presents the proposed algorithm; Section V presents the simulation and results; Section VI provides conclusion and future work.

## II. BACKGROUND AND RELATED WORK

MANET is a decentralized type of networks where each node contributes in forwarding data to the neighbor nodes [13]. MANET does not rely on routers, access points or other communication infrastructure; instead data is transmitted through the neighboring nodes based on defined routing algorithm. Several applications are available for simulating the behavior of MANET. A common one is called Network Simulator NS-2 [14]. NS-2 is an open source simulation tool which provides a discrete event simulating for TCP, routing, and multicast protocols over wired and wireless networks.

The transmission power control-based approach is introduced in a survey [11] with eight reviewed papers that are similar to our proposed scheme. Chang and Tassiulas in [15] propose a flow augmentation routing (FAR) protocol to balance the traffic between the nodes by selecting the routes and the corresponding power until the batteries of the nodes drain-out is maximized. This allows defining the optimal levels of transmission power and the optimal route. Li et al. in [16] propose an online max-min power-aware routing

protocol (OMM) that uses Dijkstra's algorithm to find the optimal path for a given source-destination pair. An empirical competitive ratio is developed to optimize the lifetime of MANET through minimizing the consumed power and maximizing the minimal residual energy of the node. Doshi and Brown in [17] introduce a minimum energy routing (MER) scheme to select a path that minimizes the energy required for routing a packet from the source to the destination. The path is selected by finding the link cost in terms of the packet transmission energy, the energy required for route discovery and the energy consumed to maintain routes. Avudainayagam et al. in [18] propose a device- and energy-aware routing (DEAR) protocol for heterogeneous wireless ad hoc network with two types of nodes: externally-powered nodes and battery-powered nodes. Based on the energy and the device awareness of the routing protocol, the externally-powered nodes have higher priorities of the transmission and perform more routing functions. Rishiwal et al. in [19] propose a power-aware routing (PAR) protocol to improve the network lifetime through selecting a less congested and more stable routes for data transmission. The selection is based on three metrics: the overall energy of a path, the status of battery lifetime and the type of data to transfer. Yanez-Marquez et al. in [20] introduce a minimum spanning tree (MST) to select the optimal routing by calculating the minimum spanning tree using a low complexity algorithm based on the binary decision diagrams (BDDs). Lalitha and Rajesh in [21] propose an hoc On-demand Distance Vector Range Routing (AODV\_RR) that improves the overall energy consumption of MANETs by reducing the communication overhead. Finally, Katiravan et al. in [22] propose an Energy Efficient Link Aware Routing with Power Control (ELRPP) to select the optimal routing using three metrics: residual energy, signal to noise ratio (SNR) and link quality. A comparison between the proposed scheme and the previous routing schemes within the same category is presented in Section V.

There are also recent researches which have been devoted great efforts on power in mobile ad-hoc networks. Kannan and Rajaram in [23] design and develop strategy of QoS aware power efficient multicast routing protocol (QoS-PEMRP) suitable for mobile nodes. The development is based on QoS metrics such as average group delivery ratio, average power consumption and average delay. Papageorgiou et al. [24] propose an energy-efficient multicasting algorithm that select the optimal energy-efficient set of nodes for multicasting. Three parameters are considered: the node residual energies, the transmission powers, and the set of covered nodes. Khan et al. in [25] focuses in reducing the coast of coding mechanism by reducing the size of data used for permutation. The idea of the mechanism is that the source permutes global encoding vectors only and not considering the whole message symbols to achieve better energy consumption. Rahman in [26] proposes an algorithm that selects the route over earlier most forward within radius (MFR) method based on weighted combination of metrics of distance, velocity and battery power. The proposed algorithm improves the load balancing and increases the network performance.

Ghode and Bhojar in [27] introduce energy constraints in Zone Routing Protocol (ZRP) in order to make the protocol works efficiently in MANET and improves network lifetime. Hassan and Muniyandi in [28] propose a QoS-routing algorithm that supports the QoS parameters of energy and delay using Cellular Automata (CA) with Genetic Algorithm+African Buffalo Optimization (GAABO) techniques. The research aims to improve the network lifetime as well as the end-to-end delay. Lu and Zhu in [29] propose a new protocol called EDCMRA. EDCMRA is a multicast routing that maintains the energy efficiency and delay of data transmission. It uses the possible multicast trees those traced in route request process as initial input chromosomes, and uses the common subtree of the any of given two multicast trees as crossover point.

Kamboj and Sharma in [30] introduce modern solutions and models that enables multicasting. The models aim to improve the network life time. While Zhao et al. in [31] present a measure called Energy Efficiency Metric (EEM), that is the result of aggregate hop-count values and relative levels of increment of lifetime. Papanna et al. in [32] addresses the consumption of energy and maximizing the route lifetime in MANETs using the Energy Efficient and Lifetime Aware Multicast (EELAM) modeling topology and compare the results the other bench marking models like EACNS, EDCMRA. Sarkohaki et al. in [33] utilizes the artificial immune system (AIS) to improve the efficiency of the Optimized link state routing protocol (OLSR). OLSR is a mobile routing protocol that uses Dijkstra's algorithm to define the shortest route between source and destination. Ray and Turuk in [34] propose an energy conservation technique to reduce the transmission power of a node in MANETs. The technique is called Location Based Topology Control with Sleep Scheduling that allows a node to go to sleep state based on the traffic condition. Alani et al. in [35] propose a new method to improve the energy efficiency and routing performance through adapting lion optimization algorithm after specifying all possible paths in MANET. Bhatia et al. [36] propose an algorithm that is an extension of Dynamic Source Routing (DSR) routing protocol. The algorithm is used to optimize the routing bandwidth and improve the energy consumption.

In summary, it is obvious that the works above have addressed features similar to our work. The major advantage of the proposed scheme is that it achieves a tradeoff between balancing transmission rate and power consumption. The scheme algorithm is simple and developed based on cascaded single-hop discovery. The scheme algorithm selects the routing path by creating routing tables for each neighboring node. The table contains the average transmission rate for the neighboring nodes and number of times the neighboring node is used for data transmission. The proposed approach affects the overall network lifetime by increasing the battery power of the nodes and decreasing the power consumption in the network.

### III. PROPOSED NETWORK MODEL

MANETs suffer from different challenges that affect their operations. One of these challenges is battery life time and

restriction of battery power. Operations of mobile nodes in MANETs depend on the power consumption. When mobile nodes run out of battery, their ability to operate in the network traffic are affected which then affects the overall network lifetime. The lifetime of MANETs can be improved by decreasing the power consumption in the network.

The proposed model of the network is considered as a coalition repeated game, where network nodes cooperate with each other's during the repeated network life cycle. For each node in the network, a scheme of two routing tables is created. The first routing table defines the number of times the node used its neighbor for data transmission within period of time. It provides an approximate of power consumed in each node by finding how many times it's been used for data transmission. The second routing table defines the transmission rates between the node and its neighbor. The purpose of the scheme is to balance between the battery power consumption of the nodes and the transmission rates. The tables are shared with the neighboring node to guarantee fairness between nodes and control node usage in the network.

The proposed model uses cascaded single-hop routing to define the connection path between the source and destination nodes. In a cascaded single-hop routing, a sending node selects an optimal next neighboring node in a sequence of single hops. Using the routing tables at each single-hop, the sending node forwards the data to the next node based on the neighbor minimum number of time the node is used for transmission and the average rate.

Fig. 1 describes a sample of the network model of our scheme with five nodes. The scheme can be applied to any number of nodes. Each node has its own scheme where  $r_{ij}$  is the average transmission rate between two neighbor nodes  $i$  and  $j$ ;  $t_{ij}$  is the number of times that node  $i$  used node  $j$  for data sending. Based on the proposed scheme, a node selects the neighbor for data transmission as follows:

$$average (r_{ij}) \times number\ of\ times(t_{ij}) = \min(r_{ij} \times t_{ij}) \quad (1)$$

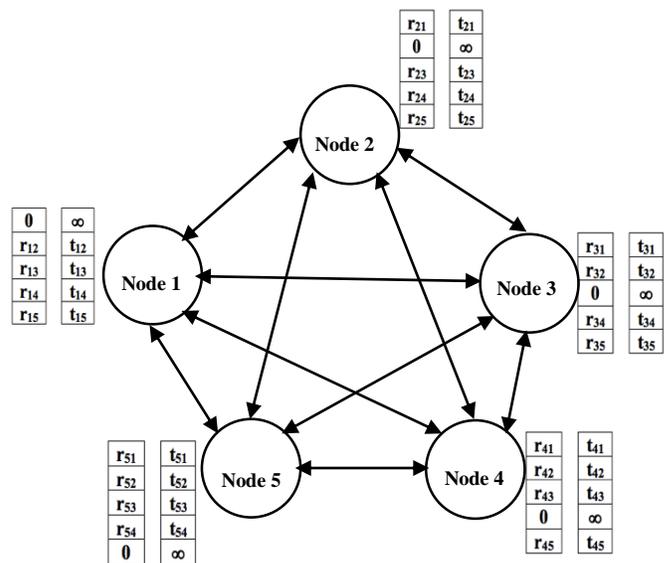


Fig. 1. A Sample of the Proposed Network Model.

The tables are updated every  $T$  time period where  $T$  is inversely proportional to the amount of data transmitted across the whole network. Each node is allowed to define its own  $T$  time period in order to provide reasonable parameters of its  $r_{ij}$  and  $t_{ij}$ . As a definition, the average transmission rate between a node and itself is zero ( $r_{ij} = 0, i = j$ ) and the number of times a node used itself for data sending is infinity ( $t_{ij} = \infty, i = j$ ).

In the proposed network model, mobile nodes communicate with their neighboring node to exchange the average transmission rates and the number of time that each node has been used for data transmission to decide which node the data will be sent through. In order to prioritize the importance of the two parameters in the proposed scheme, we introduce relative weights that is used to tradeoff between them based on the user demand and network condition. The purpose of the relative weights is providing a flexibility to the network model and comply with network demands. For a given network model with  $N$  number of nodes, let  $\alpha$  is a relative weight of the average transmission rates  $r$  and  $\beta$  is the relative weight of number of times a node used its neighbor for data transmission  $t$ . The characteristic function  $f_T$  is defined as:

$$f_T(N) = \alpha \cdot r + \beta \cdot t \quad (2)$$

where  $0 < \alpha < 1, 0 < \beta < 1$  and  $\alpha + \beta = 1$

Due to the mobility in MANETs, it is important to keep tracking and monitoring of the neighboring nodes at any time. The relative weights provide the network the flexibility and reliability of prioritizing the important parameter based on the network condition. The relative weight  $\alpha$  helps to provide the maximum weight of the transmission rate parameter, while  $\beta$  helps to provide the power usage of a given node.

#### IV. PROPOSED SCHEME ALGORITHM

In this section, we introduce the algorithm of our proposed model. Several assumptions are considered in order to operate the algorithm. For mobile nodes, we assume that there  $N$  rational mobile nodes, all nodes have the same battery capacity, individual nodes have weak chance to survive alone and all nodes are able to create two tables one for the neighbors average transmission rate and the other one is for the neighbors' power. For the network, we assume that network is not of a hierarchical type and the goal of the cooperative game is to form a stable network.

The algorithm below describes the data transmission of a node after selecting the proper neighboring node within a time slot  $T$ . The time slot  $T$  and the weight parameters  $\alpha$  and  $\beta$  can be changed according to the network requirements. Initially, the weight parameters  $\alpha$  and  $\beta$  are assigned equally to all coalition nodes. Then each node checks the transmission rate of its neighbor nodes and the number of times that a node has been used for data transmission. If node  $i$  selects a specific node  $j$ , then node  $i$  announces to all neighboring nodes, otherwise it sends nothing. When node  $i$  uses node  $j$ , all neighboring nodes updates the power usage table. The algorithm is repeated every  $T$  time slot to keep tracking the nodes power usage.

1. Assign values for  $\alpha$  and  $\beta$
2. Start for all nodes
3. Node  $i$  checks its transmission rate table and power table to assign Neighbor node  $j$  for data sending according to equation (1)
4. If node  $i$  used node  $j$  for sending data then
  - 4.1. Announce a node power usage for this specific node
  - 4.2. Else find another node
  - 4.3. End if
5. Store this power usage value in the power table
6. Share power usage value with neighbors at every timeslot.
7. All nodes continue to update their power and transmission rates tables.

#### V. SIMULATION AND RESULTS

The proposed approach is implemented using NS-2 Simulator (NS-2, 2021). The parameters for the simulation is shown in Table I where several test cases are produced based on the variations in number of neighboring nodes, weight parameters, network delay, network overhead, transmission rate and power consumption. Some of test cases show the effect of increasing the neighboring nodes with respect to their life time while others shows the effect of varying of the  $\alpha$  and  $\beta$  weight parameters of the characteristic function with respect to, the network delay and overhead. A sample of 50, 80, 100 and 150 as size of coalition nodes are used in simulating the test cases. The following sections describe the results of the simulated test cases.

TABLE I. PARAMETERS FOR SIMULATION

Parameters	Level
Area	4000 * 3200
Speed	18 m/s
Radio range	800 m
MAC	802.11
Simulation time	1200s
Size of the coalition nodes	50, 80,100 and 150
Network interface type	Wireless
Channel type	Wireless channel
Transmission rate	Vary
Initial energy	100 Joule
Transmission power	0.4 Joule
Receiving power	0.05 Joule

##### A. Energy Consumption

In this section, the test case focuses on the amount of remaining energy based on specific node. The selected node is tested based on different coalition sizes. For fairness and precise results, we assume equal energy consumption for every transmitted data. Fig. 2 describes the percentage of the remaining energy based on the coalition sizes defined in Table I. The figure shows that by increasing the size of coalition, the energy consumption for a given node is

decreased (the remaining battery energy are 51%, 60%, 66% and 80% for coalition sizes 50, 80, 100 and 150, respectively). This is because the number of neighboring node increases, so the number of times a node is used for data transmitting is reduced.

Fig. 3 shows a comparison of the overall remaining energy (in percent) of a network before and after using our scheme for a sample of 150 coalition size. As the time passes, the saving of coalition energy is improved by the proposed scheme (energy saved by 19% at 60 sec. and 28% at 120 sec).

### B. Weight Parameters

In this section, the test cases focus on  $\alpha$  and  $\beta$  weight parameters. These parameters allow the network to monitor the bias towards either the data transmission rate or the energy consumption of mobile nodes. The default situation is to have an equal value of ( $\alpha = \beta = 0.5$ ). We investigate the effects of changing the weight parameters on network overhead and number of dead nodes.

1) *Network throughput and delay*: Fig. 4 describes the relationship between the network throughput and the coalition size. The test case uses a sample of 50, 80, 100 and 150 coalition sizes. Initially all coalition sizes have an equal; and as time passes the throughput of higher coalition size becomes greater. At time= 60 sec, throughput of 50 coalition size is 51% while it is 68% for 150 coalition size. At time= 120 sec, throughput of 50 coalition size is 83% while it is 98% for 150 coalition size.

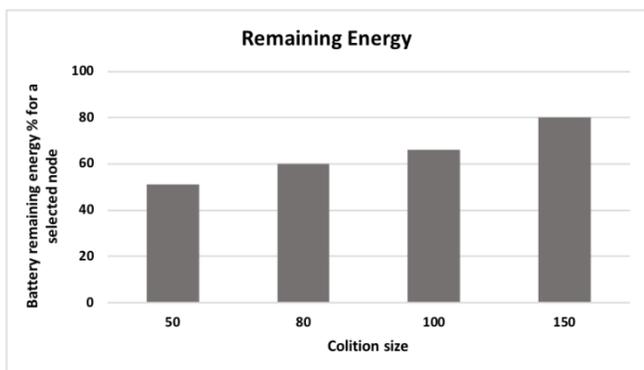


Fig. 2. Percentage of the Remaining Energy for a Coalition of Nodes.

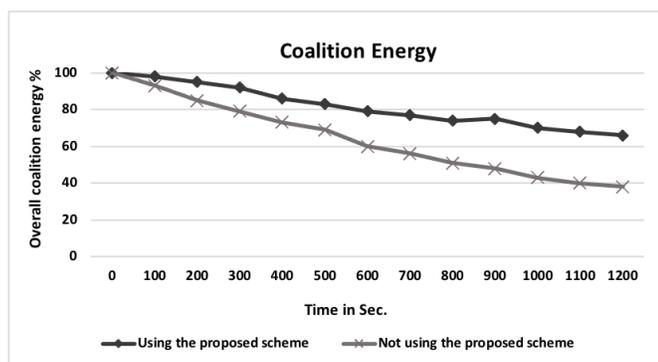


Fig. 3. Overall Coalition Energy Percentage with and without using the Proposed.

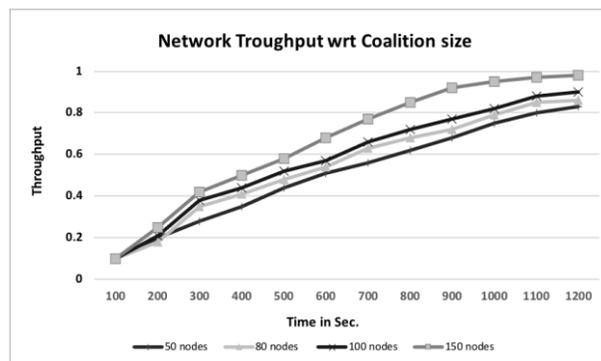


Fig. 4. Throughput for different Coalition Sizes.

The same time applies in Fig. 5 where the relationship is described between the network delay and the coalition size. The test case shows that the network delay decreases as the coalition size increases. Initially, the network delay of 50 coalition size equals to 80%, while it is 27% for 150 coalition size. At time= 10, the network delay equals to 15% for the 50 coalition size and 1% for 150 coalition size.

2) *Dead nodes and  $\alpha$  weight parameter*: Fig. 6 describes the relationship between the weight of the average transmission rate ( $\alpha$ ) and the dead nodes. The test cases of different coalition sizes show that as the weight parameter  $\alpha$  increases the number of dead nodes increases. This is because as the average transmission rate increases, the power consumption of mobile nodes increases and that would increase the chance of dead nodes. Also, the test cases show that the chances of having dead nodes decreases as the coalition size increases.

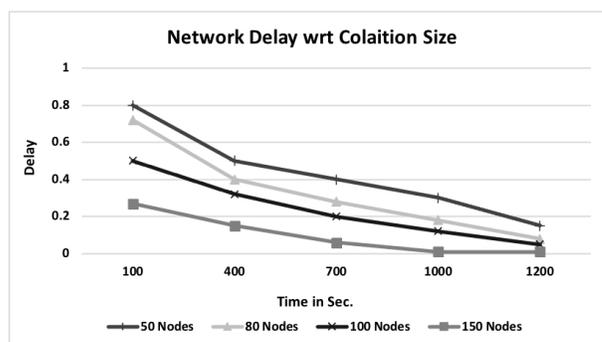


Fig. 5. Delay for different Coalition Sizes over time.

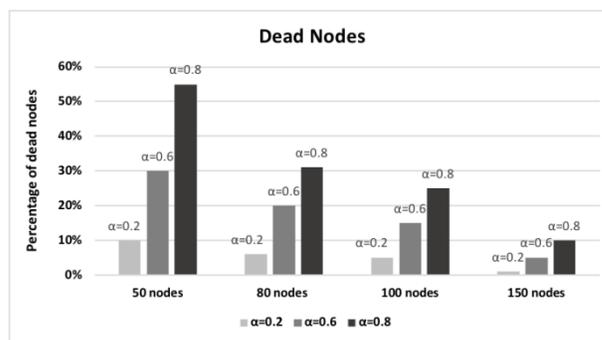


Fig. 6. Number of Dead Nodes with different Weights of  $\alpha$ .

3) Network overhead and  $\beta$  weight parameter: Fig. 7(a), 7(b) and 7(c) describe the relationship between the network overhead and the weight of number of times a node used its neighbor for data transmission. The network overhead is a reflection of network delay. The  $\beta$  weight parameter monitors the nodes remaining power battery. The test case in Fig. 7(a) shows the overhead of four coalition sizes when  $\beta=0.8$ . Initially all coalition size have the same overheads. At time=60 sec the overhead of less coalition size becomes greater, 38% for 50 coalition size and 20% for 150 coalition size. While at time=160 sec, it is 53% for 50 coalition size and 29% for 150 coalition size. The same thing applies to Fig. 7(b) and 7(c) where  $\beta=0.6$  and  $\beta=0.2$ , respectively. Notice that as  $\beta$  increases for the same coalition size, the overhead increases. As an example, for 50 coalition size, the overhead equals 13% when  $\beta=0.2$  and it is 45%  $\beta=0.6$  and it is 53% when  $\beta=0.8$ .

### C. Scheme Evaluation

In this section, we compare the proposed scheme with respect to the other schemes within the same category as described in Section 2. The comparison described in Table II

covers five criteria: power model, discovery method, merits, route metrics and performance metrics. Some of them are defined in [11]. The power model can be constant when the link cost is fixed regardless of the source-destination distance or variable when the link cost depends on the source-destination distance. The routing scheme uses single-hop discovery method when its procedure rely on the neighboring nodes or multi-hop when the procedure relies on the overall path from the source to destination.

Table II summarizes a comparison between the related schemes and the proposed one. Some of the features are similar in all routing schemes. However, our proposed scheme differs in the discovery method since it uses cascaded single-hop. The cascaded single-hop supports the optimal selection of routing path at every source-destination hop with minimum transmission overhead. Also, the algorithm of the proposed scheme is simple since the selection of the routing path depends on two metrics, the average transmission rate for the neighboring nodes and number of times the neighboring node is used for data transmission during the network life cycle.

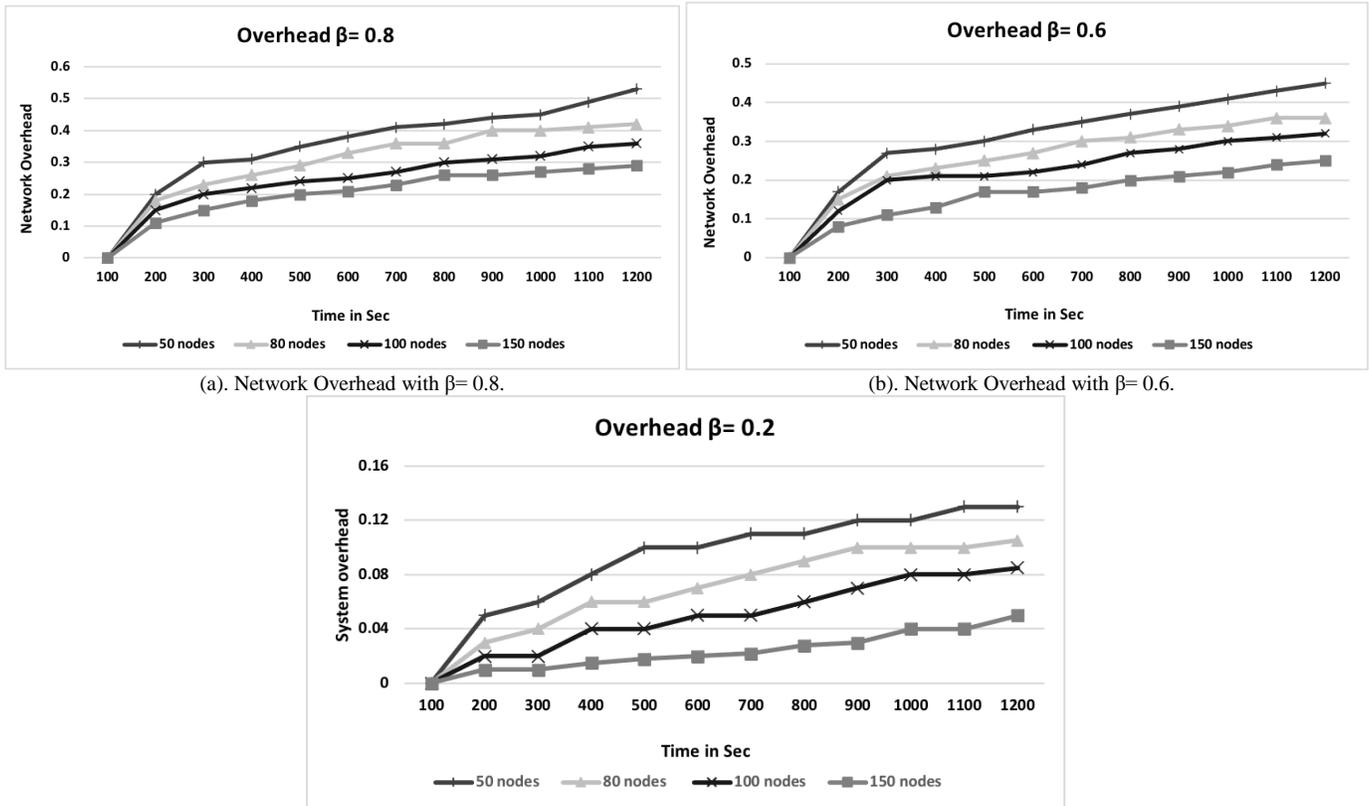


Fig. 7. (c). Network Overhead with  $\beta=0.2$ .

TABLE II. COMPARISON BETWEEN THE PROPOSED SCHEME AND RELATED SCHEMES

Routing scheme	Power Model	Discovery Method	Merits	Route Metrics	Performance Metrics
Proposed approach	Variable	Cascaded single-hop	Simple algorithm, Direct trade-off between the power consumption and number of transmissions	Number of transmissions of a node and number of times the neighboring node	Network life time, normalized residual energy and minimum transmission over Head
FAR [15]	Constant	Multi-hop	Maximize the network life time	Link and node costs	Network life time and normalized residual energy
OMM [16]	Variable	Multi-hop	Maximizes the network life time	Max–Min Residual power	Maximum of transmitted messages and ratio the optimal solution,
MER [17]	Variable	Multi-hop	Direct tradeoff between routing overhead and lower energy consumption	Minimum hop route	Normalized energy
DEAR [18]	Variable	Multi-hop	Based on energy-aware devices	Device-aware	Network lifetime
PAR [19]	Variable	Multi-hop	Selection of the less congested path and energy efficient.	Link status ratio	Network energy consumption, number of failed Nodes and average of residual energy
MST-BDD [20]	Variable	Multi-hop	Simple algorithm, Decreases the network power transmission	Minimum SPT	Time complexity
AODV_RR [21]	Variable	Multi-hop	Lower overall Energy Consumption and communication overhead	Received signal strength	Multiple of QoS such as throughput, delay, amount of overhead
ELRPP [22]	Variable	Multi-hop	Improves QoS	Link availability and existing energy	Multiple of QoS such as throughput, delay, total energy consumption, drop ratio and execution time

## VI. CONCLUSION AND FUTURE

In this paper, we propose a new scheme based on transmission power control-based approach to provide a balance between the transmission rates and power consumption of mobile nodes. The scheme uses a cascaded single-hop to discover the utilization and the average transmission rate of the neighboring node. The scheme algorithm selects the routing path by creating routing tables for each neighboring node. The table contains the average transmission rate for the neighboring nodes and number of times the neighboring node is used for data transmission. The proposed approach affects the overall network lifetime by increasing the battery power of the nodes and decreasing the power consumption in the network. Through simulating several test cases, we discussed how nodes can select a proper node for transmitting data using a unique mechanism that keeps track of the transmission rates and energy consumption of individual nodes in the network. The simulation showed how varying characteristics function weight parameters can affect the network sensitive parameters.

As a future, we are planning to study the model to that it can be scaled up to include thousands of nodes and consider the features of the proposed scheme to operate in a bigger coalition size; also, to study the response of the algorithm under different types of attacks.

## REFERENCES

- [1] S. Plass, F. Clazzer, B. Fritz, I. Yasrine, M. Maurizio, "Maritime communications – Identifying current and future satellite requirements & technologies", 20th Ka and Broadband Communications, Navigation and Earth Observation Conference, Italy, 2014.
- [2] G. Bonanno, "Game Theory: An open access textbook with 165 solved exercises", Open Access, 2015.
- [3] N. Karayiannis, S. Nadella, "Power-conserving routing of ad hoc mobile wireless networks based on entropy constrained algorithms", Ad Hoc Networks, Vol. 4, No. 1, pp. 24–35, 2006.
- [4] J. Zhu, B. Bensaou, F. Nait-Abdesselam, "Power control protocols for wireless ad hoc networks", In Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, John Wiley & Sons Inc., pp.315–352, 2008.
- [5] S. Giordano, I. Stojmenovic, L. Blazevic, "Position based routing algorithms for ad hoc networks: A taxonomy", Ad Hoc Wireless Networking, Vol. 14, pp. 103-136, 2004.
- [6] A. Al Sharah, M. Alhaj, "Using Hand-shake Transmission Rate Adaptation Scheme in MANET", IJCSNS International Journal of Computer Science and Network Security, Vol. 20, No. 2, 2020.
- [7] B. Devika, P. N. Sudha, "Power optimization in MANET using topology management", Engineering Science and Technology, an International Journal 23(3) pp 565-575, 2020.
- [8] J. Naser, A. Kadhim, "Multicast routing strategy for SDN-cluster based MANET", International Journal of Electrical & Computer Engineering (2088-8708), 10, 2020.
- [9] S. Kumar, D. Sinha, V. Kumar, "An Approach to Improve Lifetime of MANET via Power Aware Routing Protocol and Genetic Algorithm", 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 550-553, IEEE, 2020.

- [10] D. Sinwar, N. Sharma S. Maakar, S. Kumar, "Analysis and comparison of ant colony optimization algorithm with DSDV, AODV, and AOMDV based on shortest path in MANET", *Journal of Information and Optimization Sciences*, 41(2), pp. 621-632, 2020.
- [11] W. Jabbar, M. Ismail, R. Nordin, S. Arif, "Power- efficient routing schemes for MANETs: a survey and open issues", *Wireless Network Vol. 23*, pp. 1917-1952, 2017.
- [12] Y. Ko, N. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks", *Wireless Networks*, Vol. 6, No 4, pp. 307-321, 2000.
- [13] A. Al Sharah, M. Alhaj, M. Hassan, "Selfish Dynamic Punishment Scheme: Misbehavior Detection in MANETs Using Cooperative Repeated Game", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 20, No. 3, 2020.
- [14] The Network Simulator - NS-2, [Online] <https://www.isi.edu/nsnam/ns/> (Accessed 15/1/2021).
- [15] J. Chang, L. Tassiulas, "Energy conserving routing in wireless ad-hoc networks", In *Proceedings-IEEE INFOCOM*, Vol. 1, pp. 22-31, 2000.
- [16] Q. Li, J. Aslam, D. Rus, "Online power-aware routing in wireless ad-hoc networks", In *Proceedings of the 7th annual international conference on Mobile computing and networking*, pp. 97-107, 2001.
- [17] S. Doshi, T. Brown, "Minimum energy routing schemes for a wireless ad hoc networks", In *Proceedings of the Conference on Computer Communications*, Vol. 2, 2002.
- [18] A. Avudainayagam, W. Lou, Y. Fang, "DEAR: A device and energy aware routing protocol for heterogeneous ad hoc networks", *Journal of Parallel and Distributed Computing*, Vol. 63, No. 2, pp. 228-236, 2003.
- [19] V. Rishiwal, M. Yadav, S. Bajapai, S. Verma, "Power aware routing in ad hoc wireless networks", *Journal of Computer Science and Technology*, Vol. 9, No. 2, pp. 101-109, 2009.
- [20] C. Yanez-Marquez, I. Lopez-Yanez, O. Camacho-Nieto, A. Arguelles-Cruz, "BDD-based algorithm for the minimum spanning tree in wireless ad-hoc network routing", *IEEE on Latin America Transactions*, Vol. 11, No. 1, pp. 600-601, 2013.
- [21] V. Lalitha, R. Rajesh, "AODV\_RR: A maximum transmission range based ad hoc on-demand distance vector routing in MANET", *Wireless Personal Communications*, Vol. 78, No. 1, pp. 491-506. doi:10.1007/s11277-014-1763-6, 2014.
- [22] J. Katiravan, D. Sylvia, D. Rao, "Energy efficient link aware routing with power control in wireless ad hoc networks", *The Scientific World Journal*, 2015.
- [23] S. Kannan, A. Rajaram, "QoS Aware Power Efficient Multicast Routing Protocol (QoS-PEMRP) with Varying Mobility Speed for Mobile Ad Hoc Networks", *International Journal of Computer Applications*, Vol. 60, No. 18, 2012.
- [24] C. Papageorgiou, P. Kokkinos, M. Varvarigos, "Energy-efficient multicasting in wireless networks with fixed node transmission power", *Proceedings of the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, Germany, 2009.
- [25] A. Khan, Q. Sun, Z. Mahmood, A. Ghafoor, "Energy Efficient Partial Permutation Encryption on Network Coded MANETs", *Journal of Electrical and Computer Engineering*, Vol. 2017, 2017.
- [26] M. Rahman, "An teeiciffE Position based Power Aware Routing Algorithm in Mobile Ad-hoc Networks", *I. J. Computer Network and Information Security*, 2016.
- [27] S. Ghode, K. Bhoyar, "NEMA: Node Energy Monitoring Algorithm for Zone Head Selection in mobile ad-hoc network using residual battery power of node", *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, India, 2016.
- [28] M. Hassan, R. Muniyandi, "An Improved Hybrid Technique for Energy and Delay Routing in Mobile Ad-Hoc Networks", *International Journal of Applied Engineering Research*, Vol. 12, No. 1, pp. 134-139, 2017.
- [29] T. Lu, J. Zhu, "Genetic algorithm for energy-efficient QoS multicast routing", *IEEE Communications Letters*, Vol. 17, No. 1, pp. 31-34, 2013.
- [30] P. Kamboj, A. Sharma, "Power aware multicast reactive routing protocol (PAMRRP)", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 8, No. 8, 2008.
- [31] S. Zhao, L. Tan, J. Li, "A distributed energy efficient multicast routing algorithm for WANETs", *International Journal of Sensor Networks*, 2007.
- [32] N. Papanna, A. Reddy, M. Seetha, "EELAM: Energy efficient lifetime aware multicast route selection for mobile ad hoc networks", *Applied Computing and Informatics*, Vol. 15, No. 2, pp. 120-128, 2019.
- [33] F. Sarkohaki, R. Fotohi, and V. Ashrafian, "An Efficient Routing Protocol in Mobile Ad-hoc Networks by using Artificial Immune System", *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 8, No. 4, pp. 554-561, 2020.
- [34] N. Ray, A. Turuk, "A Hybrid Energy Efficient Protocol for Mobile Ad Hoc Networks", *Journal of Computer Networks and Communications*, Vol. 2016, Article ID 2861904, 2016.
- [35] S. Alani, Z. Zakaria, H. Lago, "A new energy consumption technique for mobile Ad-Hoc networks" *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 9, No. 5, pp. 4147-4153, 2019.
- [36] B. Bhatia, M. Soni, P. Tomar, "Extended Bandwidth Optimized and Energy Efficient Dynamic Source Routing Protocol in Mobile Ad-hoc Networks", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 3, pp. 1460-1466, 2018.

# Real-Time Intelligent Thermal Comfort Prediction Model

Farid Ali Mousa<sup>1</sup>

Information Technology Department  
Faculty of Computers and Artificial Intelligence  
Beni-Suef University, Beni Suef, Egypt

Heba Hamdy Ali<sup>2</sup>

Multimedia Department  
Faculty of Computers and Artificial Intelligence  
Beni-Suef University, Beni Suef, Egypt

**Abstract**—Real-time prediction model of indoor thermal comfort depending on Momentum Back Propagation (MBP) function is established by using Arduino hardware and mobile application. The air temperature indoor, air velocity, and relative humidity are gathered via temperature sensor and transferred via Bluetooth to the mobile application to predicate thermal comfort. A significant challenge in designing MBP is to decide the best architecture and parameters as the number of layers and nodes, and number of epochs for the network given the data for the AI issues. These parameters are usually selected on heuristic and fine-tuned manually, which could be as boring as the performance assessment may take hours to test the output of a single MBP parameterization. This paper tends to the issue of determining appropriate parameters for the MBP by applying chicken swarm optimization (CSO) algorithm. The CSO algorithm simulates the chicken swarm searching for the best parameter employs the Fitness function of these parameters which yielding minimum error and high accuracy. The proposed accuracy approximately equals 98.3% when using the best parameters obtained from Chicken Swarm Optimization (CSO). The proposed methodology performance is assessed on the collected dataset from weather archive and in the context of thermal comfort prediction, that mapping relations between the indoor features and thermal index.

**Keywords**—Thermal comfort; chicken swarm optimization; momentum back propagation; neural network; bio-inspired optimization algorithm

## I. INTRODUCTION

In the production of building architecture, thermal comfort proves to be one of the most critical factors. People always wanted to create a thermal climate. Thermal comfort means a "condition of mind" in compliance with ISO 7730(1993) and ASHARE Standard 55(2010) [1, 2], which reflects pleasure with the thermal environment in which the thermal environment is situated'. Thus, in work, people must be pleased with the thermal atmosphere surrounding them or they will suffer from and won't work like they used to be. The principal necessity is preserving thermal comfort and it need to be achieved with the appropriate thermal equilibrium of the human nature. The basic thermal comfort factors can influence the safety or the health of the employees [3], e.g., the possibility of a rise in heat, decline or much worse could be if temperatures are too high. Also, the possibility of employee headaches, loss of focus or nausea, may also occur when the temperature drops too much. Being sleepy or not feel at all well when they function, all these could be happened due to

the temperature in their offices or spaces. There are four fundamental thermal comfort factors [4]; first, moisture that ensures a significant amount of water is present in the air which keeps the sweat evaporation from the skin. Second, the ambient air temperature surrounding the body. Third, the air speed or the rapid flow of air in the employee's atmosphere that is the primary thermal comfort component. Thus, the air in a warmed indoor atmosphere will relax workers. There is a certain range of thermal comfort for each of the fundamental factors.

## II. RELATED WORK

Thermal comfort is largely attributed to environmental and human influences. The fundamental adaptive thermal comfort theory stated that, people living in one place already seemed to be adapted to the thermal local environment [5] and their thermal history could contribute to different conditions of thermal comfort [6][7]. Thermal conditions in thermal systems can be more effectively modeled locally and internationally, helps to design and improve building thermal systems [8][9]. Thermal conditions in humans are best viewed in terms of their thermal comfort needs.

Two distinct models, named the adaptive model and the PMV/PPD model [10], can be calibrated according to literature for the thermal comfortability measurement. The predict mean vote (PMV) should be the conventional dominant thermal comfort model [11], based on the thermal equilibrium between the human body and the environment. The model based on the heat balance concepts and the data was obtained from the chamber experiment where detailed monitoring of indoor conditions could be accomplished. In terms of the four environmental and the two personal factors mentioned before, the PMV model presents a statistical model to forecast the thermal sensation of a wide group of subjects.

These six major thermal comfort factors are grouped into environmental factors are; air temperature, mean radiant temperature, relative humidity and air speed and personal factors are; metabolic rate and clothing insulation, that directly affect the thermal comfort [12]. The PMV/PPD model is appropriate with air conditioning buildings and ventilation systems, while the adaptive model is most suited with naturally conditioned buildings without mechanical condition systems [13].

ASHRAE uses the PMV index to estimate the average reaction of a broad seven-points thermal scale of a large

number of people from cold (3) to hot (3) [14] this is known as the 'ASHRAE scale'. Zero stands for the desired value of thermal neutrality. A consumer will define a value similar to 0 for the PMV in a setting he/she finds convenient. The expected unmet percentage (PPD) is an indicator used to measure the proportion of people unfulfilled with a certain thermal condition feeling that is whether too cold or too hot as recommended from their PMV values [15].

The PPD index is thus closely connected to PMV. This dependency is seen in the Fanger equation [12].

The ThermCont model, that learns a regressor which takes the six vector parameters of PMV as an input and provides a corresponding PMV value as an output, is designed to avoid and monitor the thermal comfort of the occupant by using machine learning tools. ThermCont utilizes Multiple Linear Regression [16] (MLR) algorithm, which is focused on subjective thermal comfort findings performed in a building of an office [17]. In addition, a genetic algorithm [18] has been developed to detect thermal comfort (PMV) in real time to enhance thermal comfort for indoor people.

Data-driven approach [19] is developed to forecast thermal comfort of individual in real-time using a range of human factors and environmental factors including the six Fanger elements and the three new factors which are; gender, age and outdoor weather. The outdoor weather and three new features were added. Eventually, data of the outdoor weather was used by effective temperature because effective temperature is reflective of the weather, unlike air temperature.

The ANN is practically utilized to estimate non-linear relationships between input features and output [20]. The artificial neural networks are applied to predict PMV index values of thermal comfort in a room. In order to select the right conditions, the ANN modeling can be performed many times. But the globally optimal solution in this case is not guaranteed. We propose in this paper a better way to address this issue by using CSO to ensure an optimum modeling parameter for a neural network is the Global Minimum Square Error (MSE). The use of the CSO means that the minimum number of time slots generated also matches the real-time limit.

This paper is organized as follows: in Section 3, the overall architecture of the proposed real-time intelligent thermal comfort prediction model is introduced. In Section 4, the proposed methodology that solves the predication problem is explained. Section 5 introduces and discusses the experimental and finally the conclusion in Section 6.

### III. REAL-TIME INTELLIGENT THERMAL COMFORT PREDICTION MODEL

Fig. 1 shows the indoor air speed, air temperature and relative humidity are gathered by hardware interface. The Hardware interfaces includes the components; LM35 temperature sensor, Arduinio-uno and Bluetooth HC-05. The data are collected using the temperature sensor (LM5) which transferred using Arduinio-uno hardware. Then the data are transmitted via hardware to connected Bluetooth. The Bluetooth send the collected data to the mobile application for thermal comfort prediction. To receive the last temperature,

form the indoor atmosphere, the user just presses a button in the application. Since the data was received in Fahrenheit, it has to be converted into Celsius. The gathered data are sent via cellular network or WiFi to trained model to predict thermal comfort which is then sent back to the mobile application according to Table I.

#### A. Data Collection from Arduino

The current air speed, relative humidity and air temperature are collected from the Arduino-Uno while the rest of the input features are entered from the dataset [25] used in the experiment.

#### B. Hardware Interface

There are three components of the hardware interface: (1) LM35 temperature sensor are included in the Hardware Interface: LM35 is developed for indoor climate measurement; if the sensor and the Arduino is connected as in Fig. 2(a). The Arduino will begin receiving data from this sensor immediately; the Arduino-Uno board as shown in Fig. 2(b) by Arduino [21]. (2) The Arduino-Uno is a microcontroller board. The digital and analog input/output pins are given. This is coded in C language for every second from the temperature attached to the Arduino-Uno, for sending and receiving the temperature. The result shows that the present temperature affects the consumer at home. (3) HC-05 Bluetooth: In order to start receiving android data through Bluetooth for this part as shown in Fig. 2(c). HC-05 only connects to android operating systems.

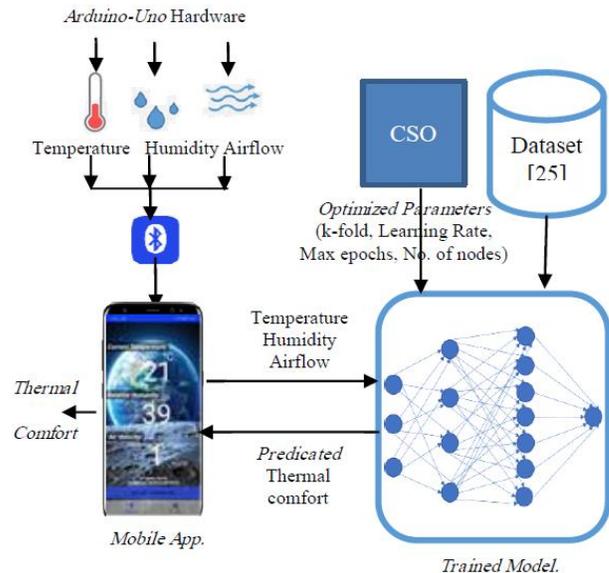


Fig. 1. Real-time Thermal Comfort Prediction Model.

TABLE I. INDEX LEVEL SCALES WITH THERMAL COMFORT

Index Level	Thermal Comfort
-2	Cold
-1	Cool
0	Comfort
1	Slightly hot
2	Hot

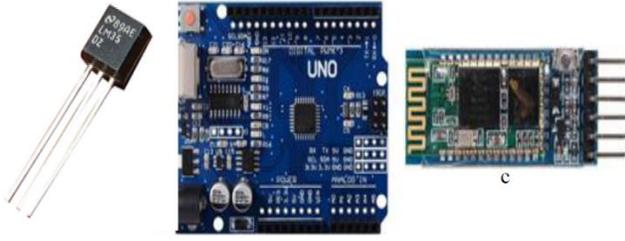


Fig. 2. Hardware Interface (a) LM35 Temperature Sensor, (b) Arduino-Uno and (c) Bluetooth HC-05.

### C. Mobile Application

The smartphone framework is designed to obtain real-time temperatures from the hardware. Measured data will be transmitted privately via Bluetooth to the inhabitants' smartphones. Officers can still send input and aggregate information through a mobile network or WiFi to our backend server. Fig. 3(a) displays a range of standard mobile app user interfaces (UIs). The current temperature, air velocity, relative humidity and current thermal comfort/discomfort are provided to the operators.

The thermal navigation button bar leads the user to another big operation, where it consists of two predictions "Predicted temperature" and "Predicted thermal comfort/discomfort" as seen in Fig. 3(b). The user will be given an opportunity to alert the application to submit a default sound on the lock-screen for the expected temperature and thermal comfort/discomfort.



Fig. 3. (a) Home Page, (b) Thermal Page Interface.

## IV. PROPOSED METHODOLOGY

In this section, the approach proposed is clarified to efficiently solve problem of prediction of indoor thermal comfort using artificial neural network (ANN) with momentum function. The novel swarm algorithm (CSO) is utilized that automatically generate the most effective architecture model of NN to maximize classification performance and minimize the mean square error (MSE).

### A. Chicken Swarm Optimization (CSO)

Chicken Swarm Optimization focused on computational optimization algorithms with bio-inspired behavior as discussed in [22]. There are a variety of communities in the chicken swarm. A dominant rooster, multiple hens and chicks are included each. The classification of these classes depends on the fitness values of the pigs. The best of the chickens would be roosters, each of whom would be the head rooster in a party. The most fitness-intensive chickens will be called chicks. The remainder is the hens. The hens chose the community in which they reside. The relationship of mother and child between hens and chicks is often formed randomly. In a collective there will be no shift in leadership, superiority and mother-and-child relationships. The hen selects classes arbitrarily in which to live and can only be changed for many generations. Chickens are hunting their group mate's rooster for food while avoiding consuming their own food, each group coordinates as a team and explore food according to a certain hierarchical order [23]. The chicken of the best fitness values of the next generation are picked of flocks.

$$X_{i,j}^{t+1} = X_{i,j}^t * (1 + \text{Randn}(0, \sigma^2)) \quad (1)$$

$$\sigma^2 = \begin{cases} 1, & \text{if } f_i \leq f_k \\ \exp\left(\frac{f_k - f_i}{|f_i| + \epsilon}\right), & \text{otherwise} \end{cases} \quad k \in [1, N], k \neq i \quad (2)$$

$$X_{i,j}^{t+1} = X_{i,j}^t + S1 * \text{Rand} * (X_{r1,j}^t - X_{i,j}^t) + S2 * \text{Rand} * (X_{r2,j}^t - X_{i,j}^t) \quad (3)$$

$$S1 = \exp((f_i - f_{r1}) / \text{abs}(f_i) + \epsilon) \quad (4)$$

$$S2 = \exp((f_{r2} - f_i)) \quad (5)$$

$$X_{i,j}^{t+1} = X_{i,j}^t + FL * (X_{m,j}^t - X_{i,j}^t) \quad (6)$$

At time  $t$ , The  $N$  number of chickens, are referred as  $X_{i,j}^{t+1}$ , where  $i \in [1, 2, \dots, N]$ ,  $j \in [1, 2, \dots, D]$  in  $D$ -dimensional space. The optimization problem is actually the problem of finding the minimum value of nonlinear equations. Therefore, the best  $Par$  corresponds to the minimum fitness value.  $Fit$ , is the corresponding fitness value. *Algorithm 1* defines the original CSO algorithm [23].

**Original Chicken Swarm Optimization (CSO) Algorithm [21]**

**Step 1:** Initialize a Maximal generations (M), Population size(pop), Dimension(d), How the chicken swarm can often be updated(G). The roosters population size (rPercent), hens accounts (hPercent), mother hens accounts for (mPercent).

**Step 2:** Initialize randomly using Gaussian random generator the size of (rooster rNum, hens hNum, chicks cNum, mother hens mNum).

**Step 3:** Evaluate the N chickens' fitness values,t=0;

**Step 4:** Check If(t%G==0) then ort the chickens' fitness values and establish a swarm hierarchal order;

Divide different swarm groups, and identify the relationship between chicks' hens in a group

**Step 5:** For i=1:N : Update roosters solutions, hen and chicken solutions (locations)

Check if i==rooster thus, modify its rooster's location using Equation 1

Check if i==hen thus, modify its hen's location using Equation 3

Check if i==chick thus, update its chick's location using Equation 6

New solution evaluation;

Check if the new solution is better than the previous solution, then update it;

Check if (t<M) go to step 4 else output results

**B. Learning Model: Momentum Back Propagation (MBP) Algorithm**

The dynamic back propagation (BP) approach was also used to adapt artificial neural networks to different problem typing patterns. One significant drawback of this system, however, is that it is highly dependent on these choices of momentum and size values [24]. Supervised learning will be needed for this study. In the classification, the momentum algorithm was used to find common properties from different classes. Also, it helps in enhancing the training speed and accuracy of finding values for weights so that given input and the computed output values are closely correctly match the known. Momentum also, consists of 3 phases. The first phase is the forward phase in which we begin the net and s(net) computation. The backward phase is the second phase that measures the error. The final and third phase is the weight update in which weights are updated from the output to the hidden layer and then to the input layers, if the error square is greater than the mean square error to get the final weights.

$$s(net) = \frac{1}{1} + e^{-net} \quad (7)$$

The backward phase calculates errors at all nodes using equations 1, 2.

For output error:

$$y_1(1 - y_1) * (d - y_1) \quad (8)$$

For hidden error:

$$z_1 * (1 - z_1) * \sum_{k=1}^m s_1 k w_1 k \quad (9)$$

The last step, if the Error square is greater than the MSE, thus it is going to apply weights update to get the final weights resulted using Equation 4.

$$W_{new} = \mu * S * Z + [\alpha * W_{old}] \quad (10)$$

After doing all of this, the final weights are used\_for thermal comfort prediction in android application.

**V. EXPERIMENTS AND RESULTS**

**A. Dataset**

From July 2005 to July 2019 data are collected for one year, from weather archive in Cairo, Egypt [25]. Totally, there are 30,354 records in the dataset, and ten input features which are; time, air velocity, air temperature, global temperature, weight, height, sex, solar radiation, temperature gradient, relative humidity, and the eleven attribute is the index value that corresponds to the comfort value associated with the input features.

**B. Experiments Evaluation and Results**

The experiment results are shown based on the iterative nature of chicken swarm optimization algorithm. Table II shows some examples of predicted results of CSO.

Table II and Fig. 4 illustrate that optimal solution has been found by chicken swarm optimization algorithm where the objective value is to minimize the error. The performance comparison between the fine-tuned neural network experiments and optimization of neural network is using the chicken swarm optimization experiment (CSO-NN). We will note that CSO algorithm produces a little time. Therefore, a low overall complexity is for modelling and forecasting. The runtime can be reduced by 1.281. It then enhances the credibility of the forecast and minimizes all MSE. The MBP architecture in Fig. 5 achieved a classification performance of 98, 25% by training the classifier using 7-folds.

Table III shows the overall confusion matrix that evaluated the performance of the developed model using the best architecture of MBA. The confusion matrix represents the five thermal comfort classes {Cold, Cool, Comfort, Slightly hot, Hot}. The results proved that the model developed is able to predict thermal comfort.

TABLE II. EXPERIMENTS RESULTS

k-fold	Learning Rate	Max epochs	No. of nodes	Accuracy (%)
27	0.2	2	(10,8,9,5)	69.246
17	0.4	44	(10,8,10,5)	88.231
21	0.4	62	(10,4,9,5)	89.300
9	0.6	66	(10,8,1,5)	93.710
9	0.2	22	(10,2,4,5)	92.130
7	0.5	46	(10,7,7,5)	98.252

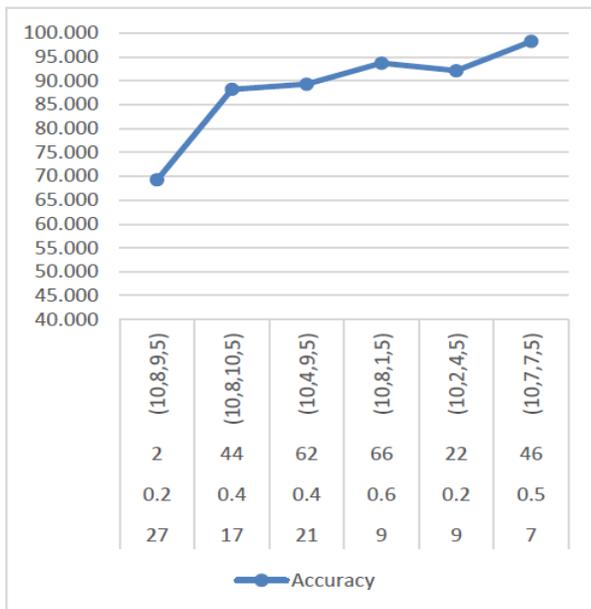


Fig. 4. Experiments Results of MBP.

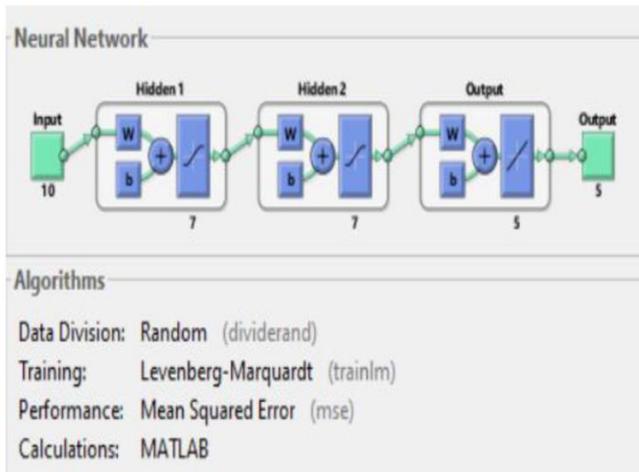


Fig. 5. Best Architecture of MBP using CSO.

TABLE III. CONFUSION MATRIX OF THERMAL CLASSES

Class Label	Class 1	Class 2	Class 3	Class 4	Class 5
Class 1 (Cold)	347	4	1	0	0
Class 2 (Cool)	55	7536	57	4	0
Class 3 (Comfort)	35	40	8120	69	0
Class 4 (Slightly hot)	0	26	80	10820	82
Class 5 (Hot)	0	0	18	60	3000

### C. Evaluation Metrics

As shown in Table IV, we calculate the evaluation metrics to the best structure of the trained neural network from CSO optimization that consists of 10 input features and 7 nodes in the first hidden layer, 7 nodes in the second hidden layer and 5 nodes in the output layer; with 46 epochs and 0.5 learning rate; we can see that the proposed method gave us a better result in all metrics.

TABLE IV. EVALUATION METRICS

Metrics	Results 10,7,7,5	Formula	Evaluation Focus
Accuracy (acc)	0.9825	$\frac{tp+tn}{tp+fp+tn+fn}$ (11)	Typically calculates the percentage of accurate forecasts over the total number of measured instances
Error Rate (err)	0.0175	$\frac{fp+fn}{tp+fp+tn+fn}$ (12)	The error of misclassification tests the ratio of false predictions to the actual number of cases assessed
Sensitivity (sn)	0.9595	$\frac{tp}{tp+fn}$ (13)	Calculate accurately classified fractions of positive patterns
Specificity (sp)	0.9914	$\frac{tn}{tn+fp}$ (14)	Calculate the proportion of the negatively patterns classified correctly
Precision (p)	0.9774	$\frac{tp}{tp+fp}$ (15)	Determine the positive patterns that are adequately predicted in a positive class by the total predicted patterns
F-Measure (FM)	0.9683	$\frac{2 \times p \times r}{p+r}$ (16)	Describes the harmony among recall and precision values
Negative Predictive Value	0.9844	$\frac{tn}{tn+fn}$ (17)	The percentage of negative test outcomes reported correctly
False Positive Rate	0.0086	$\frac{fp}{fp+tn}$ (18)	The risk that the null hypothesis for the given test will be denied falsely.
False Discovery Rate	0.0226	$\frac{fp}{fp+tp}$ (19)	The significant features rate is truly null
False Negative Rate	0.0405	$\frac{fn}{fn+tp}$ (20)	Used to conceptualize Type I error rates when evaluating null hypotheses with many comparisons. Intended to monitor the estimated percentage of false discoveries.

## VI. CONCLUSIONS

Thermal comfort impacts working efficiency at work sites, and it is very important for consumers to be conscious of the performance of such thermal environments. This paper demonstrates the practicability of the intelligent thermal comfort application for individual's thermal comfort prediction in the android application by automatic collect the relative humidity, air temperature and air velocity. The predication model proposed is based on momentum algorithm which achieved an accuracy result of 98.25% for thermal comfort, taking the final weights of the classification model, which is optimized using bio-inspired optimization algorithm (CSO). Furthermore, the analysis of the results showed that our proposed optimization model provides the optimal solution that achieved the minimum MSE of 1.7477.

### REFERENCES

- [1] Y. Song, F. Mao and Q. Liu, "Human Comfort in Indoor Environment: A Review on Assessment Criteria, Data Collection and Data Analysis Methods," in IEEE Access, vol. 7, pp. 119774-119786, 2019, doi: 10.1109/ACCESS.2019.2937320.

- [2] P. K. Rosier, "Comfort theory and practice: A vision for holistic health care and research", *Clin. Nurse Spec.*, vol. 19, pp. 49, Jan. 2005.
- [3] K. C. Parsons, *Human thermal environments: the effects of hot, moderate, and cold environments on human health, comfort, and performance*. Boca Raton: CRC Press, 2014.
- [4] N. Ma, D. Aviv, H. Guo, and W. W. Braham, "Measuring the right factors: A review of variables and models for thermal comfort and indoor air quality," *Renewable and Sustainable Energy Reviews*, vol. 135, p. 110436, 2021.
- [5] Yao R, Li B, Liu J (2009). R. Yao, B. Li, and J. Liu, "A theoretical adaptive model of thermal comfort – Adaptive Predicted Mean Vote (aPMV)," *Building and Environment*, vol. 44, no. 10, pp. 2089–2096, 2009.
- [6] D. Kong, H. Liu, Y. Wu, B. Li, S. Wei, and M. Yuan, "Effects of indoor humidity on building occupants' thermal comfort and evidence in terms of climate adaptation," *Building and Environment*, vol. 155, pp. 298–307, 2019.
- [7] H. Yan, Q. Liu, H. Zhang, H. Wang, H. Li, and L. Yang, "Difference in the thermal response of the occupants living in northern and southern China," *Energy and Buildings*, vol. 204, p. 109475, 2019.
- [8] B. Li and R. Yao, "Building energy efficiency for sustainable development in China: challenges and opportunities," *Building Research & Information*, vol. 40, no. 4, pp. 417–431, 2012.
- [9] X. Yuan, Y. Pan, J. Yang, W. Wang, and Z. Huang, "Study on the application of reinforcement learning in the operation optimization of HVAC system," *Building Simulation*, vol. 14, no. 1, pp. 75–87, 2020.
- [10] M. Rocca, "Health and well-being in indoor work environments: a review of literature," 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), 2017.
- [11] P. O. Fanger et al., "Thermal comfort. Analysis and applications in environmental engineering." *Thermal comfort. Analysis and applications environmental engineering*. 1970.
- [12] P. Bluysen, *The indoor environment handbook: how to make buildings healthy and comfortable*. London: Earthscan, 2015.
- [13] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 2007.
- [14] *Thermal environmental conditions for human occupancy*. Atlanta, GA: ASHRAE, 2017. K. Chen, Y. Jiao, and E. S. Lee, "Fuzzy adaptive networks in thermal comfort," *Appl. Math. Lett.*, vol. 19, no. 5, pp. 420426, 2006.
- [15] D. Markov, "Practical evaluation of the thermal comfort parameters", *Proc. Annu. Int. Course Ventilation Indoor Climate*, pp. 158-170, Oct. 2002.
- [16] T. Chaudhuri, D. Zhai, Y. C. Soh, H. Li, and L. Xie, "Random forest based thermal comfort prediction from gender-specific physiological parameters using wearable sensing technology," *Energy and Buildings*, vol. 166, pp. 391–406, 2018.
- [17] N. Seydoux, K. Drira, N. Hernandez and T. Monteil, "Autonomy through knowledge: How IoT supports the management of a connected apartment", *Proc. Semantic Web Technol. Internet Things (SWIT) Workshop ISWC CEUR WS*, 2016.
- [18] W. Zhang, W. Hu, and Y. Wen, "Thermal Comfort Modeling for Smart Buildings: A Fine-Grained Deep Learning Approach," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2540–2549, 2019.
- [19] T. Chaudhuri, Y. C. Soh, H. Li, L. Xie, "Machine learning based prediction of thermal comfort in buildings of equatorial Singapore", *IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, pp. 72-77, July 2017.
- [20] S. Aththajariyakul and T. Leephakpreeda, "Neural computing thermal comfort index for HVAC systems," *Energy Conversion and Management*, vol. 46, no. 15-16, pp. 2553–2565, 2005.
- [21] "ArduinoBoardUno," *Arduino*. [Online]. Available: <https://www.arduino.cc/en/pmwiki.php?n=Main%2FarduinoBoardUno>. [Accessed: 14-Feb-2021].
- [22] A. Darwish, "Bio-inspired computing: Algorithms review, deep analysis, and the scope of applications," *Future Computing and Informatics Journal*, vol. 3, no. 2, pp. 231–246, 2018. [mhttp://www.journals.elsevier.com/future-computing-and-informatics-journal/](http://www.journals.elsevier.com/future-computing-and-informatics-journal/).
- [23] Meng X., Liu Y., Gao X., Zhang H, "A New Bio-inspired Algorithm: Chicken Swarm Optimization". In: Tan Y et al., Coello C.A.C. (eds) *Advances in Swarm Intelligence*. ICSI, Part I, LNCS 8794, pp. 86–94, 2014.
- [24] Chien-Cheng Yu and Bin-Da Liu, "A backpropagation algorithm with adaptive learning rate and momentum coefficient," *Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No.02CH37290)*.
- [25] *Weather in 243 countries of the world*, 14-Feb-2021. [Online]. Available: <https://rp5.ru/>. [Accessed: 14-Feb-2021].

# Potential Data Collections Methods for System Dynamics Modelling: A Brief Overview

Aisyah Ibrahim<sup>1\*</sup>, Hamdan Daniyal<sup>2</sup>, Tuty Asmawaty Abdul Kadir<sup>3</sup>, Adzhar Kamaludin<sup>4</sup>

Faculty of Computing, Universiti Malaysia Pahang, Pekan, Pahang, Malaysia<sup>1, 3, 4</sup>

Faculty of Electrical and Electronic Engineering Technology, Universiti Malaysia Pahang, Pekan, Pahang, Malaysia<sup>2</sup>

**Abstract**—System Dynamics (SD) modelling is a highly complex process. Although the SD methodology has been discussed extensively in most breakthroughs and present literature, discussions on data collection methods for SD modelling are not explained in details in most studies. To date, comprehensive descriptions of knowledge extraction for SD modelling is still scarce in the literature either. In an attempt to fill in the gap, three primary groups of data sources proposed by Forrester: (1) mental database, (2) written database and (3) numerical database, were reviewed, including the potential data collections methods for each database by taking into account the advancement of current computer and information technology. The contributions of this paper come in threefolds. First, this paper highlights the potential data sources that deserved to be acknowledged and reflected in the SD domain. Second, this paper provides insights into the appropriate mix and match of data collection methods for SD development. Third, this paper provides a practical synthesis of potential data sources and their suitability according to the SD modelling stage, which can serve as modelling practice guidelines.

**Keywords**—System dynamics modelling; data collection methods; data source; system dynamics methodology

## I. INTRODUCTION

System Dynamics (SD) was developed by a former electrical engineer and researcher from the Massachusetts Institute of Technology in 1956, named Jay W. Forrester. He successfully incorporated the knowledge of a system control theory in electrical engineering into management science through a simulation model [1]–[3].

Generally, in simulation, the word “system” is referring to as “what, from the real world, is being simulated” [4]. The subject of “what” can refer to people, machines or/and resources. A model is a “representation of an event and/or things that are real (a case study) or contrived (a use case)”. A simulation is “a method for implementing a model over time” [4]. With SD, real-world problems or interest systems are modelled through concepts (qualitative) and quantitative methods [5]. The interest system’s available information is collected and organised in SD software to form computer simulation models [6].

Interestingly, pieces of information can come from various sources and types. They are not just in numerical form, but also comprise mental knowledge and other qualitative forms as well [3], [7], [8]. Modellers or SD experts have to depend on their expertise and skills to collect and synthesise this information

and transform it into an SD model through SD methodology [9].

Although the SD methodology has been discussed extensively in most classic literature, methods to incorporate qualitative and quantitative data during the modelling process are not explained in detail by the most influential authors [10]. To date, there are still no fixed guide or comprehensive descriptions on how to incorporate them in SD development [11]. This has raised a few questions.

What method should be used to gather data as a suitable information source? At what stage in the modelling process should these data can be regarded as useful? How are qualitative data and numerical (quantitative) data linked to SD methodology? Therefore, this paper aims to provide an overview of potential data sources and possible data collections methods that can be practically helpful in SD model development.

In an attempt to answer the questions, the initial searching began in online publications databases. Related papers on data sources and data collection methods for SD modelling were compiled for review [12]. Throughout this process, relevant articles were collected from search engines including Google Scholar, System Dynamics Reviews, Science Direct, Taylor & Francis, Sage Publications and Emerald Publishing. Keywords such as ‘knowledge elicitation for System Dynamics’, ‘knowledge elicitation for System Dynamics modelling’, ‘data collection methods for System Dynamics’, ‘data collection methods for System Dynamics Modelling’, ‘data source for System Dynamics’, ‘data collection methods for System Dynamics modelling’, were used. The papers were further analysed to connect any identified keywords with the related questions. Further elaborations were added based on expert suggestions.

The remainder of this paper is divided into three sections. Section II presents a literature digest based on the three primary data sources for SD modelling. Section III explains in details of potential data collections methods based on four SD methodology stages. Lastly, Section IV serves as the concluding remarks.

## II. DATA SOURCE FOR SYSTEM DYNAMICS MODELLING

The forefather of SD, Forrester suggested three important sources. The first is the mental database, the second is written or textual database and the third is the numerical database [13] (see Fig. 1). The first two are crucial in defining the non-linear relationships that control and generate normal behaviour [6].

\*Corresponding Author

Unlike the two databases, numerical does not reveal the cause and effect directions of the variables. It is still crucial in model testing and serving as an input for running the SD model [14].

Although the three types mentioned earlier were already known for SD modelling, the descriptions were still too general. The method to obtain the data needed was not explained in detail. Moreover, with today's technology, new methods may appear to be more beneficial than traditional methods. Several researchers had proposed several suggestions. Unfortunately, the papers were focusing only on one or two specific data sources, not all three. For examples, some researchers suggested that potential data sources be retrieved through social sciences data collection methods and analysis [10][8], but this works well mostly with mental database and written database. Whereas in separate papers, other researchers pointed out their suggestions to borrow methods from Artificial Intelligences, Data Sciences and Big Data domains [15]–[17], which suit well with the numerical database. Therefore, this section provides a revised literature review on the data sources and data collection methods for SD modelling based on the three categories aforementioned. Each is explained in Section A, B and C, respectively.

### A. Mental Database

The first data source is a mental database. The mental database is the knowledge that lies inside the stakeholder's head [2], [13], [18]. This type of expertise involves the internal representations of reality that stakeholders use to understand, believe, reason about, and predict events [2], [6], [19], [20]. It is commonly expressed in oral linguistic communication by the stakeholders [21].

The stakeholders are the leading players or actors in SD modelling projects. Usually, the actors are the problem's owner or clients, analysts, modellers, facilitators and other experts involved in the interest case study. Stakeholders are generally the valuable primary source of information [13]. Their information values reside in the local contextual knowledge, perspectives, preferences and values. It is also noted that stakeholders' reasoning, observation and imagination are not bounded by scientific rationality. From one end, this can be beneficial when dealing with poor-structured and complex problems [22]. At the same time, some may argue about its accuracy in representing reality [20]. Forrester acknowledged that mental database is trickier because it is very rich with knowledge, often missed and hard to elicit [6], [23].

Mental data base Knowledge that resides in stakeholder's head
Written data base Knowledge that resides in written artifacts
Numerical data base Knowledge that resides in numerical form

Fig. 1. Three Types of Data Sources for System Dynamics [13].

In line with Luna-Reyes and Andersen's suggestion, most SD researchers agree that social sciences methods are a suitable approach to be used for extracting mental database [10]. Fig. 2 shows knowledge elicitation from the mental database to written database and numerical database. The data collection methods can be applied whenever it is possible.

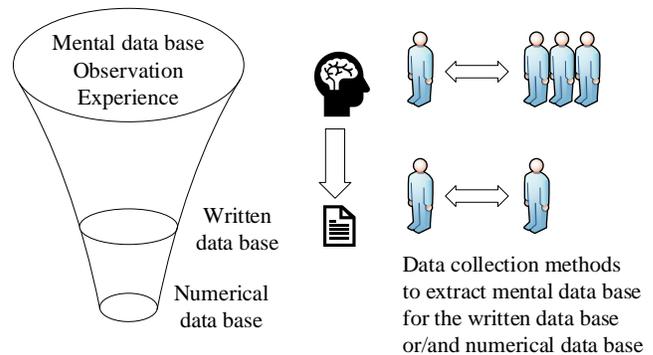


Fig. 2. Extracting and Collecting Mental Database for Written Database and Numerical Database [10].

As further explanation, listed below are ten suggested data collection methods for the mental database.

1) *Interviews*: Interviews allow for two-way communication between interviewer and interviewee(s) [10]. Interviewees are free to communicate their stories, opinions, provide descriptions in their own words. Ethically, any recordings done should be with permission. Interviews can be carried out in four ways.

First, it is face to face communication. Usually, this type of interview is set through appointments, as agreed by both parties. Interview sessions can be recorded using a voice recorder or written down in a notebook. Secondly, interviews can be done via a communication medium such as phone or Voice over Internet Protocol (VoIP) applications like Skype and Internet Phone [24]. The conversations can be recorded with supporting software. Thirdly, digital interview using text applications like Telegram, WhatsApp [25], Facebook or electronic mail (e-mail) [26] can also be conducted. The conversation is carried out in a textual form. With this method, no transcribing effort is needed. Fourthly, interviews through video conferencing such as Zooms, Cisco Webex and Microsoft Teams. These platforms are proven useful, especially when the interviewer and interviewee are geographically apart. The interview sessions can be digitally recorded and safely stored (depending on applications) with permission.

After the interviews were over, all the collected interviews data will be transformed into text. The text was analysed based on patterns, themes, definitions, stories or any key aspects that the researcher is looking for. This method is incredibly useful in discovering and building a dynamic hypothesis and understanding of the overall system process.

2) *Oral history*: Oral history is one of the main research methods to study historical information about past events through planned interviews, either verbal or video recordings

[27]. Oral history helps to obtain specific information or gain perspectives where there is no written evidence no available. This method helps discover and provide a basis for building dynamic hypotheses and how the system works, and changes happened [10].

3) *Focus group*: Focus groups are group interview session with eight to twelve individuals. This method also can be employed in pairing with either in-depth, individual interviews or surveys [28]. It is useful for discovering and building dynamic hypotheses and understanding how the overall system works based on respondents' shared beliefs.

4) *Delphi groups*: Delphi is a similar focus group extension method, but it can also be accompanied by surveys or interview analysis [29]. Besides face to face, Delphi also can be done through online discussions. The Delphi method helps the researcher reach a good understanding of critical issues, fact-finding, exploration, or discovering what is actually known or not known the problem situation, including the group's consensus and disagreements.

5) *Observation*: Observation can provide a great deal of information regarding social structures, cultures, processes, and human interactions [30]. Observation needs to be in written form, either on paper or digital. This method requires strong dedication as an observer may need to observe and collect data for a long time. A skilful observer will capture useful observational data that can satisfy the requirements for the SD model.

6) *Participants observation*: In this method, the researcher is visible to participants under the non-strict assumption that the researcher will interact with the subject of study in his/her study situation. During observations, researchers may collect data through diaries, notebooks notes, or any other documents produced by the participants that are being studied. These are precious sources of information as these sources can be used to support primary data sources (i.e. interviews data) [10].

7) *Experimental approach*: Data collections in an experimental approach can be in many forms. Some data from the experimental approach can come in numerical form and qualitative form. If the data's findings show a different sight of the issues, the modeller can contact the actors and discuss the other views. If possible, the modeller may record the differences for further analysis [10].

8) *Questionnaires*: Some modellers begin the questionnaires by building a small SD model first and giving the questionnaire to the participants to get their feedback. The questionnaires can be closed-ended or open-ended. The closed-ended type is primarily employed when the modeller wants respondents to see whether they agree or disagree with specific issues. Open-ended questions are mainly used when the modeller wants respondents to brainstorm (identifying variables), rank order information, and produce causal reasoning. A questionnaire can also be used as a means to search parameter value for variables [31]. Questionnaires are suitable for a group of people who are geographically not

together, or when the number of people in the interest group is large [23]. This type of data collection can also be employed within the Delphi approach and in multiple focus groups.

9) *Group building*: Using this method, selected group members or stakeholders are gathered together physically in one place and brainstorm together [23]. The aim is to build the model in a team where team members can communicate and share their mental databases [9], [20], [32]–[35]. Group building might involve one or more sessions to build the conceptual model. By communications, stakeholders from different domains can share knowledge, build understanding and reach the same level of consensus [34][36]. For SD, developing a model in a team has been familiarised under several names such Participatory Modelling, Participatory Simulations, Mediated Modelling, Group Model Building, Shared Vision Planning, Collaborative Learning and perhaps many more [32]. In Operation Research, this can be established in two ways. One is building with an expert, and the other is building with a facilitator [37]. Building with an expert involves OR consultant handling the client's problem/situation. Appointments and meetings are set up. Based on the information shared, the OR consultant will build a model to develop an optimal solution. Whereas in facilitator form, the consultant and the client co-develop a model together, perhaps in a series of workshops. Even though both approaches have slight differences, both methods are very interactive, making them suitable approaches in engaging stakeholders.

10) *Meetings in social media*: This method requires all the participants to have reliable internet access, the same applications installed in their computers or phones (e.g. Zooms, Cisco Webex and Microsoft Teams), and registered accounts. These platforms are proven useful, especially when participants are physically far away [38]. This method is believed able to replace physical meetings whenever required. For example, during the lockdown, quarantine time or work from home during COVID-19 outbreaks. Social media meetings for data collection can be employed with other approaches such as interviews, focus groups, Delphi, group model building and perhaps many more. Several SD experts have recently promoted social media as a platform for data collection and communication medium for SD development.

## B. Written or Textual Database

The written database contains information in the form of text. Some researchers even recommended the use of text analytics tools and text analysis software [39] or namely as Computer-Aided Qualitative Data Analysis Software (CAQDAS), to support analysis activities [40]. For examples, Nvivo, Atlas.ti etc. With these softwares, analysis on non-textual evidence such as videos, images, audio recordings, pictorials and many more can be used as supporting evidence. Despite that, this still possesses challenges as modellers are required to move between qualitative and quantitative data. However, qualitative analysis helps modellers ground textual information and apply it in the model building process. This

also allows modellers to create a storyline of the system of the case [10] (see Fig. 3). A close example of this approach is a document-model-building strategy [41].

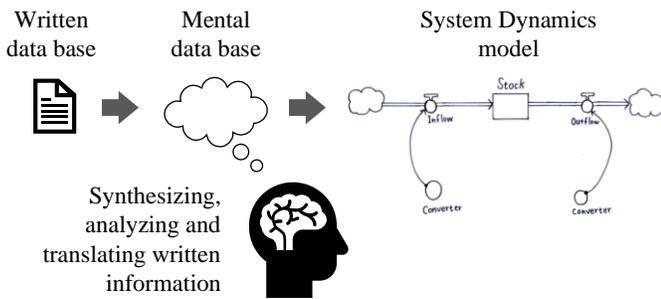


Fig. 3. Extracting Knowledge from a Written Database and Translate it into an SD Model [10].

For this, five qualitative analysis from social sciences field seems a suitable approach to be utilised here, as suggested by Luna-Reyes and Andersen [10]. However, this paper extends another one more, Semantic Analysis [42], into the group. In total, the six methods are briefly explained from (1) to (6).

#### 1) Hermeneutics

- Description: A qualitative analysis of any written text from documents, transcribed conversations, images, analogue recordings (audiotapes or videotapes), digital audio recordings and video recordings.
- Purpose: To find meanings and the pattern of relationship. This includes how they are linked to specific characteristics or expressions of specific themes in a particular study context, supporting evidence or contradicting one another.

#### 2) Discourse Analysis

- Description: A qualitative method used to study people's interactions in their natural settings. This method is suitable to be applied with observation as a method to collect data.
- Purpose: To understand how interactions and pattern of behaviours.

#### 3) Grounded Theory

- Description: A set of techniques employed to spot themes or concepts across texts. The methods can be performed on any textual data such as promotional adverts, interview transcriptions, memoranda, memorabilia, meeting minutes.
- Purpose: to link these concepts and to generate meaningful theories.

#### 4) Ethnographic decision model

- Description: The researcher's interviews are oriented toward a specific decision or policy in the system.
- Purpose: To understand the reason behind a person's decision in a particular circumstance. This approach can help the modeller to build a decision tree (or

dendrogram) describing the decision alternatives and processes.

#### 5) Content analysis

- Description: consists of a deductive coding technique, where the researcher chooses and defines a set of codes to be used. Then, researchers organise their data into a matrix of codes and texts according to the unit of analysis selected for the study. The matrix data will be analysed using almost any statistical method to test the level of agreement between coders or do qualitatively.
- Purpose: to analyse meanings of content, or causal and relationships within texts, photographs, films or digital resources. This is carried out by quantitatively using statistical methods, or by qualitative methods.

#### 6) Semantic analysis

- Description: consists of a process of extracting meaning from text or digital resources such as video recordings. This process is useful in obtaining the understanding of the system and meaning from documents.
- Purpose: to build or validate knowledge representations about the problem domain in a particular context.

### C. Numerical Database

The third data source is a numerical database. According to Forrester, the numerical database is valuable in several ways [6]. Firstly, the numerical database is useful for a parameter value. Mainly, this serves as the input of the model. Secondly, numerical data can summarise characteristic behaviour between variables. Thirdly, numerical data can contain time-series information. This information is often best for comparison with model output. Fourthly, numerical data allows SD simulation to work for quantitative analysis. It brings out the quantitative side of SD that can provide insights for possible improvements [43].

In some sense, it is believed that numerical data can provide more accurate and reliable insights than qualitative data [14]. Simultaneously, numerical data are often being discriminated against for determining model parameters [6]. Sterman specifically highlighted in his book Business Dynamics that "...no numerical data are available for many of the variables known to be critical to decision making..." [14]. For some time, this has been true for years. As a solution, Sterman suggested proper statistical methods to estimate parameters and assess the model's ability to replicate historical data when numerical data are available and suggested to look for alternative ways to measure whenever no numerical data is available [44].

Looking back in the early years, SD was not designated for numerically data-intensive applications. SD is initially intended for small data or poor data situations [45]. Traditional SD applications are usually fed with data from spreadsheet or CSV files or Microsoft Excels [46]. However, as years go by, in the era of Big Data (BD), Data Science (DS), Internet of Things (IoT), Business Intelligence and Analytics (BIA) and Industry 4.0, opportunities for SD to expand its capability seems promising and very inviting [16], [47]–[52]. With the blooming

of new technologies and applications, new arguments are starting to emerge. This can be seen from the enormous technological advances in computer technologies over the last decades. It seems fair to say that the limitations for data and storage are no longer valid. According to Pruyt, the massive amount of numerical data can enriched SD potentials in three ways “(1) to obtain useful inputs and information from (big) data, (2) to infer plausible theories and model structures from (big) data, and (3) to analyses and interpret model-generated data” [15]. Thus, the usage of these available data sources deserved to be reflected. Not every case can be considered as big data cases. Some numerical data is not big but adequate. Therefore, this arguably depends on the case study.

Apart from the mental database and written database, databases or data warehouses have become new goldmines of potential numerical data sources. Although many more specialised tools have yet to be developed [46], several SD software can support database connectivity. For examples such as (1) VenSim (DSS version) [53], (2) Anylogic [54], (3) PowerSim, and (4) iThink Some use csv-files transfer such in STELLA [46]. There are also free opensource tools such as SimSyn. This comes with a graphical user interface (GUI), connecting VENSIM to a PostgreSQL database [46]. Other examples of third-party tools such as PySD can connect the traditional SD from Vensim; iThink, or STELLA with databases and models [16]; XMILE (eXtensible Model Interchange Language), which allows SD model’s connection with the database and other analytical tools [55]; or DEE protocol (dynamic data exchange) allows data transfer between SD and other models, tools and databases.

Besides database, outputs from other simulation models also can be potential data sources for SD model [9], [15], [16], [48], [56]. If one model’s output becomes the input to the second model in a single flow, ‘loose-coupling’ between two models seems a good approach. There are many possible ways to couple the models for more complex interactions between two (or more) models, including a multi-directional flow of data. This depends on the functional suitability of the modelling approaches [9]. Potential data sources can also come from Data Science methods such as data mining. Machine learning can be mould into techniques that can catch selected data from a pool of data and use as inputs to feed SD models. Besides Big Data, some studies are already jump in to real-time data streams [15], [48], [56], [57]. Up to the present, it is no longer a surprise to see that initiative to using big data sources are already initiated by many SD researchers [17], [46], [56]–[58].

### III. ALIGNING DATA COLLECTIONS METHODS WITH SYSTEM DYNAMICS METHODOLOGY

SD researchers classify SD methodology into two mainstreams. One is Qualitative SD, and one is Quantitative SD. Some SD researchers may argue that developing qualitative models alone may not be enough to complete the problem. This is because SD relies on quantitative data to generate feedback models in simulation. This feedback provides insights for further improvements and provides a sense of certainty in prediction [21]. However, some researchers had claimed to have utilised both types of SD in

their work. The rationale of this is because the early stages of SD methodology are emphasising on qualitative knowledge. Based on qualitative knowledge, the latter then becomes the foundation of the quantitative approach [43]. This perception seems mutual among SD experts. Therefore, this paper is focusing on the combination of both types.

Based on classic literature, SD methodologies are organised in several stages, ranging from three to seven stages [10], [59]. Although they have different numbers of stages, the modelling process foundations are pretty similar [10]. For this paper, the four stages of SD methodology proposed by [9] and [10] are adopted together. The stages are distinguished as follows: (1) problem conceptualisation, (2) model formulation, (3) model verification and validation, (4) model use and application. This SD methodology framework will be used as a reference frame to discuss further how qualitative data and numerical (quantitative) data are linked to the SD methodology and at what stage are they useful. As a result of this alignment, potential data collection methods for SD methodology is organised in Table I.

#### A. Problem Conceptualisation

Problem conceptualisation stage is considered as ‘qualitative stage’ by most SD researchers [10], [39], [60]. In this stage, the SD model’s purpose needs to be determined and justified through problem identification activities [9], [60]. Problem conceptualisation process involves framing and structuring the problem of the case. How stakeholders see the problem situation, how they perceive it can be diverse and very subjective. If the uncertainty issue is of concern, then the uncertainty elements must be considered in the context of the model’s purposes. This process strongly relies on experts’ or modellers’ ability to extract the knowledge that resides in the heads of experts, modellers, and the rest of the stakeholders [61].

After critical stakeholders are identified, meetings and appointments are set up and scheduled. This is important because qualitative understandings of the problem case can be successfully gained through communications and interactions with stakeholders and not without [33]. These activities may include social learning by interest groups, knowledge elicitation and review, data assessment, discovering coverage, limitations, gaps, inconsistencies and many more, as explained in [9].

The suggested data collection method at this stage is mostly the qualitative approach. Examples are group model building team, interviews, oral history, focus groups, hermeneutics, discourse analysis and content analysis [10]. This is important to fulfil the SD model requirements. Suitable data will be collected and selected for model developments in the early stage. The rationale is to ensure that the case data must be enough to describe key variables at a minimum. This ensures the system feedback needs to be understood well enough to provide plausible estimates representing the relationships mathematically [9].

Traditionally, face to face communication interactions is encouraged throughout the SD stages, especially in the early stage. It is the most effective way to increase the

understanding with better engagement and fewer distractions. However, one may opt to have social media meetings as an alternative option if physical contact is impossible. This is useful, particularly during the quarantine period due to COVID19 [38]. Although online discussions may seem to be a promising solution, most communication theories argue that online discussion is not as effective as face-to-face discussion [62]. Therefore, if this approach is chosen, modellers have to embrace the advantages and bear the technology's disadvantages. They have to plan their data collections as best as they can.

### B. Model Formulation

Model Formulation is a stage where the concept of a dynamic hypothesis model is translated into the formal quantitative model. In other words, this can be described as the transfiguration of a qualitative conceptual model to a quantitative numerical model.

Formulating and designing a model is not a straightforward process. In this process, the modeller needs to use their understandings and judgmental data to build the model. The initial SD model will slowly evolve and expand in more than one attempts iteratively. Modeller's judgments on methodologies selection for developing SD models are critical to ensure the model's results. Since different SD mappings will lead to different results, selections would depend on how well specific SD mapping can support the model objective [9], [63]. This is also to determine whether the method can satisfy possible interests, decision options, and impacts. This is because the formulations of non-linear functions and linear is a highly qualitative process. In this stage, the modellers must gather as much information as possible.

Most of the times, modellers have to utilised what they can to incorporate variables and parameters into the model. Usually, modellers will look at (published and non-published) academic and industry documents, including reports to get the parameter values, to get the model variables, or to get ideas of similar models' structures and components of a system. A systematic or non-systematic reviews framework can be employed on documents collection to seek relevant resources in a more organised manner [41]. In qualitative modelling especially document model building approach in SD, hermeneutics, content analysis like Decision Making Trial and Evaluation Lab (DEMATEL) [64], and text analysis [39] are helpful to address the cause and effects relationships among components of a system [41]. On the same side of the coin, grounded theory and ethnographic decision models can guide and enrich the identification of critical structures and formulations based on meaning and connections [10], [39]. In some cases, statistical analysis, such as regression analysis, helps address the relationships between components from multiple sources [65].

With today's technology, knowledge is more than just in straight textual forms. Digital information can be a valuable pool of information too. For example, the information in pictorial forms like info-graphics from social media, such as Facebook, Twitter, or online newspapers. Furthermore, essential information can lie inside video recordings or audio recordings, too (analogue and digital). So, knowing where to

search, how to capture information and analyse information are critical. This is because the types of available data can shape the model's mapping [9].

It is also widespread practice for the modeller to consider variables and non-linear relations for which quantitative data are not available. Interestingly, this process can be accompanied by additional qualitative techniques to add formality to the process. Vital sources can come from interactions with individuals, groups, and clients [37]. For mental database elicitation, a number of methods appear to be more beneficial to obtain the system structures, parameters, and the policies to be included in the model [10], such as interviews, focus groups with Delphi, observation, from participant observation [14] and many more. Besides physical communications, online communications [38] can also play an essential role in data collection, such as online meetings via social media, including online interviews, phone interviews, interview via e-mails or in combination with other methods such as focus groups with online interviews, or surveys. Typically, all of the collected information will be transcribed into text and analysed.

Later in this stage, qualitative data could appear less useful and quantitative data start to take over interchangeably [10]. The most common way to elicit parameter values from stakeholders is through interviews, group sessions, or Delphi. Modeller can ask group members to estimate an unknown parameter individually. After collecting initial individual judgments, the modeller gives back a summary of the values gathered. Besides mental and written sources, numerical data sources can be retrieved from CSV files or database [46] or direct connection from databases, data warehouses [65] or devices like sensors or meters [66]. These data are usually favoured because of their completeness. These numerical figures can be presented in a single number or in time series [16], [66], or in streaming data [15], [46], [65]. If multiple simulation models are involved, the output data from other simulation models can also serve as input for SD depending on the model objectives [9], [16]. Apart from that, modellers have to determine the adequacy of data in term of size. If a real-time simulation is part of the model objective, then the suitable tools must be used to feed the SD model smoothly.

### C. Model Verification and Validation

The validity of a model is assessed according to the purpose for which it is developed [42]. Knowing the purpose of the model can help determine which data patterns are important for model evaluation. This stage always interchangeably back and forth with the "Model Formulation" stage if there are additional changes in the model structure. To be useful, simulation models must resemble the problem owner's environment in the real world. Generally, there are two common testings to increase confidence in the SD model [9], [42], [67]: structural testing and behavioural testing.

In structural testing, testing is done by direct comparison with the real system structure. These tests are performed to see how well the model's logic represents the system's real-world structure [9], [67]. These tests also look into the sense of the model (including mathematical equations). Evaluation of the model structure is often hard to formalise and quantify. This is

usually conducted qualitatively. To ensure the logic is right, stakeholders verifications are needed [35]. The stakeholders can be experts, or analysts, or problem owners. This can be done through face to face or online interviews, focus groups, Delphi groups, experimental approaches, walk-through, formal inspections, or semantic analysis [10], [42]. Cross-checking with secondary sources like reports, statistical yearbooks, and observations can increase the model's reliability and validity [68].

In behavioural testing, testing is done to assess how close the model outputs can replicate the real-world system behaviour. Typically, this is achieved by looking at general patterns produced by the model, for examples, growth, decline, and oscillation [67]. One way of doing this is by using a statistical comparison of the data against the model output. This is usually done through goodness-fit measures such as correlation coefficient, root mean squared error, mean absolute relative error, maximum relative error and discrepancy coefficient in cases where adequate data were available. In this context, numerical data from historical data, operational data, from database or data warehouse or any observed data from the fields are precious for testings.

Both of these structural test and the behavioural test is highly needed, especially in poor data situation. After all, most SD practitioners agree that it is rare to have sufficient data for all variables. It is very uncommon to have adequate data for every SD model variable [9], [60]. Therefore, formal model testing should be done whenever necessary. Simultaneously, other evaluations such as sensitivity analysis, peer review, results from patterns analysis and model comparison analysis can be used as complement [42]. All these are to ensure the output produced by the model is reasonable and acceptable.

#### D. Model use and Application

The key activities in this stage are model simulation, decision analysis, and discussions. At this stage, the model is believed ready to be used and serve its purposes. In order to run the model, numerical data should be made available and ready for simulation, either in real-time mode or otherwise. For examples, in CSV files, from database or warehouses, or output from models. The size may vary. Sometimes this can take a series of simulation runs.

Model-based simulation, like SD, can act as an analysis enabler of various situations by modelling and simulating the model over time within a computer program [4]. With the SD model, the decision-maker can design and simulate a series of tests for system change [69]. Thus, they can test specific policies, narrate insightful stories about policy experiments, and generate discussion about the problem actors related to the result. This means that decision analysis can be evaluated through experimental approaches and evaluated qualitatively through active discussions [9]. That is why, in this stage, the uses of qualitative data and data analysis in SD are rich, and could be richer still.

Apart from the experimental approach above, oral history and grounded theory can help the sense-making from the

simulation results and from the modelling process itself by providing a record of how variables or pieces of the structure can be formulated or reformulated along the way [10]. With today's communication technology, group discussion (via face to face or online) methods such as Delphi or focus groups are useful for generating discussion among actors about the meaning of the policy experiments' model results and the stories generated by the model. In oral history, discourse analysis, and grounded theory, the modeller also uses the learning accumulated during the modelling process. If a survey or questionnaires is needed, it might be helpful to be applied here too, depending on its suitability.

#### IV. CONCLUDING REMARKS

Data sources are very important for SD development. Based on the three primary pools of databases (mental, written and numerical) suggested by SD forefather Forrester, it is noted that no data are entirely perfect. Either mental data, qualitative data or numerical data, all of them possess the tendency to be flawed, biased and unreliable. The mental database is hard to capture because it is in the head. The mental database needs to be shared, so the context of the problem case is understood. The written database requires mental digestion by the modeller to translate them into knowledge mapping in SD. Numerical is reliable, but back then, numerical data was not available as much as today. Due to technological advancements, the numerical data base's traditional perceptions are now no longer fit in today's era. Thus, this deserves attention and highlighted. Due to this reason, the three sources are worth to put into consideration depending on the problem case.

At the end of this paper, suggestions of potential data collection methods are elaborately discussed and aligned with four staged SD modelling methodology. According to Sterman, system dynamics modellers should master the state of art and use these tools and follow new developments as the tools continue to evolve and innovate to develop new methods appropriate for the models. Hopefully, the alignment of SD methodology with the potential data collection methods can impact the entire modelling procedure whilst respecting the traditional SD modelling approach's key components. This is shown in various options, where the best selections of the methods to be used in an SD modelling process can be selected from Table I.

In summary, this paper provides a brief overview of the currently existing knowledge extraction methods for SD modelling. It mainly emphasises the potential data sources and their suitability for each stage/step in the process of modelling. It also gives a good foundation for understanding the existing alternatives in the field of SD modelling. Moreover, the adaptation presented in Table I for suggested data sources in each modelling phase represents a practical synthesis of existing choices as guidelines for current practice. Since different cases might face different types of problem situations, the selection of data collection methods should be based on what is feasible and how they can complement or compensate each other.

TABLE I. SUMMARY OF SUGGESTED DATA SOURCES FOR SD MODELLING. ADAPTED FROM [9], [10], [42], [67]

SD stage	Modellings steps	Suggested methods to extract mental, written and numerical databases	Suggested numerical data sources
Stage 1: Problem Conceptualization			
Model purpose	1. Define the model purpose 2. Specify modelling context and objectives	<u>For problem articulation and developing dynamic hypothesis:</u> • group model building • face to face interviews	Usually, numerical data sources are not determined in this stage yet. However, this will depend on the case and modeller.
Dynamic hypothesis conceptualisation	3. Conceptualize system, specify data and other prior knowledge	• oral history • face to face focus groups • hermeneutics • discourse analysis • content analysis • online interviews • online meetings • online focus groups	
Stage 2: Model Formulation			
Simulation model development	4. Select the model features 5. Determine how to find model structure and parameter values 6. Select estimation/ performance criteria and algorithm 7. Identify the model structure and parameters	<u>For parameters, policies and model formulations</u> • group model building • interviews • oral history • focus groups • Delphi groups • content analysis • observation • grounded theory • ethnographic decision models • online interviews • phone interviews • interview via e-mails • online meetings • online focus groups • questionnaires	<u>For running the model:</u> <u>Potential Sources:</u> • CSV files or spreadsheets • databases, or data warehouses, • outputs from a single model. • outputs from multiple models • devices (sensors, satellites, etc.)  <u>For obtaining parameter values</u> • statistical analysis • outputs from other models
Stage 3: Model Verification and Validation			
Model structure and model behaviour test	8. Carry out model verification and diagnostic testing 9. Quantify uncertainty 10. Perform model evaluation and testing	<u>To obtain expert judgment about model structure and behaviour</u> • interviews • focus groups • Delphi groups • experimental approaches • walk-through • formal inspections • semantic analysis • online interviews • online meetings • online focus groups	<u>For running the model:</u> <u>Potential Sources:</u> • CSV files or spreadsheets • databases, or data warehouses, • outputs from a single model. • outputs from multiple models • devices (sensors, satellites, etc.)
Stage 4: Model Use and Application			
Model usage	Revisit model purpose and evaluate the achievement.	<u>Techniques to test policies</u> • experimental approaches  <u>Techniques to create insightful stories to communicate model results:</u> • oral history • grounded theory • discourse analysis • group model building • online meetings  <u>Techniques to generate discussion among problem actors</u> • Delphi groups • focus groups • survey/questionnaires • online meetings	<u>For running the model:</u> <u>Potential Sources:</u> • CSV files or spreadsheets • databases, or data warehouses, • outputs from a single model. • outputs from multiple models • devices (sensors, satellites, etc.)

#### ACKNOWLEDGMENT

This study is fully sponsored under the MyPhD-MyBrain15 Scholarship by the Ministry of Higher Education Malaysia (MoHE). In addition to that, this study is also supported by research grant RDU200756, funded by Universiti Malaysia Pahang. Special thanks to several individuals who were willing to spend their time giving constructive comments during the development and improvement of this manuscript.

#### REFERENCES

- [1] J. W. Forrester, "Industrial dynamics," *J. Oper. Res. Soc.*, vol. 48, no. 10, pp. 1037–1041, 1997.
- [2] J. W. Forrester, *Industrial dynamics*. Cambridge: MIT press, 1961.
- [3] J. Sterman, R. Oliva, K. Linderman, and E. Bendoly, "System dynamics perspectives and modeling opportunities for research in operations management," *J. Oper. Manag.*, vol. 39–40, no. February, pp. 1–5, 2015, doi: 10.1016/j.jom.2015.07.001.
- [4] J. Banks, "Introduction to simulation," in *2000 Winter Simulation Conference Proceedings*, 2000, no. 1, pp. 9–16, doi: 10.1109/WSC.2000.899166.
- [5] E. F. Wolstenholme, "System Dynamics: A System Methodology or A System Modelling Technique," *Dynamica*, vol. 9, pp. 84–90, 1983.
- [6] J. W. Forrester, "System Dynamics and The Lessons of 35 Years," in *A systems-based approach to policymaking*, Springer, 1993, pp. 199–240.
- [7] S. Koul, O. A. Falebita, J.-F. K. Akinbami, and J. B. Akaraki, "System dynamics, uncertainty and hydrocarbon resources modelling: A systematic review," *Renew. Sustain. Energy Rev.*, vol. 59, pp. 199–205, Jun. 2016, doi: <http://dx.doi.org/10.1016/j.rser.2015.12.088>.
- [8] A. Mohammadi and M. Tavakolan, "Identifying safety archetypes of construction workers using system dynamics and content analysis," *Saf. Sci.*, vol. 129, no. March, p. 104831, 2020, doi: 10.1016/j.ssci.2020.104831.
- [9] S. Elsayah et al., "An overview of the system dynamics process for integrated modelling of socio-ecological systems: Lessons on good modelling practice from five case studies," *Environ. Model. Softw.*, vol. 93, pp. 127–145, 2017, doi: 10.1016/j.envsoft.2017.03.001.
- [10] L. F. Luna-Reyes and D. L. Andersen, "Collecting and analysing qualitative data for system dynamics: Methods and models," *Syst. Dyn. Rev.*, vol. 19, no. 4, pp. 271–296, 2003, doi: 10.1002/sdr.280.
- [11] G. Linnéusson, A. H. C. Ng, and T. Aslam, "Quantitative analysis of a conceptual system dynamics maintenance performance model using multi-objective optimisation," *J. Simul.*, vol. 12, no. 2, pp. 171–189, 2018, doi: 10.1080/17477778.2018.1467849.
- [12] A. Green, Bart N and Johnson, Claire D and Adams, "Writing narrative literature reviews for peer-reviewed journals: secrets of the trade," *J. Chiropr. Med.*, vol. 5, no. 3, pp. 101–117, 2006.
- [13] J. Sterman, "Learning in and about complex systems," *Syst. Dyn. Rev.*, vol. 10, no. 2–3, pp. 291–330, 1994.
- [14] J. Sterman, *Business dynamics: systems thinking and modeling for a complex world*. 2000.
- [15] E. Pruyt, "From Data-Poor to Data-Rich: System Dynamics in the Era of Big Data," *32nd Int. Conf. Syst. Dyn. Soc.*, no. 1, pp. 1–12, 2014.
- [16] J. Houghton and M. Siegel, "Advanced data analytics for system dynamics models using PySD Motivation: The (coming of) age of Big Data," *Revolution*, vol. 3, no. 4, 2015, [Online]. Available: <http://www.systemdynamics.org/conferences/2015/papers/P1172.pdf>.
- [17] E. Pruyt, "Integrating Systems Modelling and Data Science: The Joint Future of Simulation and Big Data Science," *Artif. Intell. Concepts, Methodol. Tools, Appl.*, pp. 822–840, 2017.
- [18] J. W. Forrester, "System dynamics, systems thinking, and soft OR," *Syst. Dyn. Rev.*, vol. 10, no. 2 - 3, pp. 245–256, 1994.
- [19] J. K. Doyle and D. N. Ford, "Mental models concepts for system dynamics research," 1998.
- [20] M. Schaffernicht and S. N. Groesser, "A comprehensive method for comparing mental models of dynamic systems," *Eur. J. Oper. Res.*, vol. 210, no. 1, pp. 57–67, 2011, doi: 10.1016/j.ejor.2010.09.003.
- [21] D. R. Towill, "System dynamics- background, methodology and applications. 1. Background and methodology," *Computing & Control Engineering Journal*, vol. 4, no. 5, pp. 201–208, 1993, doi: 10.1049/cee:19930050.
- [22] J. C. Refsgaard, J. P. van der Sluijs, A. L. Højberg, and P. A. Vanrolleghem, "Uncertainty in the environmental modelling process - A framework and guidance," *Environ. Model. Softw.*, vol. 22, no. 11, pp. 1543–1556, 2007, doi: 10.1016/j.envsoft.2007.02.004.
- [23] J. A. M. Vennix, D. F. Andersen, G. P. Richardson, and J. Rohrbaugh, "Model-building for group decision support: Issues and alternatives in knowledge elicitation," *Eur. J. Oper. Res.*, vol. 59, no. 1, pp. 28–41, 1992, doi: 10.1016/0377-2217(92)90005-T.
- [24] L. A. Burke and M. K. Miller, "Phone interviewing as a means of data collection: Lessons learned and practical recommendations," in *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 2001, vol. 2, no. 2.
- [25] K. Gibson, "Bridging the digital divide: Reflections on using WhatsApp instant messenger interviews in youth research," *Qual. Res. Psychol.*, pp. 1–21, 2020.
- [26] E. Burns, "Developing e-mail interview practices in qualitative research," *Sociol. Res. online*, vol. 15, no. 4, pp. 24–35, 2010.
- [27] D. A. Ritchie, *Doing oral history*. Oxford University Press, 2014.
- [28] D. L. Morgan, "Focus groups," *Annu. Rev. Sociol.*, vol. 22, no. 1, pp. 129–152, 1996.
- [29] C.-C. Hsu and B. A. Sandford, "The Delphi technique: making sense of consensus," *Pract. Assessment, Res. Eval.*, vol. 12, no. 1, p. 10, 2007.
- [30] D. E. Polkinghorne, "Language and meaning: Data collection in qualitative research," *J. Couns. Psychol.*, vol. 52, no. 2, pp. 137–145, 2005, doi: 10.1037/0022-0167.52.2.137.
- [31] W. Jing, H. I. Naji, R. N. Zehawi, Z. H. Ali, N. Al-Ansari, and Z. M. Yaseen, "System dynamics modeling strategy for civil construction projects: The concept of successive legislation periods," *Symmetry (Basel)*, vol. 11, no. 5, pp. 1–18, 2019, doi: 10.3390/sym11050677.
- [32] A. Voinov and F. Bousquet, "Modelling with stakeholders," *Environ. Model. Softw.*, vol. 25, no. 11, pp. 1268–1281, 2010.
- [33] S. Eker, N. Zimmermann, S. Carnohan, and M. Davies, "Participatory system dynamics modelling for housing, energy and wellbeing interactions," *Build. Res. Inf.*, vol. 46, no. 7, pp. 738–754, 2018, doi: 10.1080/09613218.2017.1362919.
- [34] A. van Bruggen, I. Nikolic, and J. Kwakkel, "Modeling with stakeholders for transformative change," *Sustain.*, vol. 11, no. 3, pp. 1–21, 2019, doi: 10.3390/su11030825.
- [35] M. Schwanager and S. Groesser, "System Dynamics Modeling: Validation for Quality Assurance," *Syst. Dyn. Theory Appl.*, pp. 119–138, 2020, doi: 10.1007/978-3-642-27737-5\_540-4.
- [36] M. Zolfagharian, R. Akbari, and H. Fartookzadeh, "Theory of Knowledge in System Dynamics Models," *Found. Sci.*, vol. 19, no. 2, pp. 189–207, 2013, doi: 10.1007/s10699-013-9328-9.
- [37] L. A. Franco and G. Montibeller, "Facilitated modelling in operational research," *Eur. J. Oper. Res.*, vol. 205, no. 3, pp. 489–500, 2010, doi: 10.1016/j.ejor.2009.09.030.
- [38] N. Zimmermann et al., "Moving online: reflections from conducting system dynamics workshops in virtual settings," *Syst. Dyn. Rev.*, pp. 1–13, 2020, doi: 10.1002/sdr.1667.
- [39] S. Eker and N. Zimmermann, "Using Textual Data in System Dynamics Model Conceptualization," *Systems*, vol. 4, no. 3, p. 28, 2016, doi: 10.3390/systems4030028.
- [40] M. Yearworth and L. White, "The uses of qualitative data in multimethodology: Developing causal loop diagrams during the coding process," *Eur. J. Oper. Res.*, vol. 231, no. 1, pp. 151–161, 2013, doi: 10.1016/j.ejor.2013.05.002.
- [41] A. Haji Gholam Saryazdi, A. Rajabzadeh Ghatari, A. Mashayekhi, and A. Hassanzadeh, "Designing a qualitative system dynamics model of crowdfunding by document model building," *Qual. Res. Financ. Mark.*, vol. 12, no. 2, pp. 197–224, 2019, doi: 10.1108/QRFM-07-2018-0082.
- [42] Y. Barlas, "Formal aspects of model validity and validation in system dynamics," *Syst. Dyn. Rev.*, vol. 12, no. 3, pp. 183–210, 1996.

- [43] E. F. Wolstenholme, "The Basic Concepts of System Dynamics Optimisation," *Syst. Pract.*, vol. 1, no. 1, 1988.
- [44] J. Sterman, "System dynamics at sixty: the path forward," *Syst. Dyn. Rev.*, vol. 34, no. 1, pp. 5–47, 2018, doi: 10.1002/sdr.1601.
- [45] R. Moorlag, W. Auping, and E. Pruyt, "Exploring the effects of shale gas development on natural gas markets: a multi-method approach," 2014.
- [46] C. Neuwirth, "System dynamics simulations for data-intensive applications," *Environ. Model. Softw.*, vol. 96, pp. 140–145, 2017, doi: <http://dx.doi.org/10.1016/j.envsoft.2017.06.017>.
- [47] E. Pruyt, "Using Small Models for Big Issues: Exploratory System Dynamics Modelling and Analysis for Insightful Crisis Management.," 2010, [Online]. Available: <http://www.systemdynamics.org/conferences/2010/proceed/papers/P1266.pdf>.
- [48] M. Schluse, M. Prigemeyer, L. Atorf, and J. Rossmann, "Experimentable digital twins-streamlining simulation-based systems engineering for Industry 4.0," *IEEE Trans. Ind. Informatics*, vol. 14, no. 4, pp. 1722–1731, 2018, doi: 10.1109/TII.2018.2804917.
- [49] E. Casado, "Expanding business intelligence power with system dynamics," in *Business Intelligence in the Digital Economy: Opportunities, Limitations and Risks*, IGI Global, 2004, pp. 126–140.
- [50] T. Qu et al., "System dynamics analysis for an Internet-of-Things-enabled production logistics system," *Int. J. Prod. Res.*, vol. 7543, no. August, pp. 1–28, Apr. 2016, doi: 10.1080/00207543.2016.1173738.
- [51] A. Ibrahim, T. Asmawaty Abdul Kadir, and A. Kamaludin, "Industry 4.0: Eyeing the Future via Simulation," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 769, no. 1, pp. 0–11, 2020, doi: 10.1088/1757-899X/769/1/012001.
- [52] N. Darabi and N. Hosseinichimeh, "System dynamics modeling in health and medicine: a systematic literature review," *Syst. Dyn. Rev.*, vol. 36, no. 1, pp. 29–73, 2020, doi: 10.1002/sdr.1646.
- [53] V. Systems, "Vensim Help. Connecting to Databases with ODBC [www Document]," 2016. [https://www.vensim.com/documentation/index.html?users\\_guide.htm](https://www.vensim.com/documentation/index.html?users_guide.htm) (accessed Apr. 05, 2019).
- [54] AnyLogic, "AnyLogic Help. AnyLogic Database [www Document]," 2017. <https://help.anylogic.com/index.jsp> (accessed Apr. 05, 2019).
- [55] R. L. Eberlein and K. J. Chichakly, "XMILE: a new standard for system dynamics," *Syst. Dyn. Rev.*, vol. 29, no. 3, pp. 188–195, 2013, doi: 10.1002/sdr.1504.
- [56] E. Rich et al., "An experimental platform for interpreting open-source health data through integration with dynamic disease models and geoplots," 2015 17th International Conference on E-health Networking, Application & Services (HealthCom). pp. 97–101, 2015, doi: 10.1109/HealthCom.2015.7454480.
- [57] M. Curran, E. Howley, and J. Duggan, "An Analytics Framework to Support Surge Capacity Planning for Emerging Epidemics," *Proc. 6th Int. Conf. Digit. Heal. Conf.*, no. January, pp. 151–155, 2016, doi: 10.1145/2896338.2896354.
- [58] M. Drobek, W. Gilani, and D. Soban, "A data driven and tool supported CLD creation approach," 32nd Int. Conf. Syst. Dyn. Soc., vol. The creati, no. July, pp. 1–20, 2014, [Online]. Available: <https://www.systemdynamics.org/assets/conferences/2014/proceed/papers/P1345.pdf>.
- [59] A. a Zagonel, "Model conceptualisation in Group Model Building: a review of the literature exploring the tension between representing reality and negotiating a social order," *Int. Syst. Dyn. Conf.*, no. February, pp. 1–68, 2002, doi: 10.1227/01.NEU.0000017465.78245.6C.
- [60] J. Sterman, "System dynamics modeling: tools for learning in a complex world," *Calif. Manage. Rev.*, vol. 43, no. 4, pp. 8–25, 2001.
- [61] F. Zare, S. Elsawah, A. Bagheri, E. Nabavi, and A. J. Jakeman, "Improved integrated water resource modelling by combining DPSIR and system dynamics conceptual modelling techniques," *J. Environ. Manage.*, vol. 246, no. June, pp. 27–41, 2019, doi: 10.1016/j.jenvman.2019.05.033.
- [62] S. J. Min, "Online vs. face-to-face deliberation: Effects on civic engagement," *J. Comput. Commun.*, vol. 12, no. 4, pp. 1369–1387, 2007, doi: 10.1111/j.1083-6101.2007.00377.x.
- [63] R. Scholz and O. Tietje, "Embedded Case Study Methods." SAGE Publications, Inc., Thousand Oaks, California, 2002, doi: 10.4135/9781412984027.
- [64] S. L. Si, X. Y. You, H. C. Liu, and P. Zhang, "DEMATEL Technique: A Systematic Review of the State-of-the-Art Literature on Methodologies and Applications," *Math. Probl. Eng.*, vol. 2018, no. 1, 2018, doi: 10.1155/2018/3696457.
- [65] E. Ekinci, Y. Kazancoglu, and S. K. Mangla, "Using system dynamics to assess the environmental management of cement industry in streaming data context," *Sci. Total Environ.*, vol. 715, p. 136948, 2020, doi: 10.1016/j.scitotenv.2020.136948.
- [66] F. Riva and E. Colombo, "System-dynamics modelling of the electricity-development nexus in rural electrification based on a Tanzanian case study," *Energy Sustain. Dev.*, vol. 56, pp. 128–143, 2020, doi: 10.1016/j.esd.2020.04.001.
- [67] K. H. Lim and B. Feng, "System Dynamics Modeling For Information System Research: Theory Development and Practical Application," *MIS Q. Manag. Inf. Syst.*, vol. 42, no. 4, pp. 1–28, 2018, doi: 10.25300/MISQ/2018/12749.
- [68] Y. Li et al., "Using system dynamics to assess the complexity of rural toilet retrofitting: Case study in eastern China," *J. Environ. Manage.*, vol. 280, no. October 2020, p. 111655, 2021, doi: 10.1016/j.jenvman.2020.111655.
- [69] J. P. Torres, M. Kunc, and F. O'Brien, "Supporting strategy using system dynamics," *Eur. J. Oper. Res.*, vol. 260, no. 3, pp. 1081–1094, 2017, doi: 10.1016/j.ejor.2017.01.018.

# Novel Modelling of the Hash-based Authentication of Data in Dynamic Cloud Environment

Anil Kumar G<sup>1</sup>

Assistant Professor, Department of Computer Science & Engineering, Channabasaveshwara Institute of Technology Gubbi, Tumkur, India  
Visvesvaraya Technological University, Belagavi, Karnataka, India

Shantala C.P<sup>2</sup>

Professor & Head, Department of Computer Science & Engineering, Channabasaveshwara Institute of Technology Gubbi, Tumkur, India  
Visvesvaraya Technological University, Belagavi, Karnataka, India

**Abstract**—A datacenter in a cloud environment houses a massive quantity of data in a distributed manner. However, with the increasing number of threats like data deduplication attack over the cloud environment, it is quite challenging to ascertain data's full-fledged security. In this regard, data integrity and security are highly questionable. A review of existing literature shows that the existing solutions are not much suitable to meet the requirements and support the existing distributed storage system's security demands concerning data integrity due to the usage of the inferior authentication mechanism. Also, the most frequently used public-key encryption is found not to be purely suitable resource constraint devices. Therefore, this manuscript presents a unique model of authentication of data where a simplified hashing proposition has been designed towards scheduling a distributed chain of data. The idea is to perform dynamic authentication that is present of any form of the adversary. The design of proposed scheme is lightweight which offers cross-verifiable hash-based challenges matching scheme with the provision of the non-repudiation of the tractions using the inclusion of a cloud auditor units. The experiment was carried on numerical computing tool considering, data volume, verification count and verification delay as prime performance metrics. The simulation outcomes shows that the proposed system excels in better security performance as well it is flexible compared to the existing system.

**Keywords**—Cloud computing; data deduplication; data integrity; data privacy; data security

## I. INTRODUCTION

The collaborative network-based application essentially requires cloud infrastructure to gain various advantages of availability and scalability including data storage requirements. There is various critical application used in the different functional domains of life including healthcare [1], banking [2], automated navigation system [3], transport safety [4], data security [5], secured vehicular network [6], query assessment [7], data authentication [8], selective authentication [9]. In all these applications, compromise of data integrity poses substantial security concerns. If their data are compromised, then a potential economic loss and fatal threats occur on the human being. Therefore, designing an efficient, flexible, robust, and cost-effective data authenticator for verifying integrity is an essential requirement for the data's security. The cloud service usually focuses on building the cloud services' core components, so they outsource the security requirement to

the Trusted Third Parties (TTP) [3]. There are pros and cons of relying on the TTP for the data authenticator, and even many of the collusive attacks have taken place in the recent past [10]. Though traditionally there exist many data authenticators, it lacks its feasibility because of few aspects such as the computing system evolving very dynamically. Another factor is that the attackers understand the data-authenticator's working principle and finds a way to break it. Thus, designing a robust and efficient data-authenticator to verify data integrity is an open research problem that requires researchers' attention.

The resource constraint devices fail to verify the integrity by running a local data-authenticator; some of the recent studies recommend blockchain for this purpose. Still, it is at a very nascent stage [11]. In recent times, healthcare systems potentially utilize pervasive computing integrated with the cloud infrastructure, where cloud storage is used to store patient information (P.I.). If these data are exposed to unauthorized users with malicious intension, then the data's integrity gets compromised, and in turn, a wrong diagnosis is performed. Therefore, it is an essential requirement to have a system or a method to verify P.I.'s integrity before utilizing it for medical references. The traditional approach for the verification of data-integrity involves the proprietary stakeholder itself as an authenticator. Another domain of the future system of intelligent transport system aims for a zero tolerance to the accidents that demand higher scalability on message verification operations in lower latency. Therefore, the requirement of data-authenticators adds, also, a low latency based fast data or message authentication. Blockchain technology may be promising to design distributed and strong data authenticator. There are many other applications such as the Internet of Vehicle, Spatial Query in geospatial, big data storage, and data sharing. These exhibit unique challenges and require customized treatment for data authentication for integrity verification. The applications like VANET require low delay-sensitive data authenticator. In contrast, the service-oriented architecture-based application needs to have a data authentication valid for the cross-domain. Another popular application based on the location requires verification of unique queries in low computational complexity. The WSN is used either independently or as a sub-network of IOT; the success of the application solely depends upon the timely delivery of the data using geographical routing protocols, whereas the simple denial of attack brings disruption into the

data delivery process that demands a suitable verifies to isolate the attacker nodes. Apart from these approaches, in the recent past, hardware-level security using FPGA implementation is gaining researchers' attraction, where the IoT devices to the cloud get authenticated at the hardware layer itself. The popularity of content delivery models through the cloud demands a computationally efficient and errorless joint protocol of auditing privacy-preservation and authentication [12]. One another challenge arises in Shared Storage Service (SSS), where it is essential to verify the data integrity effectively in the SSS for data, which is usually performed by the members-based auditing mechanism that poses higher computational overhead. However, the use of the lightweight method ignores security risk [13]. The process of data deduplication and integrity auditing efficacy requires optimal balance to establish a trust and cost factor [14]. The forensic process always requires access to reliable data that might be vulnerable to numerous exploits that. This problem requires a suitable verification system to verify the device's integrity, which fetches the records from the cloud [15]. The third-party-based auditor facilitates the auditing as a service (AaaS) model suffers from many challenges while providing data verification services; such challenges include non-repudiation proof sought by between the auditor and cloud service provider [16]. Integrity verification by cost-effective ways is generally not a very responsible way. The cloud infrastructure is an obvious choice today for the storage as well analytics platform for big data. The service providers make multiple replications to ensure reliable availability of the data. The existing auditing processes lack the security standards, and the overheads and synchronization of the authentication with auditing do not take place simultaneously [18]. The cloud infrastructure is now not only supporting data storage. In contrast, it also provides facilities to operate on it for modification of the data blocks. Still, the traditional remotely operated approach to ensure data integrity lacks the public auditing mechanism, which brings lots of conflicts of interest and credibility [20]. The evolution process will continue as the data verities keep coming into reality and its storage mechanism. This paper proposes a method of authentication of the cloud user over the vulnerable deployment scenario. Simultaneously, the proposed system also implements a mechanism towards auditing the integrity of the cloud data. The paper's organization is as follows: Section II discusses the current work towards data integrity, followed by briefing the research gap and different challenges from the existing system in Section III. Discussion of the proposed method is carried out in Section IV while obtain outcome of the study is briefed in Section V. Finally, Section VI discusses the summary of the proposed paper.

## II. REVIEW OF LITERATURE

A data-authenticator method for verifying the integrity of the data in the resource constraint context of IoT-based medical record system is proposed in the work of Ding et al. [1]. The model proposes using an edge server as a data authenticator in place of an IoT device, with an objective of cost-effective and independent of the third-party verifier. Blockchain technology is gaining popularity for designing suitable data integrity approaches for the resource constraint devices, as Alotaibi et al. [2] advocated. In the context of the Internet of Vehicles

(IoV), only and unique message integrity verification on edge-fog computing layer along with 2-factor authentication is present by Tsaour et al. [3]. The use of the hash chain-PKCS eliminates the use of the certificate that ensures low latency. Spatial query integrity is very sensible for many geospatial applications; a KNN based query message verification method is introduced by Jing et al. [4]. The Hadoop framework for the big data storage (HFBDS) in the cloud does not provide any security support system; Chattaraj et al. [5] proposes a fault-tolerant authentication protocol suitable for HFBDS. Data sharing (D.S.) is quite useful but challenging. Its security is taken care of by ring signature for authenticating data by the data owner itself using certificate and PKI. Still, it suffers data bottleneck while scalability that can be overcome by Identity-based ring signature (IBRS). The work of Huang et al. [6], Enhances the IBRS by provisioning forward security to make the system suitable for large scale D.S. In the context of VANET, the message authentication takes place by a joint operation of certificate and signature verification that cause privacy compromise concern. This delay-intensive process problem is studied by (Jiang et al. [7] and proposes an anonymous authentication to completely replace the certificate and signature verification by using the hash code of the message. Still, it limits the conditional security aspect of privacy. The cloud storage is essentially used for storing the spatial GPS data from the location-based applications. Strong authentication provides a vaccine for the possibility of compromising the integrity of the query. The work of Hu et al. [8] proposes a client-side query-result verification authentication model. The model uses a smaller object for the verification, so comparatively less computationally complex computationally, whereas it is not tested for scalability and lacks the auditing. The success of distributed and integrated service-oriented architecture (SOA) is the key mantra of today's web-based service in various domains of function application. Since the information moves out of the original content owner's control that requires a strong verifier for integrity. In this context, a cross-domain verifier is extensively used. Alam et al. [9] describe the cross-domain data authenticator, namely 'xDAuth' that fulfills the integrity and security protocols essentials. To overcome the effect of the denial of attack in geographical routing adopted in WSN, an opportunistic authentication scheme is proposed by Lyu et al. [10], where a cooperative verification process creates a partition between the regular and attacker nodes. An FPGA realization of the verification modules for the data integrity is carried out in Al-Asli et al. [11], which use a re-encryption scheme in a faster way for a huge data file. The content owner hosts their data to the cloud, which is being used by the subscribers. A robust and efficient auditing system requires performing the integrity check by minimizing error. Tian et al. [12] propose third-party management (TPP) light-weighted hash graph auditing method that handles the tradeoff between the security and the computational complexes [13]. Light-weighted secure deduplication for the cloud's data storage provides a balance between encryption and the storage cost by the third-party auditor [14]. The fingerprint of the accessing device and the human attributes are used in designing the verifier for the forensic stakeholder to access the cloud data [15]. To strengthen the third-party auditing system, Liu et al.,

the author in [16] proposed a computationally light-weighted scheme for formal analysis by fine-grain updates of the data. The computational cost for integrity verification is reduced by adopting a new data storing process [17]. Public auditing methods combining the authentication using a hash tree is proposed in the work of Liu et al. [18]. The auditing system for accounting the integrity shall be immune to the impersonation attack; one such work is proposed by Yuan et al. [19] For auditing the shared file integrity in a lower cost. Wang et al. [20] propose data dynamically using a hash tree for the block authentication with strong auditing support to the existing TPA authentication process. A mathematical model of a multi-party agent-based data integrity scheme is proposed by Wang et al. [21] use a multi-copy data process. Sun et al. [22] introduce a hash authentication for big data using the homomorphic scheme; in the work of Lu et al. [23], a remote data integrity scheme is proposed using the homomorphic authenticator with index verification for big data using big graph representation. Zhang et al. [24] proposes a method to balance the cost of storage with lightweight verification. The work carried out by Kavuri et al. [25], Anitha and Nair [26], Kumar & Shafi [27] have also emphasized data security. Apart from this, our prior work [28] [29] and [30] has also studied data integrity.

### III. RESEARCH PROBLEM

After reviewing all the work of existing data integrity approaches, the following research problems have been identified.

- The existing approaches towards data integrity don't consider the user's role much, which is one significant indicator of vulnerability within any form of network.
- The security is entertained in the form of user authentication and not much on data authentication, making it the server challenging to understand the legitimacy of the data.
- Adopting third parties is more to carry out secure data validation; however, it also affects the data's ownership by the cloud tenants.
- Majority of the existing approaches includes a highly sophisticated set of operation and is quite specific to the form of attack leading to vulnerable data integrity.

Therefore, the problem statement is as follows "Validating the legitimacy of the data over the vulnerable cloud environment and maintaining the highest degree of data ownership is quite challenging." The next section discusses the proposed solution.

### IV. RESEARCH METHODOLOGY

The design of a framework adopts an analytical modeling approach for data integrity to enhance the security level for data privacy. The proposed study's exceptional contribution is to offer a cost-effective solution to authenticate the communicating nodes in a cloud environment. Unlike the existing system, the proposed course emphasizes a more lightweight validation approach with no retention of stale information within the network. Hence, all possibility of any intermediate intrusion is avoided. It is quite challenging to

achieve synchronization between data integrity and data deduplication. The cloud storage system achieves an optimal balance between data privacy and storage bottleneck by deduplication. This tradeoff is made feasible using the divide. It conquers rule, so this framework mainly focuses on the auditing aspects of data integrity. Future research direction considers a joint implementation of more robust authentication, data integrity, and data duplication to provide a process protocol for the secure distributed cloud storage system. Therefore, this system model is a sub-framework for offering robust data integrity as a complement contribution to data privacy. The system model consists of three building blocks of the framework that includes: 1) Identity-based Registration and Authentication Block (RAB), 2) Cloud Data-Storage Service Dashboard (CDSSD), and 3) Access Cloud Auditing Management Dashboard (CAMD). This section discusses the modules and their respective design with algorithm implementation towards a research aim elaborately addressing the existing research problem.

#### A. Identity-based Registration and Authentication Block

The Registration and Authentication Block (RAB) provides access to both the stakeholders, namely, Cloud Tenant (CT) and the Cloud Auditor (CA). The CT allows two operations = {ct<sub>R</sub>, ct<sub>A</sub>}, where ct<sub>R</sub> is the registration process for the new C.T., and the ct<sub>A</sub> is the authentication process for the legitimate C.T. The ct<sub>R</sub> takes three attributes to complete the registration process. These attributes are the set (S<sub>ct<sub>R</sub></sub>) = {ct<sub>N</sub>, ct<sub>E</sub>, ct<sub>P</sub>} which gets updated into the RAB's registration database (auth-RAB). Whereas the ct<sub>A</sub> performs authentication of the legitimate C.T. by accepting and matching the value pair of ct<sub>E</sub> and ct<sub>P</sub> with the corresponding tuple: (ct<sub>E</sub>,ct<sub>P</sub>) stored in the auth-RAB-CT to gain access into the next block of operation of Cloud Data-Storage Service Dashboard (CDSSD). A closer look into this module shows that it offers a hierarchy of operations that is beneficial for the inclusion of maximum effort for attackers to have access, which will eventually lead to failure. The process flow of the RAB unit of the framework is shown in Fig. 1.

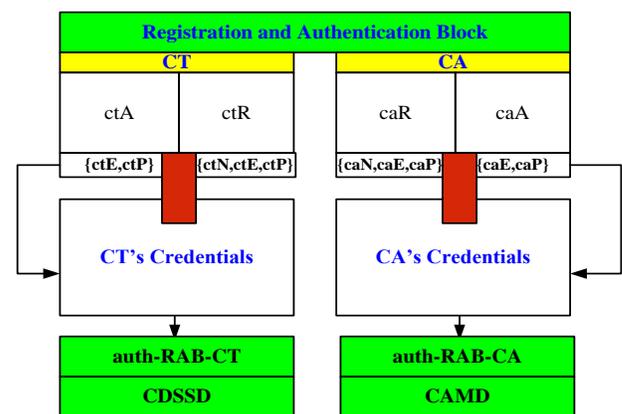


Fig. 1. Process flow of the RAB Block of Framework.

In Fig. 1, the process of registration and authentication of is shown for both cloud tenant and cloud auditor. The registration process takes place considering credential in form of name, email and password, which further gets updated into the identity based registration and authentication database. The

authentication process executes by taking and matching the value pair of credential provided at the time of registration and followed by corresponding tuple set to gain access to the cloud services.

**Algorithm 1.** Registration and Authentication Block

```

Input : ctN, ctE, ctP
Output: Auth
Start :
auth-RAB ← ctR(ctN, ctE, ctP)
  while Authentication:
    if ctR(ctE, ctP) == auth-RAB(tuple: ctE, ctP)
      Pass ← Auth
      Access → CDSSD
    else
      Suspect Dictionary attack ← Access
      Denied
  end
End.

```

In the same manner, the new C.A. performs registration by providing {ca<sub>N</sub>, ca<sub>E</sub>, ca<sub>P</sub>} credentials to 'car' and while authentication of C.A., by match process of the {ca<sub>E</sub>, ca<sub>P</sub>} with the *auth-RAB-CA* to gain access cloud auditing management dashboard (CAMD).

**B. Cloud Data-Storage Service Dashboard (CDSSD)**

This module acts as a bridge of communication between the system and the user. The term dashboard will refer to the user-friendly interface, which the stakeholder uses to store or access their contents over the cloud storage units. Unlike the existing approach, the proposed system offers flexibility to access the user's data and not system-defined, which provides more strength to ownership of data. The CT dashboard, namely: CDSSD, provides a handler to upload the C.T.'s data(ct<sub>D</sub>) to the cloud bucket storage (CB<sub>S</sub>) in an indexed manner as record-ID(r<sub>ID</sub>), and every upload of the ct<sub>D</sub> maintains a times-stamping instance(ctD-TS) is updated along with the respective ct<sub>D</sub> and r<sub>ID</sub>. The respective C.T. can view their records with the r<sub>ID</sub>. The simple presentation of the record upload and view is shown in Fig. 2.

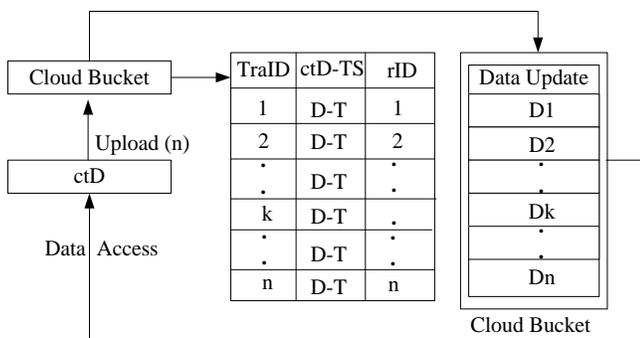


Fig. 2. Cloud Bucket Indexed Data.

The process algorithm is for the Cloud Tenant (CT), where the Data Transaction updates carried out to Master Meta-Data Record (MMDT) of c<sub>A</sub> is described in Algorithm2.

**Algorithm 2.** Cloud Tenant (C.T.) Data Transaction update to Master Meta-Data Record(MMDT) of c<sub>A</sub>

```

Input: ctE, ctP, CDSSD
Output:
Start :
∀ "i" ctD ∈ (CT)k ∈ { auth-RAB }
(TraID)i ← (ctData)i
(ctD-TS)i ← f-time(clock)
MMDT ← {TraID, ctD-TS, auth-RAB}kth
Challenges[cA] ← RPGF(cT-P1, cT-P2)
Update:
cA[SD] ← MMDT ∪ Challenges
End.

```

The CDSSD provisions a dashboard to all the registered Cloud Tenant. Whenever any registered and authenticated cloud users upload their data, the identity of the cloud tenant and the data records with timestamps gets updated into the Master Meta-Data Record (MMDT) matrix of c<sub>A</sub> shown in Fig. 3.

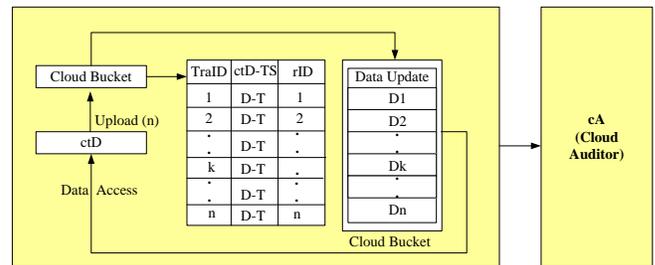


Fig. 3. Kth – cT Data Transaction update to Master Meta-data Record (MMDT) of c<sub>A</sub>.

To maintain a random seed for the data authentication, two initial seed: {cT-P1, cT-P2} gets generated by the random prime generator function (RPGF), in a very chaotic permutation of randomness, which goes as a challenge to the c<sub>A</sub> and the complete information of the transaction with the transaction I.D., timestamp and challenges (cT-Ch) gets updates for the commerce of data upload by the respective cT<sub>s</sub> as seeded data into the c<sub>A</sub> as cA[S.D].

**C. Cloud Auditor Data-Authentication Dashboard (CADAD)**

This module is called a cloud auditor, which is meant for performing authentication of the data. This module cross-checks the basic legitimacy of the data. Unlike any existing method, the proposed system harnesses the potential of hashing-based methods to incorporate data security. The novelty of this mechanism is to ensure data integrity and privacy at the same time. The CADAD maintains the updates of the ∀ cT with details of {ct<sub>E</sub>} and gains access to the number of transactions made by the (cT)<sub>k</sub> from cA[S.D.]. For each record, the c<sub>A</sub> generates a challenge message (Ch<sub>msg</sub>) with the ctD-TS and cT-Ch using an SHA-256 hashing

algorithm. The algorithm for this process is given in Algorithm 3.

**Algorithm 3.** Data integrity flag using  $c_A$  and CPS hashed challenge

**Input:**  $ct_E, c_A[SD]$ .

**Output:** DIF

*Start:*

for  $\forall c_A[SD]$ , Generate,  
 $Ch_{msg} \leftarrow hash\text{-function}(ct_E, c_A[SD])$   
 $Ch_{csp} \leftarrow Hash\text{-function}(ca_E, c_A[SD])$   
*end*

Data Integrity flag  $\leftarrow [Ch_{msg} \sim Ch_{csp}]$

*End.*

The  $c_A$ 's  $\{Ch_{msg}\}$  and another corresponding challenge message from the CSP as  $\{Ch_{csp}\}$  is used for verifying the proof of authenticity with all the credential matches between the  $c_T$ ,  $c_A$ , and the CSP with the  $c_T$ 's identity, in-charge auditor, timestamp of data records, data identification number, respective challenges from the  $c_A$  and the CPS. Based on mutual verification between  $[Ch_{msg} \sim Ch_{csp}]$ , each data upload gets a Data Integrity flag (DIF) as verified or not verified.

### V. RESULTS AND DISCUSSIONS

To perform an assessment, the proposed system constructs a test-bed where there are 50 accesses given for cloud auditors and 100 accesses provided for cloud tenants. The proposed method's implementation is carried out using MATLAB, where the idea is to testify the effectiveness of the proposed algorithm concerning defined performance parameters. The system model maintains and auditing ledgers for non-repudiation. Fig. 4 illustrates the traffic of cloud device access and data authenticator at any time,  $\Delta t$ .

Table I and Fig. 4 above show the traffic count of cloud device access to the data panel either for uploading new data or accessing the uploaded data and delivering the frequency count of access to the security panel of the data authenticator model. From Fig. 4, it can be seen that the analysis is carried out on test sample values of 3 and 6 frequency count of access for cloudlet device and data authenticator showing that data authenticator is capable of validating double the number of the cloud tenants.

Fig. 5 exhibits the analysis of data volume per cloud let devices followed by quantified observation in Table II. The graph trend it can be analyzed that each cloudlet device can hold different volumes of data.

Fig. 6 and Table III exhibits analysis concerning verification count per Data-Authenticator. The analysis from graph trend shows that the data authenticator can validate multiple scores and volumes of data.

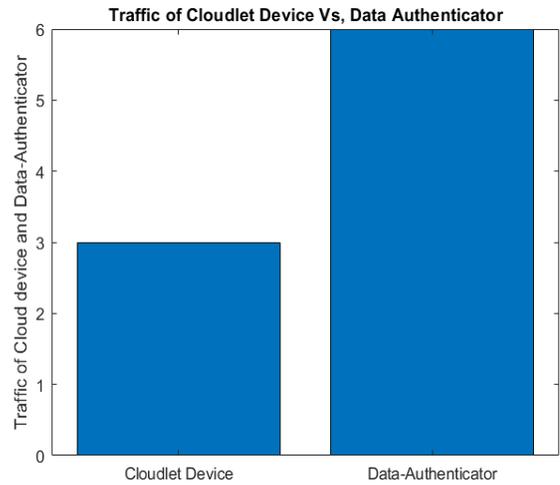


Fig. 4. Analysis of Traffic.

TABLE I. NUMERICAL OUTCOMES OF ACCESS COUNTS

Traffic type (Stakeholders)	Frequency count of access
Cloudlet Device	3
Data-Authenticator	6

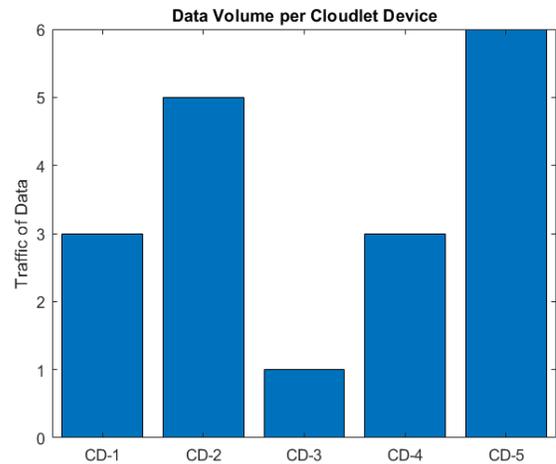


Fig. 5. Analysis of Data Volume.

TABLE II. NUMERICAL COUNT OF DATA VOLUME

Cloud Device	Traffic of Data
CD-1	3
CD-2	5
CD-3	1
CD-4	3
CD-5	6

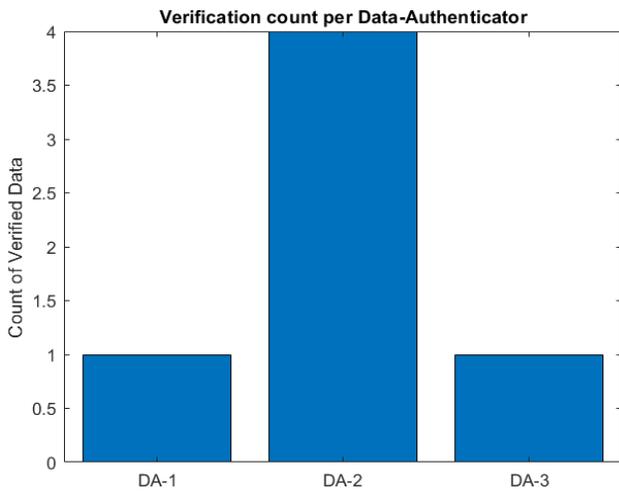


Fig. 6. Analysis of Verification Count.

TABLE III. NUMERICAL OUTCOME OF COUNT OF VERIFIED DATA

Data Authenticator	Count of Verified Data
DA-1	1
DA-2	4
DA-3	1

Fig. 7 highlights that the proposed system offers better performance in contrast to the existing authentication system. Although, with an increase in the number of entities, the verification delay increases, which is expected, the proposed method exhibits considerably less duration for verification as compared to the existing system. The prime reason behind the proposed system getting better performance is that a simplified hashing-based authentication mechanism is designed which performs a faster assessment without much depending on computational resources dependency or storage demands unlike any existing protocols (shown in Table IV). The conventional technique is associated with complex operation involves a recursive operation in its implementation design and requires large storage space.

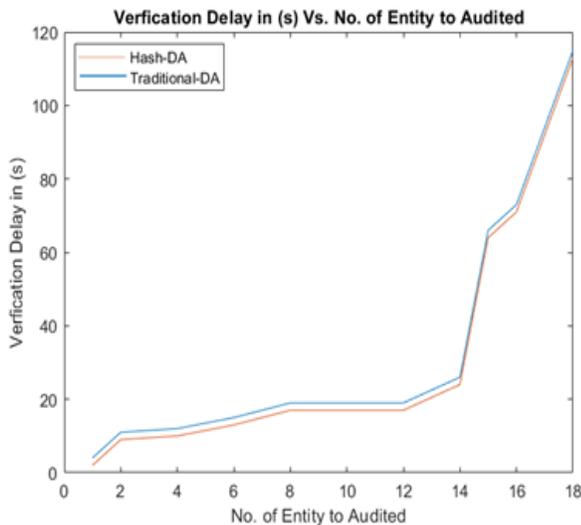


Fig. 7. Analysis of Verification Delay.

TABLE IV. NUMERICAL OUTCOMES OF VERIFICATION DELAY

No of Entity to be Audited	Verification Delay (Hash-DA)	Verification Delay (Traditional-DA)
1	4	2
2	11	9
4	12	10
6	15	13
8	19	17
10	19	17
12	19	17
14	26	24
15	66	64
16	73	71
18	115	113

## VI. CONCLUSION

The continuous adaptation of the cloud eco-system for data storage, even for critical applications, raises the robust and efficient data authenticator design for data integrity verification. This paper introduces an analytical framework for a scheme for cross-verifiable hash-based challenges matching scheme for assign a flag of data integrity verified by the data authenticator with the provision of the non-repudiation of the tractions using the inclusion of a cloud auditor units. The performance metric justifies its scalability for the data traffic volume, several devices connected to the cloud for the data upload, and the verification delay lower and consistent. The scheme can be fine-tuned for the adoption in the real cloud scenario for non-repudiated auditing for the data integrity verification by the authenticator. The contribution of this manuscript are: i) a simplified hashing-based authentication mechanism is constructed which performs a faster assessment, ii) The authentication is performed for both the user as well as data for any target nodes, iii) the proposed system offers almost nil key dependency or storage demands unlike any existing protocols, iv) higher scope of resiliency is incorporated which provides security without having any dependencies of any apriori information of attacker or network. In the future, the system can be extended to synchronize within data confidentiality issues while data deduplication in the cloud storage system. The study intend to adopted lightweight design of encryption technique for data security and hashing mechanism for integrity verification.

## REFERENCES

- [1] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight Privacy-Preserving Identity-Based Verifiable IoT-Based Health Storage System," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8393-8405, Oct. 2019, doi: 10.1109/IJOT.2019.2917546.
- [2] B. Alotaibi, "Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review," in *IEEE Sensors Journal*, vol. 19, no. 23, pp. 10953-10971, 1 December 1, 2019. doi: 10.1109/JSEN.2019.2935035.
- [3] W. Tsaur and L. Yeh, "DANS: A Secure and Efficient Driver-Abnormal Notification Scheme with IoT Devices Over IoV," in *IEEE Systems Journal*, vol. 13, no. 2, pp. 1628-1639, June 2019.
- [4] D. Chattaraj, M. Sarma, A. K. Das, N. Kumar, J. J. P. C. Rodrigues and Y. Park, "HEAP: An Efficient and Fault-Tolerant Authentication and

- Key Exchange Protocol for Hadoop-Assisted Big Data Platform," in *IEEE Access*, vol. 6, pp. 75342-75382, 2018.
- [5] X. Huang et al., "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," in *IEEE Transactions on Computers*, vol. 64, no. 4, pp. 971-983, 1 April 2015. doi: 10.1109/TC.2014.2315619.
- [6] S. Jiang, X. Zhu and L. Wang, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193-2204, Aug. 2016. doi: 10.1109/TITS.2016.2517603.
- [7] L. Hu, W. Ku, S. Bakiras and C. Shahabi, "Spatial Query Integrity with Voronoi Neighbors," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 4, pp. 863-876, April 2013. doi: 10.1109/TKDE.2011.267.
- [8] Q. Alam et al., "Formal Verification of the xDAuth Protocol," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1956-1969, Sept. 2016. doi: 10.1109/TIFS.2016.2561909.
- [9] C. Lyu, X. Zhang, Z. Liu, and C. Chi, "Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks," in *IEEE Access*, vol. 7, pp. 31068-31082, 2019. doi: 10.1109/ACCESS.2019.2902843.
- [10] Y. Jing, L. Hu, W. Ku, and C. Shahabi, "Authentication of k Nearest Neighbor Query on Road Networks," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 6, pp. 1494-1506, June 2014. doi: 10.1109/TKDE.2013.174.
- [11] M. Al-Asli, M. E. S. Elrabaa, and M. Abu-Amara, "FPGA-Based Symmetric Re-Encryption Scheme to Secure Data Processing for cloud-integrated Internet of Things," in *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 446-457, Feb. 2019. doi: 10.1109/JIOT.2018.2864513.
- [12] B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu, and T. Qiu, "An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing," in *IEEE Access*, vol. 4, pp. 7899-7911, 2016. doi: 10.1109/ACCESS.2016.2621005.
- [13] J. Tian and X. Jing, "A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage," in *IEEE Access*, vol. 7, pp. 68071-68082, 2019. doi: 10.1109/ACCESS.2019.2916889.
- [14] J. Wu, Y. Li, T. Wang, and Y. Ding, "CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing," in *IEEE Access*, vol. 7, pp. 160482-160497, 2019. doi: 10.1109/ACCESS.2019.2950750.
- [15] A. Liu, H. Fu, Y. Hong, J. Liu, and Y. Li, "\$LiveForen\$ : Ensuring Live Forensic Integrity in the Cloud," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2749-2764, Oct. 2019. doi: 10.1109/TIFS.2019.2898841.
- [16] C. Liu et al., "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2234-2244, Sept. 2014. doi: 10.1109/TPDS.2013.191.
- [17] J. Li, X. Tan, X. Chen, D. S. Wong, and F. Xhafa, "OPoR: Enabling Proof of Retrievability in Cloud Computing with Resource-Constrained Devices," in *IEEE Transactions on Cloud Computing*, vol. 3, no. 2, pp. 195-205, 1 April-June 2015. doi: 10.1109/TCC.2014.2366148.
- [18] C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, and J. Chen, "MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud," in *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2609-2622, 1 September 2015. doi: 10.1109/TC.2014.2375190.
- [19] J. Yuan and S. Yu, "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1717-1726, Aug. 2015. doi: 10.1109/TIFS.2015.2423264.
- [20] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011. doi: 10.1109/TPDS.2010.183.
- [21] C. Wang and X. Di, "Research on Integrity Check Method of Cloud Storage Multi-Copy Data Based on Multi-Agent," in *IEEE Access*, vol. 8, pp. 17170-17178, 2020. doi: 10.1109/ACCESS.2020.2966803.
- [22] Y. Sun, Q. Liu, X. Chen and X. Du, "An Adaptive Authenticated Data Structure With Privacy-Preserving for Big Data Stream in Cloud," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3295-3310, 2020. doi: 10.1109/TIFS.2020.2986879.
- [23] Y. Lu and F. Hu, "Secure Dynamic Big Graph Data: Scalable, Low-Cost Remote Data Integrity Checking," in *IEEE Access*, vol. 7, pp. 12888-12900, 2019. doi: 10.1109/ACCESS.2019.2892442.
- [24] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient Public Verification of Data Integrity for Cloud Storage Systems from Indistinguishability Obfuscation," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 676-688, March 2017. doi: 10.1109/TIFS.2016.2631951.
- [25] Sathesh K S V A Kavuri, Gangadhara Rao Kancherla, Basaveswararao Bobba, "An Improved Integrated Hash and Attributed based Encryption Model on High Dimensional Data in Cloud Environment," *International Journal of Electrical and Computer Engineering*, Vol.7, No.2, 2017.
- [26] Anitha K L, T.R. Gopalakrishnan Nair, "Data storage lock algorithm with cryptographic techniques," *International Journal of Electrical and Computer Engineering*, Vol.9, No.5, 2019.
- [27] Y. Kiran Kumar, R. Mahammad Shafi, "An efficient and secure data storage in cloud computing using modified RSA public-key cryptosystem," *International Journal of Electrical and Computer Engineering*, Vol.10, No.1, 2020.
- [28] Anil Kumar G and A.S.Poornima, "A Survey on Data Integrity Methods in Cloud Storage," *EJERS, European Journal of Engineering Research and Science*, Vol. 1, No. 5, November 2016.
- [29] Anil Kumar G., Shantala C. P., "An extensive research survey on data integrity and deduplication towards privacy in cloud storage," *International Journal of Electrical and Computer Engineering (IJECE)* Vol. 10, No. 2, April 2020, pp. 2007~2018.
- [30] Anil Kumar G., Shantala C. P., "Framework towards Higher Data Privacy by Novel Data Integrity Scheme," *1st International Conference on Innovation in Computer Science, Electrical and Electronics Engineering (ICICEE)*, 2020.

#### AUTHORS' PROFILE



Mr. Anil Kumar G is a Research Scholar in the Computer Science and Engineering department of Channabasaveshwara Institute of Technology at Visvesvarahya Technological University. He perused his bachelor's degree in Computer Science & Engineering from Gulbarga University, Karnataka, India, and masters in Computer Science & Engineering from Dr. MGR Educational Research Institute, Chennai, India. Mr. Anil Kumar has good academic and research experience in Computer Networks, Unix Systems Programming, Cloud Computing with many publications.



Dr. Shantala C P is Professor & HOD in the Computer Science and Engineering department of Channabasaveshwara Institute of Technology at Visvesvaraya Technological University. She is vice-principal of Channabasaveshwara Institute of Technology. She has completed her Ph.D. in the area of Data Security and Masters in Computer Science & Engineering. Her research interests lie in Network & Data Security, Cloud Storage, Data Mining & Brain-Computer Interface. Her research works brought her various awards like Seed Money for Young Scientist from VGST & Women Achiever Award from IEEE.

# Cybersecurity Awareness Level: The Case of Saudi Arabia University Students

Wejdan Aljohani<sup>1</sup>, Nazar Elfadil<sup>2</sup>, Mutsam Jarajreh<sup>3</sup>

Computer Engineering Department  
Fahad Bin Sultan University  
Tabuk, Saudi Arabia

Mwahib Gasmelsied<sup>4</sup>

Finance and Investment Department  
University of Tabuk  
Tabuk, Saudi Arabia

**Abstract**—Cybersecurity plays an important role in reliance on digital equipment and programs to manage daily lives chores including the transmission and storage of personal information. Therefore, it is a global issue in our growing society, and it becomes increasingly important to measure and analyze the awareness of it. In this paper, a questionnaire has been designed to measure the current level of cybersecurity awareness (CSA) among Saudi university students. Cybersecurity students' awareness level questionnaire has been adapted from few other previous cybersecurity awareness campaigns. In this questionnaire, a total of 136 students have participated in the survey. The questionnaire was collected to measure the cybersecurity students' awareness level through their knowledge, culture, and surrounding environment or through students' behavior by three affected factors. These are: gender, location, and study department of the students. The study findings reveal that the students' awareness is in an average has no significant difference in cybersecurity awareness level between male and female students, but females show a bit more concern about cybersecurity. However, there is a clear and high awareness of students of computer and information technology departments compared to others. Moreover, urban students outperformed students in remote areas in awareness of cybersecurity. The survey results indicate that the study model has been effective in measuring students' awareness.

**Keywords**—Cybersecurity; awareness; protection; internet; students; higher education; security awareness; survey; APAT

## I. INTRODUCTION

The huge technological revolution in every aspect of our everyday life, such as smart devices, smart homes, and smart cities, cybersecurity has become an important component of any information system as it includes all elements of computer/network security that secure devices from unauthorized access, changes and destruction of information systems [1]. Cybersecurity vulnerabilities are the elements that put a system or network at risk of being infected with malicious software. When one recognizes that a system was influenced by an assault, this illustrated that an assault on the framework occurred and being effective. This can be assumed that the system was powerless against the assault, then the expression vulnerability can be used to refer to the peculiarities or features of the framework that causes it defenseless and helpless against all assaults [2]. Malwares are shown all over internet services to influence devices daily and carry out assaults that render devices, networks and data vulnerable. Osterman's research survey discovered that eleven million

malware differences were detected by 2008 and ninety percent of the malware derived from concealed downloads from trusted and prominent sites.

Network security is a huge referent question, yet its political significance emerges from associations with the aggregate referent articles of "The State", "The Society", "The Nation" and "The Economy" [3].

### A. Statement of the Problem

IT represents all the technology available from hardware, software, and all applied techniques such as communication. IT risks can be classified into three main types; they are operational risks, security risks, and risks from the organization and people living within it. With the increase in the spread and use of the internet, those risks have increased [4]. In security risks, the computer infrastructures components may predispose a device at a risk, they include software, hardware, and network. Securing these three elements or components implies accountability that is utilized to detect malicious elements and a perimeter defense system. This system is used to defend and resist the breach of infrastructure by malicious elements. It has also an access control mechanism that is used for authorization of incoming/outgoing data.

On the other hand, college students are the most groups that use a network, and they are supposed to be the most aware group of cybersecurity, also cybersecurity awareness culture should be established at an early stage [5]. University students are on this stage which is edge to enter the workforce. There is a great variety in the quality, capacity, importance, and nature of the students' data, but no one denies the importance of preserving them and not changing, falsifying, or distorting them, and preserving data even exceeds to include their formats and arrangement. It is a very sensitive nature, and any slight change may cause many problems to the users. IT systems, cyber networks need special treatment as they contain numerous data for students; they should be maintained and kept confidential, otherwise they will be exposed to many threats. All universities need to secure their students data, avoid risks, and avoid all potential associated effects or at least minimize the effects of these risks [6]. The unawareness of students about threats and risks that can face them in cyberspace, can cause successful execution of such threats. Students should establish a culture of cybersecurity awareness before entering the workforce. One of the most important steps in this way is measuring the cybersecurity awareness of university students.

### B. Research Objectives

The end user is seen as a weak link [7]. Therefore, if students are not aware enough to recognize a security threat, they cannot be expected to avoid it, report it or remove it. Students are on the edge to enter the workforce, should be prepared and aware of security risks to avoid being a victim of cybercrime. They need cybersecurity awareness. The aim of this study is to evaluate the level of information security awareness among KSA university students. Online security is important to any society because it is part of the world which is viewed as a global village. Thus, it must be at the beginning of every educational system to secure the safety within cyber environments.

### C. Research Questions

Identifying the research questions is the first step that must be concise and clear. In the context of this study, the research questions are stated as follows:

- RQ1. How much do KSA university students know about information security?
- RQ2. Is there an impact of gender, study department, or residential area on awareness levels?

This paper is organized in 5 sections. An introductory was clearly elaborated in section 1. While section 2 contained the related work. The research method discussed in section 3. The survey result findings were thoroughly discussed in section 4. The review concludes by discussing research limitations and conclusion.

## II. RELATED WORKS

A log analyst needs good cyber situation awareness to perceive malicious activity, comprehend the impact and type of threat, and predict future consequences. The paper of [8] describes the development and validation technique to measure log analysts' situation awareness, especially when it comes to practical examples. The validation was conducted in a realistic setting by forming two questionnaires designed for the two different roles in log analysis and during an exercise involving five professionals. The results suggest that the technique can be used to evaluate cyber situation awareness for log analysts to keep track of incidents. To address the same issue, a framework was proposed [9] to help network analysts to evaluate the security situation of the network and increase their awareness from three dimensions: threat, vulnerability, and stability, and merge the results at decision level to measure the security situation of the overall network.

In [10], the security awareness of data in the Middle East area, especially in educational environments such as undergraduate students, researchers, academic staff, and employees has been studied to analyze and identify the awareness level of IS in this environment. The results revealed that there is a clear lack of knowledge of IS principles, the participants do their daily work and practical application without the requisite knowledge and understanding of the importance of IS basics. The researchers were interested in investigating the impacts associated with security risks and the lack of the security awareness in the institutions. The paper set several recommendations to reduce the harms of this situation,

the important one of these recommendations was through supporting the training and awareness programs as well as adopting all the necessary safety measures by academicians and employees of the institution to enhance the security and safety of their data. Other studies [11-13] focused on the analyzing and raising the awareness of cybersecurity on college students. Researchers [14] attempted to measure the level of cybersecurity parental awareness to protect their children. A quantitative data analysis was performed using statistical software.

In [2], employees are the most vulnerable links, they need cybersecurity awareness and training to protect themselves and the company against new evolving cyber-attacks. An (Analyze-Predict-Aware-Test) APAT based Model along with Algebraic Equation has been adopted in developing a proactive approach towards enhancing the cybersecurity by making employees aware of new forms of security threats and what measures to follow when a suspicious activity is identified. Other research [15, and 16] developed and validated a model which assists in reducing big data security and privacy risk caused by employee weakness.

In the research paper [17], the researchers investigated the cybersecurity awareness of the public people in Saudi Arabia. The investigation was based on various aspects and contexts including demographics, cybercrime awareness, cybersecurity practices, and incident reporting as well as, a quantitative online survey was used to collect information related to cybersecurity awareness among Saudi nationals. The results revealed that the Saudi citizens had a good knowledge of IT, but they have limited awareness of the threats associated with cybersecurity practices, cybercrime, and the organizations and government roles in guarantee information safety across the Internet. Additionally, Internet skills influence cybersecurity practices from the end users. The study recommended to develop a model to create cybersecurity awareness in the region to reduce cybercrime.

In the same field and in the Middle East region and in a different country other than Saudi Arabia, Fadi [3] discussed the need for security education, training, and awareness programs in United Arab Emirates. The study involved and focused on the chances of the fall victims to phishing, a comprehensive wireless security survey of access points in Dubai and Sharjah and the Radio-frequency identification (RFID) security awareness. These determinants and aspects have been studied and discussed in Emirati schools, universities, and private and government organizations. Many counter measures that enhance the security awareness among students and professionals in UAE were reported. Recently, a study conducted by Moti [18] was carried out in four countries Palestine, Slovenia, Poland, and Turkey. The aim was to investigate cybersecurity awareness, beyond the differences of the respondent's country or gender.

Many researchers, such as Ashish [19, and 20] set models to measure accurately cybersecurity awareness and enhance the level of effective information security measures taken against all types of attacks. These models defined awareness as a problem not a solution, to solve this problem, one must be able to measure it and promote the awareness level according to the

measurements. Dynamic model is superior to other models set by the researchers [5, and 21] because it was designed in a stepped structure with leveling standardization, applicable to all groups/levels and capability-based approach used. After displaying most of our research-related ideas, the researcher of the current study can conclude that there is a lack of addressing some of the concepts that authors must deal with in measuring and analyzing the cybersecurity awareness of university students in KSA, such as effects of gender, study department and residential area as affected factors in awareness level of cybersecurity; also, awareness analysis and measurements through knowledge, culture and surrounding environment or through student behavior.

Authors studied in-depth survey about the awareness of cybercrime amongst the people of Bangladesh [21-23]. The survey has been carried out through responses both the online and offline questionnaires. Statistical Package for the Social Sciences (SPSS) software was accompanied for detailed analysis. Based on this study, the results shown negative results about people which were unaware of standard practices for cybersecurity and the government which was not vibrant regarding cybercrime related issues.

The information warfare and security awareness grabbed a high research attention recently and will be the on the research scope of many information security researchers in future [21, 24], and, thus of significance of this work.

### III. RESEARCH METHODOLOGY

A survey is formed and carried out to gather data of evaluating students' awareness about cybersecurity threats. The target subjects of the survey are KSA universities students, students need to be educated about security issues early, the earlier they are aware of Information Security vulnerabilities, the safer they will be in the future as they will be able to pay more attention to security matters and avoid engaging in illegal behavior. The location, gender, and department are all the possible variables that may affect the security awareness level of the students. Therefore, the sample who answer the questionnaire should be students from different departments and from different areas in KSA. The data of the students' responses will be used to determine how students are aware of the information security threats. To achieve this goal, this study uses of the research methods.

#### A. Research Design

This research used the descriptive and quantitative method of gathering data to offer a clear view of the security awareness level of the universities students and it guarantees the validity and reliability of the research. In the quantitative design, the descriptive statistics are used to indicate the scores' distribution using a few indices. Structured of the questionnaire was distributed manually. These methods are preferred because they are fast, suitable, and economic for each questionnaire. The main steps can be listed as follows: (1) Students from different Universities, gender, location, and departments were asked to take part of this survey, (2) Students were evaluated based on their responses, (3) Survey is carried out voluntarily and randomly, (4) The questionnaire required approximately

10 to 15 minutes to be completed, and (5) Survey was distributed in a period of 2 months.

#### B. Data Sources

Two sources of data collection were used in this study, the first is primary data sources which is the data were collected by developing a structured questionnaire to study, analyze and discuss Saudi university students' awareness of cybersecurity and their affected factors. In the questionnaire, 136 completed samples were collected, and the second is secondary data which is the data that were collected from websites, previous scientific research, books, journals, articles, and thesis. The main objective of collecting these data is to design a suitable, structured questionnaire that accommodates all aspects of the university students' awareness of cybersecurity.

#### C. Questionnaire Analysis

The research depended on the structured questionnaire as the main tool for data collection, which was distributed on the research's sample to fill the required information. In the questionnaire, there are 24 questions in the Survey. This questionnaire includes two directions, they are:

- Awareness through knowledge, culture, and surrounding environment, which covered by 11 closed questions.
- Awareness through student behavior, which covered by 13 closed questions.

The answers to all the questions were closed, cast in the positive direction for each direction and designed on 4 score Likert Scale from 1 to 4 values as follows: (a) Strongly Disagree= 1, (b) Disagree =2, (c) Agree= 3, and (d) Strongly Agree= 4. After the collection of questionnaires from respondents, the data were entered into the computer and processed by using the Statistical Package for the Social Sciences (SPSS V.20). SPSS is a widely used program for statistical analysis in social science. It is also used by market researchers, health researchers, survey companies, government, education researchers, marketing organizations, data miners, and others.

### IV. SURVEY RESULTS AND ANALYSIS

In this study, the data from the questionnaire answered by the Saudi universities' students are used to determine how students are aware of information security threats. This chapter presents the statistical results which were collected from the questionnaire responses. Data were analyzed using SPSS to compute various statistics. The responses were collected and recorded on tables to compute the frequencies and percentages of each question. Authors selected descriptive statistic as analytical approach for analyzing the collected data from the questionnaire.

#### A. Quantitative and Descriptive Analysis

The questionnaire was distributed, which includes two directions, they are: 1) Awareness through knowledge, culture, and surrounding environment (covered by 11 closed questions) and 2) Awareness through student behavior (covered by 13 closed questions). There are two influencing factors that were

considered; namely: (a) student gender, (b) student department or learning background.

Nevertheless, 136 samples were collected; Table I and Fig. 1 show the details. The answers to all the questions were closed and cast in the positive direction for each direction. The Likart scale was used for their analysis, Table II collected the answer to questions and the answers were as follows.

SPSS is used to extract the quantitative and descriptive analysis of these results. The arithmetic mean clearly indicates the trend in answering each question. Of course, mean values indicate the tendency of the respondents to the questionnaire to one of the four answers, and this is evident by the appearance of the top (Maximum) of the bell curve at or near a specific value. The thinner and higher the curve, the greater the conformity of the participants' opinion towards a specific answer. Where, the standard deviation is a measure of the amount of variation or dispersion of a set of values. A low standard deviation indicates that the values tend to be close to the mean (also called the expected value) of the set, while a high standard deviation indicates that the values are spread out over a wider range.

**B. Effects of Factors and Directions**

To analysis the effects of factors and directions authors use the following procedures:

- Authors set three hypothesis that have determinant factors, they are Gender, Location and department, but the expectation that department will have high, direct and clear effects so, authors will investigate the effects of the department as in dependent factor, where location and gender as dependents together with department.
- The Stem-and-leaf plots are used which it is a method for showing the frequency with which certain classes of values occur. Also, plots window will fulfill this purpose; there are three different display options for boxplots: Factor levels together, Dependents together, and none. The Factor levels together and Dependents together settings only affect analyses with two or more numeric variables.
- Calculate the Pearson Correlation, is a statistic that measures linear correlation between two variables it's suitable to measure of the strength of a linear association between our two directions.

The windows or boxplot appearing in the form of the stem-and-leaf plots each of them show how many participants are associated with one of the factors in the answers, and indicate the distribution or concentration of the values of their answers in each question, and through that, it is possible to know the effect of the parameter in each question.

**C. Answering Research Questions**

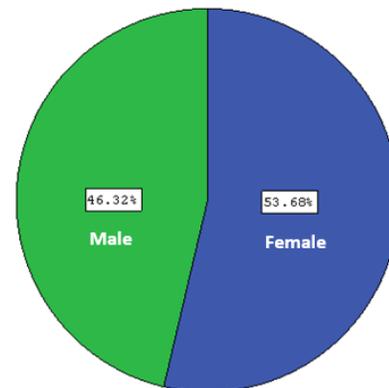
This section summarizes and discusses the answers to the research questions.

RQ1. How much do KSA students know about information security? The analysis of the collected questionnaires showed that students' awareness of urban cities about cybercrime

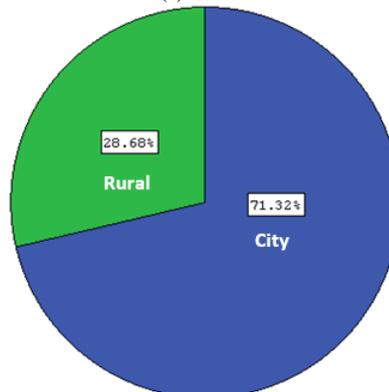
greater than remote areas and the countryside (rural), of course, due to the availability of modern technologies.

TABLE I. FREQUENCY SAMPLES

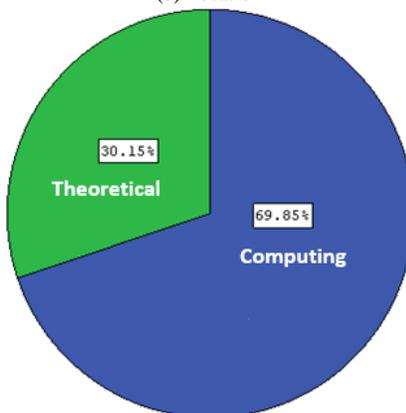
Location		Department			Gender			
Percent	Frequency	Percent	Frequency	Percent	Frequency	Gender		
71.3	97	City	69.9	95	Computer	53.7	73	Female
28.7	39	Rural	30.1	41	Theory	46.3	63	male
100.0	136	Total	100.0	136	Total	100.0	136	Total



(a) Gender.



(b) Location



(c) Department.

Fig. 1. Pie Chart of Samples, a) Gender, b) Location, and c) Department.

TABLE II. THE ANSWER OF SURVEY'S QUESTIONS

value	1		2		3		4	
	samples							
	%		%		%		%	
Q1	5.1	7	8.1	11	14.0	19	72.8	99
Q2	0	0	2.2	3	16.2	22	81.6	111
Q3	.7	1			2.9	4	96.3	131
Q4			4.4	6	5.1	7	90.4	123
Q5	2.9	4	6.6	9	13.2	18	77.2	105
Q6					.7	1	99.3	135
Q7							100.0	136
Q8	1.5	2	8.8	12	16.2	22	73.5	100
Q9	2.9	4	10.3	14	12.5	17	74.3	101
Q10	8.1	11	17.6	24	50.0	68	24.3	33
Q11	8.1	11	22.8	31	64.0	87	5.1	7
Q12			.7	1	20.6	28	78.7	107
Q13							100.0	136
Q14			5.1	7	66.2	90	28.7	39
Q15			80.1	109	9.6	13	10.3	14
Q16			27.2	37	4.4	6	68.4	93
Q17	3.7	5	22.8	31	16.9	23	56.6	77
Q18							100.0	136
Q19	3.7	5	12.5	17	32.4	44	51.5	70
Q20	11.0	15	11.8	16	59.6	81	17.6	24
Q21	30.9	42	61.8	84	3.7	5	3.7	5
Q22	9.6	13	51.5	70	21.3	29	17.6	24
Q23	41.2	56	31.6	43	16.2	22	11.0	15
Q24	13.2	18	35.3	48	27.2	37	24.3	33

RQ2. Is there an impact of gender, study department, or residential area on awareness levels? The female participated are more exclusive and more knowledgeable about cybercrime, and at the same time the knowledge of the computer department's affiliates increased on the theoretical departments. But, there is no clear effect of the relationship of the department with gender from the provided answers.

Nevertheless, both genders were fully agreed that increasing training will increase awareness, and the students of the computer department are more aware of the importance of training in increasing cyber.

It is worth to mention that Gender, Location, and Department have significant effects of the two (culture and behavior) direction. Students of the computer department are the most fortunate and the most knowledgeable, aware, and safe of cybercrime risks.

Finally, the Pearson correlation coefficient can take a range of values from +1 to -1. A value of 0 indicates that there is no association between the two variables. A value greater than 0 indicates a positive association; that is, as the value of one variable increases, so does the value of the other variable. A

value less than 0 indicates a negative association; that is, as the value of one variable increases, the value of the other variable decreases. From SPSS the entering data give Pearson correlation coefficient between our two directions as +0.411, this mean the relation is Positive with medium strength of association.

## V. CONCLUSION

The objective of this research study was to measure students' cybersecurity awareness level. The study elaborates on the literature related to cybersecurity awareness among university students. For this purpose, a questionnaire was developed. The proposed questionnaire focused on students' awareness as part of the information security concepts and intended to measure cybersecurity awareness level. Nevertheless, study findings indicate that students have had average levels of awareness regarding cybersecurity concepts. It is worth mentioning that students' awareness levels did not differ significantly in terms of gender, and student's class level, but female showed bit more concern about cybersecurity. However, there is a clear and high awareness of students of computer and information technology departments. This study recommends necessary policy measures to be taken by universities to ensure that students from all places have same level of cybersecurity awareness. The results show that urban students outperformed students in remote areas in awareness of cybersecurity.

Cybersecurity awareness is normally neglected by educational institutes. University students should be aware of the possible threats that can face them while using the internet. Therefore, a culture of awareness must be established for students to be able to identify possible threats. This culture should be establishing from an early stage. Furthermore, students should be well prepared and aware of security measures that users can apply to avoid being a victim of cybercrime.

## REFERENCES

- [1] N.Thakur and C. Y. Han, "An Ambient Intelligence-Based Human Behavior Monitoring Framework for Ubiquitous Environments," MDPI Information, vol.12,no.2,pp.81-107, Feb.2021.
- [2] A.H.khan, P.Sawhney, S.Das, D.Pandey, "SartCybersecurity Awareness Measurement Model (APAT)," International Conference on Power Electronics &IoT Applications in Renewable Energy and its Control (PARC), February 2020. <https://doi.org/10.1109/PARC49193.2020.236614>.
- [3] M. O'Connell " Cybersecurity without Cyberwar," Journal of Conflict and Security Law, vol. 17, pp.187-209, 2017.
- [4] J. H.Pardue, P.Patidar, "Threats to Healthcare Data: A Threat Tree for Risk Assessment," Issues in Information Systems, vol XII, No. 1, pp. 106-113, 2011.
- [5] S.E.Erol, S.Sagioglu, "Awareness Qualification Level Measurement Model, " International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Dec. 2018.
- [6] M.Jaber, M.Dhaini, A.Fakherdine, and R.A. Haraty, "A Novel Privacy-Preserving Healthcare Information Sharing Platform Using Blockchain," Security and Privacy Issues in IoT Devices and Sensor Networks. Advances in ubiquitous sensing applications for healthcare, pp.245-261. Elsevier, 2021.
- [7] Thomason, "People -The Weak Link in Security," Global Journal of Computer Science and Technology Network, Web & Security, vol.13, Issue 11, 2013.

- [8] P.Lif, M.Granasen, T.Sommestad, "Development and validation of technique to measure cyber situational awareness," International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pp.367-379, June 2017.
- [9] X.Rongrong, Y.Xiaochun, H.Zhiyu, "Framework for risk assessment in cyber situational awareness," IET Information Security, vol. 13, Issue. 2, 2019.
- [10] S.Al-Janabi, I.Al-Shourbaji, "A Study of Cybersecurity Awareness in Educational Environment in the Middle East," Journal of Information & Knowledge Management, vol. 15, No. 1, 2016.
- [11] E. B. Kim, "Information Security Awareness Status of Business College: Undergraduate Students," Information Security Journal: A Global Perspective, vol.22, pp. 529-551, 2013.
- [12] M. O'Connell " Cybersecurity without Cyberwar," Journal of Conflict and Security Law, vol. 17, pp.187-209, 2017.
- [13] Y.K.Peker, L.Ray, S.D.Silva, N.Gibson, C.Lamberson, "Raising Cybersecurity Awareness among College Students," Journal of The Colloquium for Information System Security Education (CISSE), vol.4, no.1, September, 2016.
- [14] N.Ahmad, U.Aasma, W.F.P. Fauzi, Z.Othman, Y.Yeop, S.Noru, "Cybersecurity Situational Awareness among Parents," Cyber Resilience Conference (CRC), Nov. 2018.
- [15] P.Potgieter, "The Awareness Behaviour of Students On Cybersecurity Awareness by Using Social Media Platforms: A Case Study at Central University of Technology," Kalpa Publications in Computing vol.12, pp. 272-280, Proceedings of 4th International Conference on the Internet, Cybersecurity and Information Systems 2019.
- [16] L.Hadlington, "Employees Attitude towards Cybersecurity and Risky Online Behaviours: An Empirical Assessment in the United Kingdom," International Journal of Cyber Criminology, vol. 12, Issue 1, June 2018.
- [17] F.Alotaibi, S.Furnell, I.Stengel, M.Papadaki, "A survey of cybersecurity awareness in Saudi Arabia," 11th International Conference for Internet Technology and Secured Transactions (ICITST), Dec. 2016.
- [18] M.Zwilling, G.Klien, D.Lesjak, Ł.Wiechetek, F.Cetin, and H.N. Basim, "Cybersecurity Awareness, Knowledge and Behavior: A Comparative Study," Journal Of Computer Information Systems, vol. 60, 2020.
- [19] A.Malviya, G.A. Fink, L.Sego, B.Endicott-Popovsky, "Situational Awareness as a Measure of Performance in Cybersecurity Collaborative Work," Eighth International Conference on Information Technology: New Generations, April 2011.
- [20] M.Evangelopoulou, C.W. Johnson, "Empirical framework for situation awareness measurement techniques in network defense," International Conference on Cyber Situational Awareness (CyberSA), pp. 234-238, June 2015.
- [21] S.Tirumala, M.R.Valluri, G.A. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," International Conference on Computer Communication and Informatics (ICCCI), Jan. 2019.
- [22] N.Ahmed, U.Kulsum, M.I.Bin Azad, A.S.Zaforullah, M. E.Haque, M.S.Rahman, "Cybersecurity Awareness Survey: An Analysis from Bangladesh Perspective," IEEE Region 10 Humanitarian Technology Conference, Dhaka, Bangladesh, pp. 564-569, 2017. <https://doi.org/10.1109/R10-HTC.2017.8289074>.
- [23] N.Ahmed, M.R.Islam, U.Kulsum, M. Rajibul, M. Haque, M. Rahman, "Demographic Factors of Cybersecurity Awareness in Bangladesh," 5th International Conference on Advances in Electrical Engineering (ICAEE), pp.923-928, Dhaka, Bangladesh, 2019.
- [24] R.A. Haraty, "C2 Secure Database Management Systems - A Comparative Study," Proceedings of the ACM Symposium on Applied Computing. San Antonio, TX. March 1999.

# Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things

Monika Parmar<sup>1</sup>

Chitkara University School of Engineering and Technology  
Chitkara University, Himachal Pradesh, India

Harsimran Jit Kaur<sup>2</sup>

Chitkara University Institute of Engineering and  
Technology, Chitkara University, Punjab, India

**Abstract**—Cryptography algorithms play a vital role in Information Security and Management. To test the credibility, reliability of metadata exchanged between the sender and the recipient party of IoT applications different algorithms must be used. The hashing is also used for Electronic Signatures and based on how hard it is to hack them; various algorithms have different safety protocols. SHA-1, SHA-2, SHA3, MD4, and MD5, etc. are still the most accepted hash protocols. This article suggests the relevance of hash functions and the comparative study of different cryptographic techniques using blockchain technology. Cloud storage is amongst the most daunting issues, guaranteeing the confidentiality of encrypted data on virtual computers. Several protection challenges exist in the cloud, including encryption, integrity, and secrecy. Different encryption strategies are seeking to solve these problems of data protection to an immense degree. This article will focus on the comparative analysis of the SHA family and MD5 based on the speed of operation, its security concerns, and the need of using the Secure Hash Algorithm.

**Keywords**—Blockchain Technology; IoT; Secured Hash Algorithms; IoT Security; SHA; MD5

## I. INTRODUCTION

The Internet of Things is a connecting network of multiple things that are not only connected to one other but are also connected to the Internet. The basic services of IoT are rapidly increasing owing to its enormous range of applications by providing scalable solutions with lowered expenditure [1]. These scalable solutions always need fast and efficient authorization, information protection, confidentiality, intrusion responsiveness, fast implementation, and self-maintenance. Through implementing blockchain technology, certain specifications can be provided to the IoT solution of a business.

Blockchain is a program with a vast variety of implementations, typically related to cryptography. Besides that, it has subsequently been recently implemented as a distributed and permanent ledger that enables the phase of transfer registration and consultation. One should think about transactions happening in banking sectors as blockchain network transactions as a hypothetical example [2]. These days, to transact currency, the individual is dependent on banking and perhaps other reputable financial institutions. The payment respondents confirmed that the entity handling the transfer has the requisite infrastructure to ensure that it is

conducted efficiently and, quite notably, in a secure way. Besides that, as in the event of unforeseen failure, these intermediate institutions can collapse and therefore the faith is violated and so will be the transactions and products entrusted to them [3]. In distributed ledger technology, the confidence element is taken into account through the use of encrypted structures to include the statistical evidence of the total transaction performance. This testimony is unequivocally valid that the members in a blockchain are equipped with safety and integrity.

IoT systems can exchange data with others, to improve the knowledge of all members of the network and the surroundings. The IoT operation consists of a mixture of Interconnection, actuators, programmable controllers, and sensors [4]. Methods of a certain level IoT are applied at a quick speed with ideas such as smart homes, smart cities, and wearable devices which map out their characteristics prospective and efficient usage. Provided that blockchain is a hierarchical ledger system and also the IoT framework is naturally decentralized, it can be concluded that, in a real possibility, their synergy can be advantageous, thereby adding to the protection and accountability of IoT transactions. In view to improve the effectiveness of applications, Blockchain uses a technology in which computers consume large quantities of resources and processing power. IoT, on the contrary, is a network of objects that usually have a comparatively fewer number of resources, but it may even be of significant impact to merge these solutions [5]. The goal of this study is to explain the application of blockchain technologies in IoT applications, and even the effect on resource-constrained systems of many hash functions. At first, as we seek to explain how the system performs and the mechanisms involved, the blockchain concept will be explored in specific. This study investigated certain hashes methods that have been submitted by academics, but the majority of them have not been checked against blockchain and IoT threats. Section II summarizes the literature review of cryptographic hash functions in blockchain technology. Section III introduces the Blockchain technology and Cryptographic Hash functions, Section IV addresses the potential threats in blockchain and IoT, Blockchain Implementation to IoT is depicted in Section V, Section VI analyzes the proposed scheme for an effective hash function, and Section VII comprises the result and conclusion.

## II. LITERATURE REVIEW

Zeyad et al. [6] suggested the Pros and Cons of the optimization techniques and the impact on the performance level by performing experimental setup for SHAs by FPGA optimization methods.

B.P. Kosta et al. [7] demonstrated a Strong and a Secure lightweight cryptographic hash function is proposed in which each 512-bit of a data is compressed to 256-bit. Afterward, it is divided further into 8 blocks having 32-bits each.

F. Pfautsch et al. [8] validated the SHA-1 and SHA-3 hash functions because of the brute force threats on UltraScale+ FPGA dual-core systems. They have evaluated the passwords with 6 characters in 3 minutes time span and because of high complexity, the time raises by 5.5 for the SHA-3 Hash Algorithm.

N. Khan et al. [9] surveyed a thorough and in-depth survey of traditional authentication and the hash function is performed in this article, supported by a reasonable contrast of the period and computer processes usage of such methodologies.

C. White et al. [10] suggested Blockchain technology and picture hashes are used to create an image verification system. The concept developed in this paper, however, needs to be refined, as it tends to strive in some circumstances. This research demonstrates whether blockchain can be used to authenticate images, especially through picture hashing. Other findings provide the fact that in certain instances, utilizing adjacent frames hash operations around the same time will enhance efficiency, but that each type of cryptocurrency experiment will have its own distinct set of data.

Table I and Table II summarize the literature review for the given context.

## III. BLOCKCHAIN TECHNOLOGY AND CRYPTOGRAPHIC HASH FUNCTIONS

A Peer to Peer network may be a decentralized computing model if any of its technical services, such as computing power, space, and scanners, are shared by its members. To provide the infrastructure and information provided on the platform, these common services are essential. Blockchain is a distributed platform with no data analysis resources and no users to order them [12]. A node, therefore, depicts a system member. Every member has the authority to function as a server as well as the client, leading to the absence of a hierarchical system between them and providing the identical function in all networks. A protection scheme should be perceived when blockchain technology is decentralized because, unlike a centralized system where there is a single point of failure, is not the case here and can be targeted, thus it is tougher to interpret the information. This characteristic, even then, is not adequate to secure information passes through the system security and reliability. Blockchain is based on encryption to accomplish that. Generally, the cryptographic hash functions are of various types that provide different bit values depending on the type of hash and the same is depicted in Fig. 1.

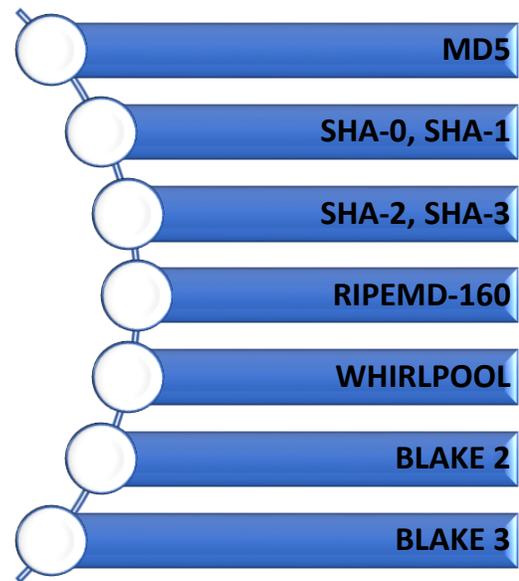


Fig. 1. Types of Cryptographic Hash Function.

Typically, two cryptographic methods are used for the blockchain framework: private and public key for the hash functions. The public key, which confirms the authenticity of whoever made the transfer, has to be used for exchanges to be digitally authenticated. It relies on a key to encipher and a dissimilar key to decipher [13]. Two very different keys are conceptually difficult to find, understanding only the encryption techniques used to produce them. This ensures the security and authenticity of the information if somebody confirms their transfer through its secret key since decrypting is only primarily driven by that of the hash value that is public in nature.

When the decoding results are positive, clients realize that the author of the secret key is someone who validated the agreement, and the information is not compromised or altered, else the decoding will not be efficient. The conversion of some form of data into a sequence of words is translated by these mechanisms. The same knowledge will still lead to almost the same key, and the slightest shift in the source information will create a hash that varies from the previous one. It's a minor processing operation to create a hash, but the reverse does not occur. It is virtually impossible to execute the reverse process to retrieve the actual data once the hash data is known [14]. As soon as the new block is generated, these hash functions are being utilized to confirm the block. Each block is connected to the previous block with the hash key and if someone wants to intrude in between, the hash value will change and will no longer be the same value in the blockchain. So there the frauds can be detected. hen an intruder happens to alter a block that is a member of a blockchain, together with its key, its value will alter in that way that this will not fit with the hash value present over the upcoming block in the chain.

The SHA functions in the SHA family comprise SHA-0, SHA-1, SHA-2, and SHA-3; while there are functionally distinct ones from that very same group. SHA-0 had several bugs and was not very common. So, SHA-1 was subsequently developed in 1995 to fix suspected SHA-0 vulnerabilities. Of the current SHA algorithms, SHA-1 might be the most commonly used one for SSL authentication. It has many variations in bits, for example, SHA-224, SHA-256, SHA-384, and SHA-512. It is based on the number of hash bits in the hash function. However, SHA-2 is a good cryptographic algorithm but it follows the same architecture as SHA-1 [15]. NIST introduces another algorithm that is Keccak algorithm considered as the SHA-3 Hash function. It presents various advantages, including efficient quality and reasonable tolerance for threats.

However, SHA-2 is a good cryptographic algorithm but it follows the same architecture as SHA-1. NIST introduces another algorithm that is Keccak algorithm considered as the SHA-3 Hash function. It presents various advantages, including efficient quality and reasonable tolerance for threats.

#### IV. POTENTIAL THREATS IN BLOCKCHAIN AND IOT

Each technology comes with its pros and cons so is blockchain technology. Several threats that deal with blockchain technology include double-spending threats, threats involved in mining, threats in wallets, threats based on the network, and threats in the smart contracts. Each above mentioned has many threats/attacks associated with it that can have a significant impact on the blockchain network and is shown in Fig. 2. Whenever a network infrastructure is affected, a double-spending threat can occur and virtual currency is generally seized. To make it appear valid, the hacker will indeed send a duplicate copy of the currency or could expunge the transfer of funds entirely. However, it is not widespread, double-spending does happen. This type of threat includes a 51% attack in which a node miner or team of miners on a public ledger tries two times to invest one's digital currency on that public ledger [16]. They are trying to invest twice in them; thus, the title double-spending attack is given. This is not always aimed at doubling crypto spending, but almost always discrediting a particular crypto or blockchain technology by influencing its credibility.

It informs us that more successful clustering power contributes to greater protection against a 51 percent attack while testing the Proof of Work (PoW) algorithm [17]. However, small-size blockchains that run on PoW could be slightly more prone to this kind of attack, given that the intruder does not cope with even more computing power which is the reason that 51% of attacks tend to happen on smaller blockchains whenever these occur in any way. The Bitcoin blockchain still hasn't experienced a 51 percent intrusion yet.

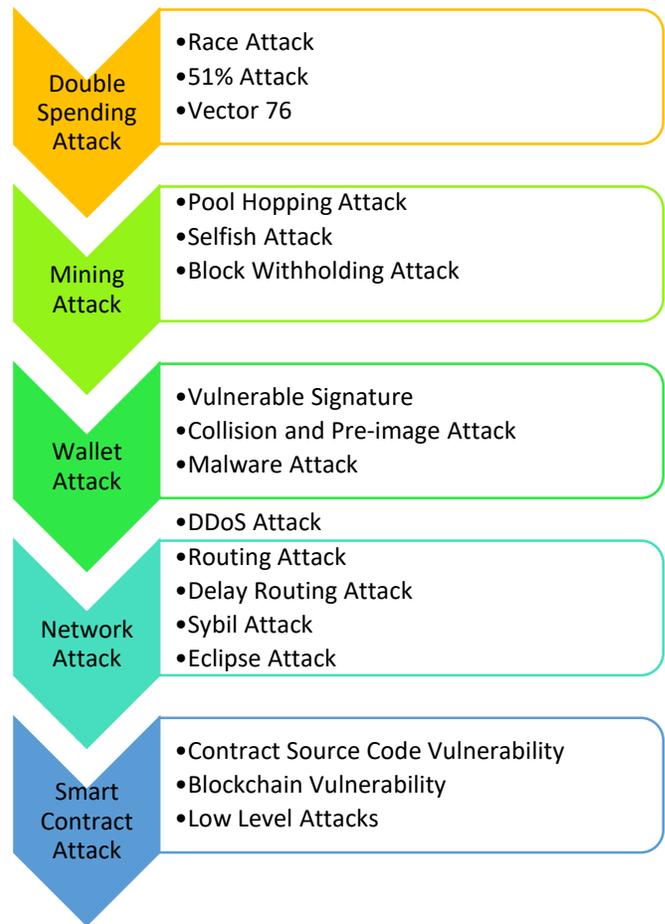


Fig. 2. Threats at Blockchain Levels.

Whenever an intruder makes two opposing transfers, a race attack will be launched. The first-ever transfer would be sent to the individual who, instead of any wait for clarification of the transfer, confirms the transfer (and delivers a service, for example). At the same instance of time, a different transfer is distributed to the server that returns the equal amount of digital currency to the intruder, ultimately rendering the very first transactions null. A decentralized wallet that helps customers to exchange and handle cryptocurrency, as well as ether, is called a blockchain wallet. This wallet is created by Blockchain which is an e-wallet that helps users to manage and move bitcoins [18]. A pre-image threat on cryptographic operations in hashing aims to locate a document that seems to have a particular hash code. A hash of cryptography can withstand threats upon the pre-image. Network attacks include DDoS attacks, Sybil attacks, Routing threats, etc. In general, a DDoS attack may burden a network with new chunks of information inside a network, which would compel a blockchain to function slowly to use its computing capacity. It

is a Denial-of-Service intrusion and is a tactic to interrupt connectivity to a network interface or internet platform by normal nodes. Usually, this is done by overburdening the endpoint with a large amount of activity or by injecting fake requests that enable the targeted system to fully fail or collapse. Sybil attacks are prominent in P2P systems where several nodes are successfully run simultaneously by a network interface and compromise the power in credibility schemes [19]. The primary purpose of this threat is to obtain the bulk of the power in the systems to enable unlawful acts in the framework. Such numerous false profiles tend to be legitimate specific attributes for the system. The absence of smart contract technology requirements passes more of the pressure to the organization as it opens its connection details to possible damage. As when the event reveals, the contract applied cannot reflect the agreeing partners' real purpose. In IoT, some architectural levels layers include the Physical layer, Network layer, Middleware, and Application layer [20]. On each layer of IoT, there are different threats and are shown in Fig. 3.

As IoT is growing at a rapid so its challenges include security issues in many IoT applications, it is cost and traffic, increased load capacity on Cloud Service and services insufficiently, Issues in System infrastructure/Architecture, and manipulating information [21]. Table I shows the challenges towards IoT applications, various attacks included, and the possible blockchain solution for the same.



Fig. 3. Security Threats at IoT Architectural Levels.

TABLE I. CHALLENGES OF IOT APPLICATIONS AND THE POSSIBLE BLOCKCHAIN SOLUTION

Challenge Towards IoT	Inclusion Attacks	Specification	Possible Blockchain Solution
<b>Security Issues in IoT Applications</b>	• Node Capturing	IoT applications are prone to exposure to personal information.	For this issue, permission type blockchain can be used that can enhance security[15].
	• SQL Injection Attacks		
	• Man-In-Middle-Attack		
	• Data Thefts		
	• Sniffing Attacks		
<b>Cost and Traffic</b>	• Phishing Site Attack	To handle exponential growth in IoT devices	It can be solved by the decentralization feature of the blockchain. In this, central servers are not being used as every node can directly communicate to each other [27] [28] [29].
	• Booting Attacks		
	• Data Transit Attacks		
	• Routing Attacks		
	• Access Control Attack		
<b>Increased load capacity on Cloud Service and services insufficiently</b>	• DDoS/DoS Attack	Owing to security issues/threats or the attacks on the cloud, the services from the cloud discontinues	Each file is updated separately as a ledger on every node/device on the network so single point failure is not possible in such a case [31].
	• Firmware Updates		
	• Service Interruption Attacks		
	• Flooding Attack in Cloud		
<b>Issues in System infrastructure/Architecture</b>	• Side-Channel Attacks	Every section in IoT are prone to single point failure and it affects the systems and whole infrastructure	Verification of data is done with the help of encryption techniques utilizing the blockchain[28].
	• Eavesdropping and Interferences		
	• Sleep Deprivation Attacks		
	• Secure On-Boarding		
	• Extra Interfaces		
	• Reprogram Attacks		
<b>Manipulating Information</b>	• False Data Injection Attack	Information is deliberately taking out from IoT units and manipulating the information maliciously.	A blockchain ledger is updated at every node so if there is any malicious node that updates the information, other nodes will decline that[30].
	• Malicious Code Injection Attack		
	• Access Attack		
	• Signature Wrapping Attack		
	• End-to-End encryption		

V. BLOCKCHAIN IMPLEMENTATION TO IOT

Today many IoT implementations rely on a centralized server/client model, in which clients link across the Network to services virtualized on to the cloud. While these methods are feasible, as IoT expands a new mechanism is required. Decentralized alternatives have been suggested yet Peer to Peer alone cannot assure security and confidentiality [32]. Blockchain has the power to respond to a number of the problems that come from the use of IoT: IoT implementations are costly because of the expense of central server management in the cloud. To improve protection and loyalty, accountability is important. An open-source approach is desired and should be considered in the development of the next version of IoT products. Since IoT usually requires a central agency, the central level failure problem is prevalent. Factors such as time synchronization, registries, anonymity,

and reliability are tough to control reliably [33]. IoT applications are renowned for moderate computational power and also energy efficiency. This system may not be able to use the highest cryptographic algorithms since it takes much longer to access. As per storage is concerned, all nodes hold a backup of all dealings which has existed in the database since its development. The scale would grow as time has gone through or IoT devices might not even be capable of storing it [34]. The problems of ledger extended to IoT originate in its minimal investment. Although the computing capacity is limited, these machines can still execute activities as long as protocols and frameworks designed for them are utilized [35].

So, hash algorithms have to be checked thoroughly for their performance level. A comparative analysis of blockchain and IoT-based systems is being presented in Table II.

TABLE II. A COMPARATIVE ANALYSIS OF AN EXISTING SURVEY ON BLOCKCHAIN AND IOT BASED SYSTEMS

<b>** represents covered partially, ✓ represents covered in detail, and ✗ represents not covered in the literature</b>					
<b>Application Criteria</b>	<b>Year of publication</b>	<b>Major Inclusion</b>	<b>Considered Factors</b>	<b>Discussion on Storage Issues</b>	<b>Discussion on Security Issues</b>
Blockchain-based IoT applications	2019 [11]	Overview of Opportunities and challenges of IoT and Blockchain is provided	<ul style="list-style-type: none"> <li>• Interoperability</li> <li>• Security and privacy of IoT</li> </ul>	**	**
	2018[12]	Detailed discussion on blockchain techniques, applications, and challenges	<ul style="list-style-type: none"> <li>• Consensus algorithms</li> <li>• Security issues in blockchain</li> </ul>	✗	✓
IoT storage optimization	2017[13]	A detailed analysis of optimizing the level of performance in distributed storage onto the cloud.	<ul style="list-style-type: none"> <li>• Improvement in transmission efficiency.</li> <li>• Distributed cloud storage</li> <li>• The adaptive network coding scheme</li> </ul>	✓	✗
	2020[14]	An in-depth approach for optimizing the data access storage architecture in the Internet of Things, in which factors of data access storage distribution are fully considered, and secured hashing is being used to configure the data for storage optimization.	<ul style="list-style-type: none"> <li>• Data processing efficiency</li> <li>• Time consumption for reading the files</li> <li>• File download efficiency</li> </ul>	✓	✗
Blockchain-based IoT storage optimization	2017[15]	A brief discussion on lightweight BC-based architecture for IoT that virtually eliminates the overheads of classic BC.	<ul style="list-style-type: none"> <li>• Block validation processing time</li> <li>• PoW</li> <li>• BC-based smart home</li> </ul>	✓	**
	2019[16] [26]	An investigation about lightweight blockchain management with a superior reduction in resource usage and also save the significant information about IoT framework.	<ul style="list-style-type: none"> <li>• WSN</li> <li>• CPS</li> <li>• PoS consensus mechanisms</li> <li>• Mobility based blockchain management</li> </ul>	✓	✗
Blockchain for IoT security	2017[9] [23] [24]	A comprehensive case study of smart home	<ul style="list-style-type: none"> <li>• Security analysis</li> <li>• DDoS attack</li> <li>• Packet overhead</li> <li>• Energy consumption</li> </ul>	✗	✓
	2020[18] [25]	Detailed insights of a software-defined blockchain architecture to realize the configurations for blockchains. Also, a consensus function virtualization approach with application-aware workflow is proposed.	<ul style="list-style-type: none"> <li>• Consensus algorithms</li> <li>• SDN</li> <li>• Throughput of transactions</li> <li>• Energy consumption</li> <li>• Consensus switch accuracy</li> </ul>	✗	✓
Security issues of IoT	2019 [17] [19]	A comprehensive survey of security, issues, challenges, and considerations of IoT	<ul style="list-style-type: none"> <li>• Physical attacks</li> <li>• Networks attacks</li> <li>• Software attacks</li> <li>• Encryption attacks</li> </ul>	✗	✓

	2020 [21] [22] [36]	A discussion about security, privacy, and trust in the Internet of Things	<ul style="list-style-type: none"> <li>Secured middleware</li> <li>Mobile security in IoT</li> <li>Public key cryptography (PKC)</li> </ul>	✗	✓
Comparative analysis of a secured hash algorithm for IoT applications	This article	Detailed insights about cryptographic hash algorithms for Blockchain and IoT	<ul style="list-style-type: none"> <li>Threats to IoT</li> <li>Performance checks for various cryptographic algorithms</li> <li>The practical applicability of blockchain</li> <li>Secured strategies</li> </ul>	✓	✓

### VI. PROPOSED SCHEME FOR EFFECTIVE HASH FUNCTION

In the proposed scheme, three levels of comparison are being carried out that is based on the output size bits of the hash algorithm, size of the file and time to execute these files through a hash function, and based on the speed performance of various hash algorithms. Six different iterations are taken to compare the time execution of hash algorithms. For the six iterations, two major cases are being taken that include a short sequence of data that is to be hashed and a large sequence of data that is to be hashed and the comparison is in between MD5, SHA-1, SHA-256, and SHA-512. Fig. 4 depicts the three levels of comparison for the hash algorithm.

Based on the output size (in bits), different hash algorithms are analyzed. It is depicted in Fig. 5 that the more the number of hash bits, the higher the security. So, from this, it is shown that SHA-512 and SHA-256 have comparable output bits.

Also, the file size for execution is an important factor while deciding the secured hash algorithm. For a file of size 1KB, 5Kb, and 10 KB, the time taken for execution is depicted in Fig. 6 below. So, for large-size files, SHA1 is taking less time as compared to SHA2 and SHA3.

Also, hash algorithms can be compared based on their speed, and accordingly, a particular hash is selected. In this, six iteration were taken for the two major cases and that includes a small sequence having immutable universally unique identifier string, immutable universally unique identifier including system current time, and random immutable universally unique identifier with system current time and large sequence that will include two immutable universally unique identifiers, two immutable universally unique identifier with current system time, and three random immutables universally unique identifier with current system time. The setup is implemented in java with these six iterations and outcomes from several samples are collated and evaluated. There are six primary instances and are mentioned in Table III.



Fig. 4. Three Levels of Comparison of Hash Algorithms.

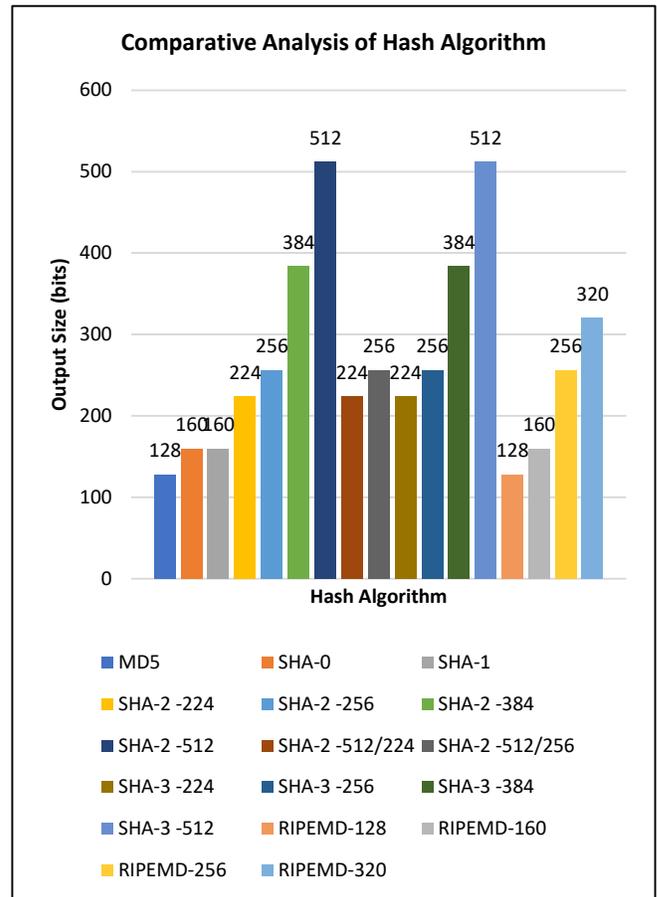


Fig. 5. Comparative Analysis of Hash Algorithm based on Output Size (Bits).

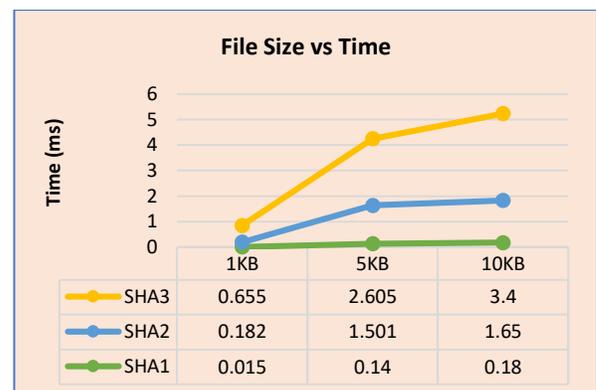


Fig. 6. Comparative Analysis of Hash Algorithms based on File Size.

TABLE III. SIX ITERATIONS EXECUTION TIME FOR SMALL AND LARGE SEQUENCE

HASH ALGORITHM	SMALL SEQUENCE (ms)			LARGE SEQUENCE (ms)		
	ITERATION 1	ITERATION 2	ITERATION 3	ITERATION 4	ITERATION 5	ITERATION 6
MD5	542	715	1425	798	892	1606
SHA-1	458	466	1146	601	716	1319
SHA-256	513	492	1120	639	750	1339
SHA-512	379	469	1172	593	750	1349

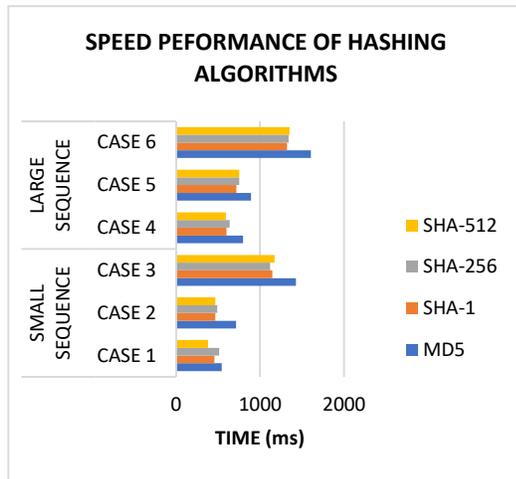


Fig. 7. Comparative Analysis of Speed Performance for Hash Algorithms.

From the above cases, it is being concluded and shown in Fig. 7 that MD5 is faster in speed response than SHA-1 with 29.57% for small sequences and faster 25.04% for large sequences. Also, SHA-1 is slow as compared to SHA-256 with 2.59% for small sequences and a 3.37% slower use level when selecting secured hash algorithm. MD5 is faster in speed response than SHA-1 with 29.57% for small sequences and faster 25.04% for large sequences. Also, SHA-1 is slow as compared to SHA-256 with 2.59% for large sequences. SHA-256 is 5.2% faster than SHA-512 for small and faster than SHA-512 with 1.34% for large sequences. Also, out of all, SHA-1 is the fastest with 708.3 ms for small sequences and 909.3 ms for long sequences. For future work the Hybrid Cryptographic Hash Function could be suggested for a security evolved approach which would increase network consensus, however, the ledger node's confidence in current IoT devices cannot be guaranteed, and reaching a consensus would consume a large number of wireless communications.

### VII. CONCLUSION

Blockchain systems can supply IoT through a distributed ledger system to exchange data in a secure nature intimidating the centralized power model that remains presently on IoT. In cryptographic currencies, the Internet of Things, chain management, financing, information exchange, and other areas, Blockchain is broadly adopted. In blockchain systems, although, there seems to be safety issues of different extents. A cryptographic hash is used to validate the authenticity and

validation of transmissions in a variety of ways. MD5, SHA-1, SHA-2, and SHA-3 have all become the industry norms. The majority of them were discovered to be either usable or inefficient in terms of time. This study investigated certain hashes methods that have been submitted by academics, but the majority of them have not been checked against blockchain and IoT threats. Therefore, hash performance plays a crucial role in blockchain as well as in IoT. So, this paper focuses on the different cryptographic hash algorithms and it is conferred that it is indeed safe to limit MD5 and SHA-1 because they have been vulnerable and not secured. However, if the performance is considerably better than stable SHA-2 family for a specific scenario and protection is not so necessary, they can be selected. It is dependent on the use level when selecting a secured hash algorithm. SHA-1 is the fastest with 708.3 ms for small sequences and 909.3 ms for long sequences.

### REFERENCES

- [1] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, no. March, pp. 648–651, 2012, doi: 10.1109/ICCSEE.2012.373.
- [2] F. Lin et al., "Survey on blockchain for internet of things," J. Internet Serv. Inf. Secur., vol. 9, no. 2, pp. 1–30, 2019, doi: 10.22667/JISIS.2019.05.31.001.
- [3] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, no. c, pp. 32979–33001, 2018, doi: 10.1109/ACCESS.2018.2842685.
- [4] K. Biswas and A. B. Technology, "Securing Smart Cities Using Blockchain Technology," 2016 IEEE 18th Int. Conf. High Perform. Comput. Commun. IEEE 14th Int. Conf. Smart City; IEEE 2nd Int. Conf. Data Sci. Syst., pp. 1392–1393, 2016, doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.
- [5] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain Based Data Integrity Service Framework for IoT Data," 2017, doi: 10.1109/ICWS.2017.54.
- [6] M. Abu-elkheir, M. Hayajneh, and N. A. Ali, "Data Management for the Internet of Things: Design Primitives and Solution," pp. 15582–15612, 2013, doi: 10.3390/s131115582.
- [7] Zeyad A. Al-Odat, Mazhar Ali, Assad Abbas, and Samee U. Khan. 2020. Secure Hash Algorithms and the Corresponding FPGA Optimization Techniques. ACM Comput. Surv. 53, 5, Article 97 (October 2020), 36 pages. doi:https://doi.org/10.1145/3311724.
- [8] B.P Kosta, and P.S. Naidu " Design and Implementation of a Strong and Secure Lightweight Cryptographic Hash Algorithm using Elliptic Curve Concept: SSLHA-160 ",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 2, 2021.
- [9] Pfautsch, Fr., Schubert, N., Orglmeister, C., Gebhart, M., Habermann, P. & Juurlink, B., (2020). The Evolution of Secure Hash Algorithms. PARS-Mitteilungen: Vol. 35, Nr. 1. Berlin: Gesellschaft für Informatik e.V., Fachgruppe PARS. (S. 5-15).
- [10] N. Khan, N. Sakib, I. Jerin, S. Quader and A. Chakraborty, "Performance analysis of security algorithms for IoT devices," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 2017, pp. 130-133, doi: 10.1109/R10-HTC.2017.8288923.
- [11] White, C., Paul, M. and Chakraborty, S., 2020. A Practical Blockchain Framework using Image Hashing for Image Authentication. arXiv e-prints, pp.arXiv-2004.
- [12] L. Wan, D. Eyers, and H. Zhang, "Evaluating the impact of network latency on the safety of blockchain transactions," Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019, pp. 194–201, 2019, doi: 10.1109/Blockchain.2019.00033.
- [13] J. Li, J. Wu, and L. Chen, "Block-secure: Blockchain based scheme for secure P2P cloud storage," Inf. Sci. (Ny.), vol. 465, pp. 219–231, 2018, doi: 10.1016/j.ins.2018.06.071.

- [14] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 464–467, 2017, doi: 10.23919/ICACTION.2017.7890132.
- [15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work.* 2017, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.
- [16] K. Hossain and S. Roy, "A Data Compression and Storage Optimization Framework for IoT Sensor Data in Cloud Storage," *2018 21st Int. Conf. Comput. Inf. Technol.*, pp. 1–6, 2018.
- [17] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, vol. 2018-July, no. i, 2018, doi: 10.1109/ICCCN.2018.8487348.
- [18] T. Alam, "Blockchain and its Role in the Internet of Things (IoT)," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, no. January 2019, pp. 151–157, 2019, doi: 10.32628/cseit195137.
- [19] J. Li, Y. Liu, Z. Zhang, J. Ren, and N. Zhao, "Towards Green IoT Networking: Performance Optimization of Network Coding Based Communication and Reliable Storage," *IEEE Access*, vol. 5, pp. 8780–8791, 2017, doi: 10.1109/ACCESS.2017.2706328.
- [20] M. Wang and Q. Zhang, "Optimized data storage algorithm of IoT based on cloud computing in distributed system," *Comput. Commun.*, vol. 157, no. February, pp. 124–131, 2020, doi: 10.1016/j.comcom.2020.04.023.
- [21] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," *Proc. - 2017 IEEE/ACM 2nd Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2017 (part CPS Week)*, pp. 173–178, 2017, doi: 10.1145/3054977.3055003.
- [22] A. R. Shahid, N. Pissinou, C. Stajer, and R. Kwan, "Sensor-Chain : A Lightweight Scalable Blockchain Framework for Internet of Things," *2019 Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, pp. 1154–1161, 2019, doi: 10.1109/iThings/GreenCom/CPSCoM/SmartData.2019.00195.
- [23] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.
- [24] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang, "Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT," *IEEE Netw.*, vol. 34, no. 1, pp. 69–75, 2020, doi: 10.1109/MNET.001.1900179.
- [25] A. Gajbhiye and D. Sen, "Attacks and Security Issues in IoT Communication : A Survey," pp. 1688–1693, 2020.
- [26] F. Buccafurri, G. Lax, L. Musarella, and A. Russo, "Ethereum transactions and smart contracts among secure identities," *CEUR Workshop Proc.*, vol. 2334, pp. 5–16, 2019.
- [27] M. Sigwart, M. Borkowski, M. Peise, S. Schulte, and S. Tai, "Blockchain-based data provenance for the internet of things," *ACM Int. Conf. Proceeding Ser.*, 2019, doi: 10.1145/3365871.3365886.
- [28] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment," *2018 IEEE Int. Conf. Inf. Reuse Integr.*, pp. 15–22, 2018, doi: 10.1109/IRI.2018.00011.
- [29] D. Liu, J. Ni, C. Huang, X. Lin, and X. Shen, "Secure and Efficient Distributed Network Provenance for IoT: A Blockchain-based Approach," *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2020, doi: 10.1109/jiot.2020.2988481.
- [30] K. Kumar, S. Kumar, O. Kaiwartya, Y. Cao, J. Lloret, and N. Aslam, "Cross-layer energy optimization for IoT environments: Technical advances and opportunities," *Energies*, vol. 10, no. 12, 2017, doi: 10.3390/en10122073.
- [31] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, *An Overview of Blockchain Security*, vol. 2. Springer Singapore, 2019.
- [32] Y. Qian et al., "Towards decentralized IoT security enhancement: A blockchain approach," *Comput. Electr. Eng.*, vol. 72, pp. 266–273, 2018, doi: 10.1016/j.compeleceng.2018.08.021.
- [33] H. Kim, S. H. Kim, J. Y. Hwang, and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," *IEEE Access*, vol. 7, no. September, pp. 136481–136495, 2019, doi: 10.1109/ACCESS.2019.2940052.
- [34] R. Yasaweerasinghelage, M. Staples, and I. Weber, "Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation," *Proc. - 2017 IEEE Int. Conf. Softw. Archit. ICSA 2017*, no. October, pp. 253–256, 2017, doi: 10.1109/ICSA.2017.22.
- [35] Y. Xu and Y. Huang, "Segment blockchain: A size reduced storage mechanism for blockchain," *IEEE Access*, vol. 8, pp. 17434–17441, 2020, doi: 10.1109/ACCESS.2020.2966464.
- [36] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, p. 102481, 2020, doi: 10.1016/j.jnca.2019.102481.

# Proof-of-Review: A Review based Consensus Protocol for Blockchain Application

Dodo Khan<sup>1</sup>, Low Tang Jung<sup>2</sup>, Manzoor Ahmed Hashmani<sup>3</sup>

Department of Computer and Information Science  
Universiti Teknologi Petronas, Seri Iskandar  
32610 Perak Darul Ridzuan, Malaysia

**Abstract**—Blockchain is considered one of the most disruptive technologies of our time and in the last 2 decades and has drawn attention from research and industrial communities. Blockchain is basically a distributed ledger with immutable records, mostly utilized to perform the transactions across various nodes after achieving the mutual consensus between all the associated nodes. The consensus protocol is a core component of Blockchain technology, playing a vital role in Blockchain's success, global emergence, and disruption capability. Many consensus protocols such as PoW, PoS, PoET, etc. have been proposed to make Blockchain more efficient to meet real-time application requirements. However, these protocols have their respective limitations of low throughput and high latency and sacrifice on scalability. These limitations have motivated this research team to introduce a novel review-based consensus protocol called Proof-of-Review, which is aimed to establish an efficient, reliable, and scalable Blockchain. The "review" in the proposed protocol is referring to the community trust on a node, which is entirely depending on the node's previous behavior within the network which includes the previous transactions and interaction with other nodes. Those reviews eventually become the trust value gained by the node. The more positive the reviews the more trustworthy is the node to be considered in the network and vice versa. The most trustworthy node is selected to become the round leader and allows to publish a new block. The architecture of the proposed protocol is based on two parallel chains i.e. Transaction Chain and Review Chain. Both chains are linked to each other. The transaction chain stores the transaction whereas the review chain will store the reviews and be analyzed with an NLP algorithm to find the round leader for the next round.

**Keywords**—Blockchain; consensus protocol; transaction chain; review chain; prove-of-review; PoW; PoS

## I. INTRODUCTION

Blockchain technology is one of the most hyped decentralized innovation these days with an enlightening future. Initially, Blockchain was introduced by Haber and Stornetta [1] and later gained intense attention because of the Bitcoin by Nakamoto in 2008 [2]. Bitcoin earns intense success in the cryptocurrency arena. Many similar currencies have been launched in the following years. There are 2017 crypto currencies available on the internet by 2019 [3] with the different business models. Besides global cryptocurrency hype, Bitcoin holds the highest market capitalization of up to 53%. Blockchain is serving as the fundamental technology behind Bitcoin. Besides cryptocurrency, Blockchain gain lots of attraction from a diverse range of fields and has shown a noticeable growth like

in insurance[4], healthcare[5-7], economics [8-10], IoT [11-13], supply chain, software engineering [14-16], transport, government agencies, distributed video coding [58] and finance. As per the survey conducted by World Economic Forum [17], Blockchain will be soaring to 10% of global GDP by 2027.

The primary properties of this technology are decentralization, resiliency, integrity, anonymity which are the driving force for industries to adopt Blockchain. Along with various technical components, the consensus protocol is the main component in which Blockchain relies on. Consensus protocol plays a vital role in blockchain's success, global emergence, and disruption. It serves to achieve the consensus of information sharing, replicating state, and broadcast the transaction amongst the Blockchain network participants without any controlled 3rd party or authority. The success of Blockchain is heavily dependent on an efficient consensus mechanism for its great impact on the overall performance which shall include transaction throughput, latency, scalability, and fault tolerance.

There are many comprehensive definitions of consensus protocol available in the literature. However, in this study "The agreement on the common state of ledger in between the group of nodes in Blockchain application" is adopted as the definition. There are ranges of consensus protocols available for Blockchain implementations. Nakamoto proposed PoW[2] with Bitcoin to address double spending issue in digital cryptocurrency system in a trustless environment. Since the day Bitcoin is launched, it is continuously growing in terms of the number of transactions and the nodes. Due to the exponential growth, it encounters several performance issues. The most highlighted are the huge amount of energy consumption, low transaction throughput, high latency, and poor scalability. Currently, the Bitcoin network consists of around 10 thousand nodes [18] while it can only process 7 transactions per second (TPS) with a latency of 10 min. Moreover, the transaction throughput can possibly be raised to 25 TPS after fine tuning of the key parameters without compromising the security [19] and it also consumes huge amount of energy [20].

There are centralized applications performing better than Bitcoin. For example, VISA network is comprising of around 50 million users and at maximum, it can process up to 65000 TPS [1]. Researchers tried to address the blockchain limitations with new consensus mechanisms/approaches to reduce energy-intensive mining and the energy

consumption while increasing throughput. For example, Proof of Luck [21], Proof of Authority (PoA), Proof of Space [22], Proof of Elapsed Time (PoET) [23], and Proof of Stake (PoS). Every available protocol comes with its own advantages and disadvantages but mostly lacking in real-time transaction processing. Besides, there is no universal generic consensus protocol so far which can possibly be implemented in every domain with diverse set application requirements.

This research utilizes an emerging area of Blockchain consensus protocol but least investigated, the review-based approach. This approach intends to make every node accountable for every transaction and allowing all the nodes as a whole to decide which node will generate the next Block. The “reviews” is referring to the community trust on a node, which entirely depends on the node’s previous behavior within the network which shall include the previous transactions and interaction with other nodes. Every node will share its experience with other nodes in the reviews form and those reviews will eventually become the trust value of the node after the analysis through an NLP algorithm. The more positive the reviews the more trustworthy a node shall be considered in the network and vice versa. Securing good and positive reviews is not easy and not a one-day job. It needs consistently good behavior to earn others’ trust. It cannot be spent and bought therefore the only way to increase trust is to behave honestly. Blockchain and reviews would be a good combination where reviews serve as an incentive and blockchain is responsible to keep reviews record safe.

In this study, we propose a new proof-of-review consensus protocol to establish a reliable and scalable Blockchain. This protocol intends to address the shortcoming of the previous model in terms of throughput, latency, scalability, and energy consumption. The architecture of the proposed protocol is based on 2 parallel chains, the transaction chain, and the review chain. Both chains are linked to each other. The transaction chain, as usual, stores the transactions whereas the review chain will store the reviews and those that will be analyzed by an NLP algorithm to determine a round leader to generate a new Block while other nodes will be involved in the block verification process. The proposed protocol is also tolerant to some of the major attacks such as Sybil attack, bad-mouthing, on-off, etc.

The rest of the paper is structured as follows. In Section 2, we discuss the Background of Blockchain and the consensus model. Section 3 discusses the related work in consensus model. Section 4 describes the proposed proof-of-review (PoRv) consensus protocol with details. Section 5 discusses the block structure. Section 6 is about the security analysis of PoRv which includes the potential attacks and strategies to address the attacks. Section 7 discusses the preliminary results and Sections 8 and 9 discuss the conclusion and future work respectively.

## II. BLOCKCHAIN BACKGROUND

### A. Blockchain Characteristics

There are several definitions of Blockchain available in the literature. Most of them define the context it is supposed to be used. For example, a publicly shared ledger for maintaining the

transaction by many nodes anonymously without control of any central party [24]. A decentralized database with the capacity to work in the decentralized environment without trusting the intermediaries [24]. A shared, distributed, immutable replicated, and tamper-evident ledger letting every participant to access read, and verify the legitimacy [25]. A type of distributed ledger maintaining the information regarding the transaction which are shared between all the participants in the network [26]. Transparency, Immutability, distributed database, ledger, auditability, and intermediary are the common terminologies used in every definition.

Fig. 1 illustrates that in the Blockchain, the first Block is referred as Genesis Block. The previous hash in the genesis block would be equal to Zero. The Block in the Blockchain contains an organized set of records and every block is cryptographically coupled with the next block. Since Blockchain works in distributed and decentralized fashion, it maintains a long list of Block and every Block contains many transactions depending on its size. Moreover, Blocks are divided into two sections: Block header and transaction. Block header comprises of Version, Prev\_Hash, Merkle root, timestamp, nonce Hash (the unique identity of each Block) which is entirely different for every block like figure prints.

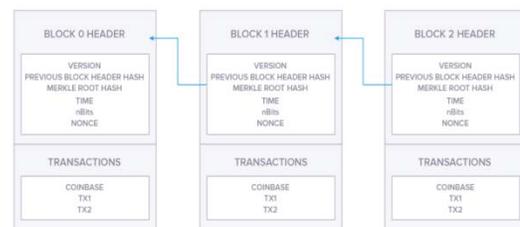


Fig. 1. Bitcoin Blockchain Structure.

Every Block carries the hash of prior block therefore every block is connected to one another through the hash. Any manipulation in the information of the block alters the hash number and that block will be unrecognizable for the next block [27]. Fig. 1 shows the Bitcoin blockchain structure.

In general, Blockchain is classified into three different categories. Namely, Public Blockchain, consortium Blockchain, and Private Blockchain [28]. The major differences in these categories are based on who can participate in the Blockchain consensus process [29]. For example, in Public Blockchain all nodes are welcome to participate in the consensus process whereas in Consortium and Private Blockchain only selected and validated set of nodes can participate.

- **Public Blockchain:** The Public Blockchain network is entirely opened for everyone to freely join and leave at any time as they please. Therefore, it works in between completely anonymous and entrusted nodes. In Public Blockchain, information is accessible and shared to all network participants. It comes under the umbrella of a permissionless Blockchain. Moreover, every node is welcome to participate in the consensus process to ensure the validity and integrity of data. Bitcoin and Ethereum are classic examples of Public Blockchain.

- **Federated Blockchain:** Federated Blockchains are also referred as Consortium Blockchain. In which every node can access data. However, only a predetermined group of nodes would be able to change and take part in the consensus process. Most of the consortium Blockchain are implemented in banking sector [30]. Because in the banking settings, the idea is to share the power between the authorities rather than one controlled authority who can possibly make biased decisions. Here are some well-known examples of Consortium Blockchain, R3 (Bank), EWF (Energy), B3i (Insurance).
- **Private Blockchain:** Federated Private Blockchain is kind of centralized blockchain in which central authority or predefined group of nodes can read and write or participate in the blockchain. Only pre-validated nodes would be able to join the network. Furthermore, the known and authorized nodes take responsibility to maintain the consensus process. Private Blockchain are considered as Permissioned Blockchain where data is accessible to authorized groups of nodes. These groups can change acceptance by consensus procedure. Private Blockchain is designed for settings where all nodes are known and authorized.

#### B. Key Properties of Blockchain

Some of the key properties of blockchain are described in this section,

- **Persistency:** Blockchain transactions are maintained in shared ledger which are considered as persistent because the ledger is shared across the distributed network, where every node is made accountable and on control of its record and maintains the integrity by the consensus protocol. So, persistency can only be retained if majority of the nodes acts honestly. Several Blockchain properties are derived from persistency, i.e., transparency, immutability which makes Blockchain auditable [31].
- **Validity:** Unlike several distributed system, Blockchain does not need every node to perform validation. Blocks and transaction are broadcasted across distributed network and their legitimacy will be validated by all other nodes that process is referred as consensus mechanism. Therefore, any illegitimate action would easily be identified with the source node. There are 3 major roles for this process. (1) Proposer: the one who proposes the value (2) Acceptor: The one who verify the value and take a decision and (3) Learner who accepts on the chose value [24].
- **Anonymity and Identity:** Anonymity is one of the primary properties of Public Blockchain. Node identification could be linked with the real-life identity. A single user can acquire multiple identities for avoiding identity exposure [32]. There is no central entity is required to maintain the private data such as identity. On the other hand, in private Blockchain identities are required to operate and governed by known entities and authorized group of nodes.

#### C. Consensus Characterization

In Blockchain the key tasks are the block validation and the continuous maintaining of the security which can be achieved by a well-structured mechanism called consensus protocol. Since Blockchain is a distributed and a shared ledger so there is no need for a centralized authority to ensure the legitimacy of all the transactions. Therefore, it is challenging to achieve consensus among the nodes on the transaction in a block without compromising on the security [26]. Therefore, the consensus protocol is considered as the heart of any Blockchain application. In the distributed environment, achieving consensus is not a trivial task to get all network participants (Nodes) to agree on accepting or rejecting a potential block. Once a new Block is accepted, all node members are supposed to append this block into their respective chain.

The consensus protocol is an active research area in the last two decades. It has been and being deep studies for its resilient for a node failure, message delay, portioning of the network, message out of order or missing. In Blockchain network, the consensus protocol is supposed to deal with the malicious, selfish, faulty nodes and make sure that all nodes have reached consensus among them on the global state of the ledger. In the context of Blockchain, the three key properties of consensus mechanism namely Safety, Liveness, and Fault Tolerance shall determine the applicability and efficiency of any consensus protocol [31].

- **Safety:** This property is the responsible for ensuring that nothing malicious will ever take place in the Blockchain. It refers to the properties of validity and agreement in the conventional consensus set out in the distributed systems. Validity is defined as "A correct mechanism proposed a value X then another correct mechanism should also produce the same the value X". Whereas the Agreement property made responsible to ensure that two correct processes should not provide different output. Generally, consensus protocol is considered safe when upon one honest node produces valid output and subsequently every other node in the network obtain the same output. The produced output should be valid and be the same as all other nodes, referring to consistency of the share state [33].
- **Liveness:** This property ensures that eventually, something good will take place. Liveness of consensus mechanism can only be ensured if all honest nodes participate in the consensus process and ultimately generate a value and all right/correct requests will eventually be processed. There is no time limit to decide on a value, it is not necessary for all nodes to have a same state at a given point of time.
- **Fault Tolerance:** A consensus protocol is considered fault tolerant when it is resilient to failure of nodes which are participating in the consensus process. The node failure can be planned in two types.

Fail-Stop - It deals with all nodes who discontinue processing temporarily or permanently. And those also stop producing, receiving messages, or taking part in consensus process.

Byzantine failure – It deals with faulty and malicious nodes specially designed to crash consensus mechanism properties. Leslie Lamport [34] identified and characterized as the Byzantine General's Problem.

Considering the importance of consensus mechanism in Blockchain implementations, all the three properties are essential for any consensus protocol. However, it is agreed by many researchers [35] that all three properties can't be achieved at one time. A deterministic asynchronous consensus mechanism can possibly achieve at most of two out of three properties and compromise on at least one of them. It is not a random task to select two properties and compromise on one, but it entirely depends on application requirements. Fault tolerance can't be compromised because it is the most important property [33] for any blockchain implementation. Therefore, the nature of application is to decide which property to let go of, either on liveness or safety. For instance, Raft [36], Paxos [37], view-stamped replication used consensus protocol that take fault tolerance and safety and let go the liveness. Bitcoin [2], Ethereum [38], Ripple [39], stellar [40] and other cryptocurrencies chose fault tolerance and liveness and sacrifice on the safety.

### III. RELATED WORK

Nakamoto launched Bitcoin in 2008 [2] with its secured intense success in the field of cryptocurrency. Therefore, many similar currencies have been launched in the following years. There are 2017 cryptocurrencies available on internet by 2019 [3] with different business models. Besides global cryptocurrency hype, Bitcoin holds the highest market capitalization of up to 53%. Blockchain is serving as fundamental technology behind Bitcoin. It aims to influence almost every industry. Its application is not restricted to only financial eco-system [3] but it is set to revolutionize the politics, healthcare, and society science arena [41].

The consensus protocol is the main and core component of Blockchain technology, and it plays a vital role in Blockchain for its success as global emergence and disruptive technology. Nguyen and kin [42][43] recommend in their respective research to categorize the Blockchain consensus mechanism into two major groups. Proof Based and Voting Based consensus mechanism. Proof-based consensus mechanisms are mostly used in permissionless Blockchain in which anyone is free to join and leave at any time they want. They are supported by the several cryptographic techniques and the incentive-based design. Moreover, this group of consensus mechanism, offer comparatively better support for nodes scalability but the on the cost of performance which includes the throughput and latency. In proof based consensus model performance of Blockchain compromised with increasing size of network. Whereas, voting based consensus model mostly utilized in permissioned Blockchain. It offers quick consensus finality which eventually bring high number throughput [44]. In the voting based consensus model nodes communicate with each other, due to high communication

complexity it doesn't support large network and restricted to small network.

Bitcoin uses Proof of work consensus protocol. Therefore, it has attracted wide research interest in last two decades. Due to the complex block mining process, it consumes huge amount energy and require other specialized equipment do intensive mathematical computation. Therefore, it is also referred as resource hungry and energy inefficient and eventually, it offers low throughput and high latency. Moreover, most important concern of research community in PoW is limited scalability, it only supports seven transaction per second (TPS) which is entirely not acceptable in business real world application. Firstly, Proof of stake (PoS) was presented at Bitcoin community forum later Ethereum adopted it. It was proposed to provide ease in block mining and reduce high wastage of energy in PoW and referred as energy efficient variant of PoW. This new idea changed entire Block mining concept, so the expensive and extremely powerful equipment's are no longer needed for block mining. However, miners (nodes) are required to hold and show stake in the form of certain number of coins. The node holding high stake has more chances to become block producer and earn the reward. Apparently, it certainly saves more energy as comparison to PoW but there are different attacks arises such as nothing at stake problem. Ethereum only support 15 transaction per second (TPS) which is also very low in comparison with other mainstream application. There is another proposed alternate, proof of space it strives to utilize physical storage resources as a substitute of computational power in PoW [45] [22].

Proof of Coin Age [46] support the same mechanism as proof of stake. Where nodes are needed to show the ownership of certain amount currency for performing the virtual mining. Proof of activity [47] create the mining lottery of every node own the number of coins. The lottery winner will produce the block and claim its reward by signing message within interval of time. Intel proposed proof of elapsed time [48] and which has been implemented in HyperLedger project. Proof of elapsed time are required to use the Intel SGX supported CPUs for performing the online voting via random sleeping time. Researcher tried to address above discussed limitations with various new consensus mechanism and approaches, which do not require energy intensive mining, and reduce the energy consumption and increase throughput, For example proof of space [49], Proof of Authority (PoA), Proof of luck [21].

Besides all the approaches, there is another emerging area for Blockchain consensus model but unfortunately least investigated. Reputation based consensus mechanism. This area intended to make every node accountable on every transaction and return power to the nodes as whole.

A recent published study proposed the Proof of Reputation (PoR) [50] in which reputation would be served as the incentive for nodes positive behavior, time, utilized energy as well as block publication rather than the coins. Therefore, mining node are no longer required in this technique. The lab-based simulation proved that it can be scaled up to the thousand nodes with processing capacity of more than hundreds of transactions (TPS). Reputation scheme [51]

designed on the similar concept of PoR. It involves both honest nodes as well as malicious nodes together in the positive manner. It rewards the good behavior as reputation and, also proposed the punishment factor in the revenue payment function of reputation. Therefore, the cooperative behavior would be rewarded, and non-cooperative behavior would be punished. The implementation of this reputation-based incentive module on state-of-the-art PoX protocol can achieve better results than usual. Another protocol Proof of QoS [52] designed on the similar idea of reputation, where good quality of service would be encouraged. Mostly it has been used in permissionless Blockchain. In this protocol, the whole network would be categorized into small group and each group will nominate a node based on its quality of service, then the consensus would be achieved in between the nominated nodes with Byzantine Fault Tolerance (BFT). The architecture of Proof of QoS has entirely based a hybrid protocol, where it utilizes Proof-of-QoS to select nodes for running BFT-style consensus.

Proof of X-repute protocol designed for Blockchain enabled - IoT systems [53] it introduced new module of repute method and to illustrate the potential of repute that it can be utilized to manage the integrity of consensus protocol. The reward and punishment in the repute method sets the nodes repute values; the nodes behavior would either be rewarded or punished which certainly impact the security and integrity of consensus protocol. Another study proposed Blockchain Reputation based consensus (BRBC) [54] protocol for private blockchain networks. In this protocol network sets a trust threshold level and all nodes are supposed to secure higher reputation score than trust threshold for getting a chance to append a new block in the chain. Moreover, miner (nodes) activities are monitored by randomly selected judges and they sign their reputation score based on their behavior. Judges will reward good and cooperative behavior whereas punishment factor also included on the malicious and non-cooperative behavior.

In one study reputation integrated as module ReCon [55] in which external reputation system has been integrated with Blockchain consensus protocol to achieve scalable permissionless consensus protocol. Where it utilizes external reputation ranking mechanism as input to rank the nodes. Node ranking would be done based on the result of consensus rounds performed by small committee. Therefore, current reputation would be used to select the committee. Delegated Proof of Reputation [56] designed to replace coin-based stake with the reputation ranking system. The reputation system developed on design of famous ranking theories (PageRank, NCD aware Rank and HodgeRank). RepuCoin [57], uses miner reputation as its strength as key function of its work and energy integrated over the time of complete Blockchain rather than immediate computational power with possibility of borrowing, temporarily and rapidly. Whereas the reputation would be earning with the span of time. RepuCoin claims that it will tolerate 51% attack and put limits on the rate of voting power growth of the entire system.

## IV. PROTOCOL DESCRIPTION

### A. Important Definition

- **Block:** A block is the main data structure of Blockchain. It consists of Block header and list of transaction, Block header containing metadata i.e., timestamp, Prev\_Hash, Merkle tree etc. Like figure print, Hash is the unique identity of every block and it is identified with its hash. The prev\_Hash in the metadata of every block is to connect the prior block and this series of chronologically connected blocks forms chain.
- **Genesis Block:** The first Block in the Blockchain is referred as Genesis Block. Therefore, the previous hash must be equivalent to zero because there is no block before it. If you start from any block and following the chronologically chain backward you will reach at genesis block.
- **Round:** The round is a set of five steps to achieve consensus. At the end of round, a block supposed to be added into both chains i.e., transaction chain as well as review chain.
- **Nominated Round leader (NRL):** Nominated Round leaders are the nodes selected based on their behavior in the network and sentiment analysis of the review with NLP algorithm. In every round top three nodes with highest positive reviews will be selected as NRL. Initially every node strives to become NRL and get a chance to become round leader. To become an NRL it is required to meet minimum criteria which is the node should not be currently blacklisted and minimum positive reviews.
- **Round Leader:** Round Leader is node with highest positive reviews selected from NRL or the most trustworthy node selected from NRL. RL will only be selected from list NRL. A new RL will be selected for every round to propose a block, and the selection process is independently done through an NLP algorithm. To become RL it is required to meet minimum criteria which is node should not be blacklisted and minimum positive reviews.
- **Step verifier (SV):** Step verifiers are the set of nodes independently selected on the basis on their behavior and availability in the network. A new set of SVs are selected for every step in the consensus process and each SV are tasked to perform different activities to contribute to each step in the round. Each step verifier is required to meet a minimum review and not currently blacklisted.

### B. Overview

The core idea behind the proposed Proof-of-Review consensus protocol is to allow and therefore to give power to each node to post reviews and rating in the form of stars for every other node. Nodes are required to maintain their good and positive behavior consistently to secure positive reviews from other nodes, and those reviews will eventually become their trust value in the network. The trust value cannot be bought, spent, or shared but it can only be earned with good

and positive behavior. The node with more positive reviews will be considered more trustworthy in the network. The most trustworthy node will get higher chance to publish a new block.

- If node maintain a good and positive behavior, it will receive a good and encouraging feedback/review and which eventually increase their trust value in the network.
- If node act maliciously, selfishly, it will get negative feedback/review, and which decrease the trust value in the network.

The proposed model works on a 2-chain architecture. There would be 2 parallel chains – the first chain as usual will store the transactions and referred as transaction chain whereas the other chain is designed to store the reviews given by nodes and referred as Review Chain.

To achieve the proposed protocol, we will answer following questions:

*C. Question 1: In this Model, How to keep Ledger and Review Consensus?*

As Bitcoin uses the PoW consensus protocol, which strives to allow entire network of nodes to agree on every single block in the chain. The first node that has solved the computationally intensive puzzle secure the right to publish the block, while remaining nodes will be allowed to take part in Block verification. Similarly, in Proof-of-Review (PoRv), the node with most positive reviews will get a chance to publish the Block. Positive reviews from other nodes will eventually become their trust value, which means the most positive reviews means more trustworthy and vice versa. And the block verification is open for all other nodes. Since PoRv protocol work on the 2-chain architecture, a Transaction chain and Review chain, therefore every node is required to agree on both the transaction and the review block.

*D. Question 2: How to Produce Block through PoRv*

The response of this concern will be like Bitcoin, it utilized the proof of work consensus protocol, in which the node solves the mathematical puzzle before all other nodes will get a chance to publish the next Block in the Blockchain while other nodes will verify the block. In PoRv protocol, the node with most positive review (which eventually becomes the trust value), will generate and publish a new block while other nodes can verify the block. Every node is required to maintain the good behavior consistently because any bad review will cause a reduction in the trust value.

*E. Question 3: How to Encourage other Nodes to Publish Block*

There is no reward or incentive in this model for publishing new block as comparing to cryptocurrencies like Bitcoin and Ethereum. In this model we are giving power back to every node in the network. This is to empower every node to rate and to post reviews on others' behavior in the network. Those reviews will become trust value or trustworthiness of a node which cannot be bought, spent, and transferred but the only way to earn trust value is to stay honest and with good

behavior consistently. Nodes with highest positive reviews reflects the high trust value and comparatively offer better services as well as not likely to attack the system. In every round only one node with highest trust value will be selected as Round Leader and publish the block. Publishing a block will certainly help to get more positive reviews from other nodes which eventually increase the trust value.

In each round the PoRv execute the following task. A round starts with a transaction and ends with new Block being added to Ledger.

- Step # 1. Select Nominated Round Leader (NRL)

All online nodes appear to be Potential Round Leader (PRL) and get a chance to become Nominated Round Leader (NRL). The restriction of minimum trust value and not to be blacklisted will be applied to all nodes in the network. Each PRL will evaluate their own reviews (text format).

The evaluation calls on the Natural Language processing (NLP) to evaluate the text to determine a trust value. Then, the trust value will be compared against their rating. The PRL's trust and rating should be identical with negligible difference otherwise the node will be blacklisted with status involved in "Malicious Activity" for current round.

Top 3 nodes with highest positive Reviews/trust value out of all PRL will be selected as Nominated Round Leader (NRL). NRL will propagate a message using GOSSIP protocol to all other nodes in the network which includes their (NRL) trust value and their hashed credentials.

- Step # 2. Select Round Leader

All nodes in the network will listen message a from NRL from Step 1.

Nodes with highest online time will be identified and selected as "Step Verifier". (Other nodes which are not selected as Step Verifier, they need stay online for next step to be selected as Step Verifier). The restriction of minimum trust value and not to be blacklisted will be applied to each "Step Verifier".

Each SV will wait certain amount to time (System defined duration) to receive the messages from 3 NRL (from Step 1). NRL are selected with condition to be online, there are less changes of no message.

SV will re-evaluate reviews of each NRL. If results are identical with received, the minor difference is negligible. The node with highest trust value will become a Round Leader (RL) and other 2 nodes will remain Nominated Round Leader (NRL) and stay in a queue.

If re-evaluation results are not identical for node with a highest trust value, then that particular node will be blacklisted with status involved in "Malicious Activity" and re-evaluation will be done for next node from NRL and process goes until the RL is selected.

SV will propagate a message using GOSSIP protocol to all nodes in the network which includes the RL recommendation and its trust value.

- Step # 3. Propose a Block

All nodes will listen message from SV from Step 2.

Nodes with highest online time will be identified and selected as "Step Verifier". The restriction of minimum trust value and not to be blacklisted will be applied to each "Step Verifier". SV will wait maximum amount of time (System defined duration) to receive the minimum number of messages (from Step 2) for RL recommendation and its review number (SV are selected with condition to be online, there are less chances of no message.).

SV will re-evaluate the reviews of RL and compare it with the one received in the message from Step 2. If result is identical only then the process will move on otherwise RL will be blacklisted and it goes back to Step 2 and select a new RL from the remaining NRL.

If all go well, the RL will assemble a block and add transaction from its transaction poll until the block size hit. RL will technically verify the Transaction (e-signature) and sign a Block.

RL will prorate a message which includes its RL trust value as a Signed Block.

- Step # 4. Block Verification

All nodes will listen message from SV from Step 3.

Nodes with highest online time will be identified and selected as "Step Verifier". The restriction of minimum Review Number and not to be blacklisted will be applied to each "Step Verifier". SV will wait maximum amount of time (System defined duration) to receive the message From (from Step 3) the Signed Block and its trust value.

SV will re-evaluate reviews of RL and compare with the one received in the message from Step 3. If result is identical the process will move on otherwise RL will be blacklisted and it goes back to Step 2 and select a new RL from remaining NRL.

Each SV seeks to verify and validate the block and its associated transactions. Each SV will iterate over transactions in the block. With each transaction, every SV will evaluate the transaction by processing it into its VERIFY () function. The verify function will either return a Yes or No. "YES" means Transaction is good and "NO" means Transaction is bad. If it returned Yes, and remaining technical checks are good (e.g e-signature), SV will move to next transaction. Once all the transaction are verified and validated as good and no disagreement found, each SV will propagate a message with vote in continuance of this RL and Block and its trust value.

Verify – Another parameter will also be part of message, YES/NO depending on the number of votes in confidence. YES, when the number of votes in confidence meets minimum threshold value and vote is still in agreement for a leader. Otherwise, if it is No for any transaction, it is considered a bad transaction. This disagreement will allow verifier to conclude the RL evaluation is bad and consequently the RL is acting maliciously and Blacklisted and it goes back to Step 2 and select a new RL.

- Step # 5. Block Decision

All nodes will listen message from SV from Step 4.

Nodes with highest online time will be identified and selected as "Step Verifier". The restriction of minimum trust value and not to be blacklisted will be applied to each "Step Verifier". SV will wait maximum amount of time (System defined duration) to receive the minimum number of messages (from Step 4) for Verify value YES. (SV are selected with condition to be online, there are less changes of no message.).

SV will re-evaluate reviews of RL and compare with the one received in the message from Step 4. If result is identical the process will move on, otherwise RL will be blacklisted, and it goes back to Step 2 and select a new RL from NRL.

Each SV will come to a final decision on the Block. SV are listening to messages that includes a signed value Yes or No in addition to the vote of confidence to Round Leader and a Block. If they receive the maximum number messages containing Yes along of the vote of confidence to RL and a Block, SV will approve the Block and the same block is supposed to be broadcasted to all other nodes.

## V. BLOCK STRUCTURE

This consensus protocol is entirely dependent on the community (other nodes) reviews. It is essential to store the reviews whose legitimacy is verified by all other nodes. Therefore, in the proposed protocol, there would be 2 parallel chains. First chain will store the transactions and referred as Transaction chain whereas the other chain is designed to store the reviews given by step verifiers and it is referred to as Review Chain shown in Fig. 2.

The block structure of the first chain would be as usual as in conventional Blockchain, which is separated into 2 parts. Block header and list of transaction. Block header contains the version, prev\_hash, timestamp, nonce, Merkle root, transaction parts contain the transaction only. The structure is illustrated in Fig. 3.

Whereas the Block structure for review chain is a bit different. It is also divided into two parts, Block header and Review Transaction. Blockheader contains the version, previous hash, timestamp, merkel root, hash of the transaction Block. Therefore, both the chains are linked with each other but carrying different information. The review transaction part contains the list of reviews and public keys of the node that have written the review. The structure is illustrated in Fig. 4.

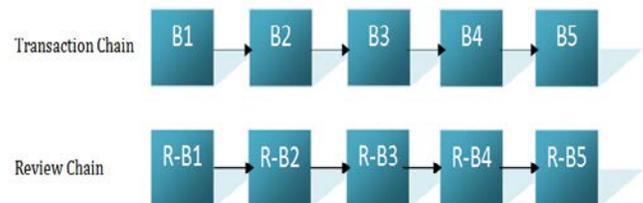


Fig. 2. 2 Parallel Chain Architecture.

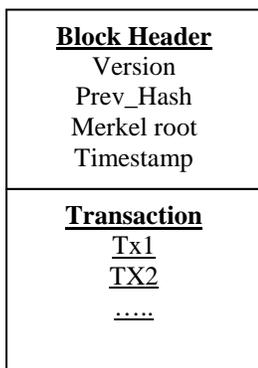


Fig. 3. The Block Structure of Transaction Chain.

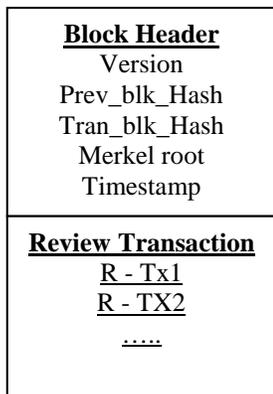


Fig. 4. The Block Structure of Review Chain.

The Fig. 5 explains the complete workflow of the proposed protocol system. Basically, there are two parallel chains. This system works in round structure, where in each round a new Round Leader will be selected. The Round Leader will be responsible to generate two blocks in one round, the transaction Block, and the Review Block and both blocks would be linked to each other. Initially, RL generates the transaction Block after successfully achieving the consensus then Step verifier will be allowed to post their reviews and ratings. Consensus will also be achieved on the reviews. Then the RL generates the Review Block which will hold the hash of transaction Block. For the next round, the new RL will be selected from the latest Review Block, and Block generation process will continue.

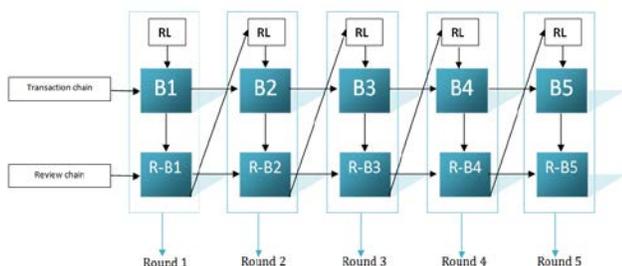


Fig. 5. The Complete Workflow of PoR Consensus Protocol.

## VI. SECURITY ANALYSIS

We presume the communication between the nodes in the network are set up through a reliable peer-to-peer network but there are chances it can still be damaged by selfish behavior, malicious attack, or node failure. This section will discuss some potential attacks in peer-to-peer networks and specially in trust-based protocols and strategies to address them efficiently without damaging the network.

Following are several potential attacks [20] and strategy to address them.

- **Bad-mouthing attack:** In this attack, malicious nodes want negatively to influence other node's trust value. Therefore, they deliberately and continuously give bad/negative reviews to one or all nodes to undermine their trust value or defame the good nodes. which eventually help them level up their trust level.

In our model, reviews are associated with the step verifiers, and new step verifiers are selected on every step in the consensus process. Moreover, the reviews will be analyzed with strong NLP algorithm which confirm the date and time of the reviews and the sentiments. The NLP algorithm will not count any malicious review or any review with malicious doubt therefore it would not affect the system.

- **Camouflage attack:** In this attack, malicious nodes show of the honest and good behavior to secure positive reviews which increase its trust value. Once they got required trust value, they randomly attack the system. The prefix "non" is not a word; it should be joined to the word it modifies, usually without a hyphen.

In our model, there are two chain architecture, it stores reviews of every node in the separate chain. A NLP algorithm measure the trust level and ensures the legitimacy of every review on every step of consensus process. Therefore, any random malicious act will be easily detected, and malicious node will be blacklisted right away.

- **Sybil Attack:** This attack has been discussed in almost all consensus Model. In this attack, malicious node creates multiple account. if one account gets defame by getting negative review and acting maliciously, it quickly switches to other account and start.

In our model, every node needs to earn positives review consistently, if a malicious node switches new account, so it wouldn't be able to hurt because it needs a minimum trust value to participate in consensus process which make it to act honestly, and it wouldn't cost effect to create a new account every now and then.

- **On-off attack:** In this attack, the attacker shows mix of behaviors, good as well as bad alternatively. In order to get mix reviews therefore remain undetectable and occasionally cause damage.

In our protocol, there are two chains architecture, a separate chain is recording the reviews of every node in the network and NLP algorithm measure the overall trust level and analyze the legitimacy of every node in the step verifiers on every step in the consensus process. Therefore, any On-off attack can be easily reported.

The reason for attackers to attack the system is 2-fold, they want to downgrade other nodes' trustvalue to push up their trust in the network to get more chances to perform malicious actions. Other reason could be they want to damage the system. Our model discourages any kind of malicious activity and provide equal opportunities to all nodes to earn more positive reviews and increase their trust value in the network. It entirely works on the other node's reviews and the nodes trust value to make every node act and behave honestly and consistently.

### VII. PRELIMINARY RESULTS

This section will discuss the Proof of concept (PoC) for evaluating reviews which is done on by performing the sentiment analysis of reviews (Text) through NLP. Therefore, we used freely available on the standard Kaggle dataset. It consists of reviews (tweets) for six US based airlines. The tweet is the mix of positives, negative and neutral. However, our focus was on the positives and negative. The analysis was done on those tweets to find the most trustworthiness of airlines and exactly sample idea would be replicated in the proposed system.

Sentiment analysis is performed to analyze the feeling and opinion about anything i.e., Text or image. Basically, it is used for decision making when you have multiple choices and you need to select the most reliable.

A simple program has been written in python programming language using multiple NLP libraries and all the coding work has been done on Jupyter Notebook.

The Fig. 6 illustrates the sentimental analysis of tweet for six US based airlines those are United, US airways, Southwest, Delta, Virgin America. The analysis is measured either positive and negative and the neutral category is discarded for this evaluation. In the figure x-axis presents the number of reviews (tweets) and y-axis shows the airlines. The figure illustrates comparatively their high number of negative and less positive for all the airlines.

However, our focus is on the positives, and the southwest got the highest number of positive tweets and followed by the Delta and the United.

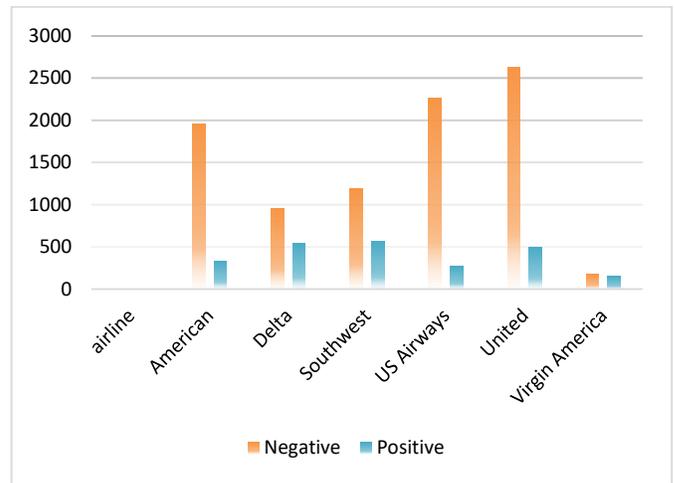


Fig. 6. Sentimental Analysis of Tweet for 6 US based Airlines.

### VIII. CONCLUSION

To conclude, we propose a new PoRv consensus protocol to make blockchain more efficient, reliable, and scalable. In this protocol, we are utilizing the trustworthiness of node by empowering every node to post reviews for every other node on their previous behavior within the network. The trust may include the previous transactions and interaction with other nodes. An NLP algorithm is used to analyze the reviews and to calculate the trust value of every node. The trust value will be linked to every node to efficiently select the round leader node and that will increase the throughput with less latency. Node with most positive reviews will be selected as the round leader and can publish new block to earn more positive reviews. The proposed protocol is designed on a 2-chain architecture that both chains are cryptographically linked to each other. The first chain is utilized to store the transaction whereas the second chain is used to store the reviews. The proposed system is found to be tolerant to some major attacks such as Sybil attack, bad-mouthing, and on-off attack.

### IX. FUTURE WORK

The in-depth/detailed investigation and experiments of the proposed protocol is ongoing. The separate blockchains are in the development phase based on the PoRv consensus protocol. Experiment/simulation are to be used to validate and verify the proposed protocol. The implementation and experiments on the proposed PoRv shall be published in the future papers.

### ACKNOWLEDGMENT

This study is conducted in Universiti Teknologi PETRONAS (UTP) as "Generic Consensus Model for Improving Nodes Syndicating Performance in Blockchain" under the Fundamental Research Grant Scheme (FRGS) from the Ministry of Higher Education (MOHE) Malaysia.

REFERENCES

- [1] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," in Conference on the Theory and Application of Cryptography, 1990: Springer, pp. 437-455.
- [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, 2019.
- [3] A. Tapscott and D. Tapscott, "How blockchain is changing finance," Harvard Business Review, vol. 1, no. 9, pp. 2-5, 2017.
- [4] Z. Hess, Y. Malahov, and J. Pettersson, "Eternity blockchain," [Online]. Available: <https://aeternity.com/aeternity-blockchainwhitepaper.pdf>, 2017.
- [5] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare: MedRec" prototype for electronic health records and medical research data," in Proceedings of IEEE open & big data conference, 2016, vol. 13, p. 13.
- [6] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), 2016: IEEE, pp. 25-30.
- [7] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, no. 10, pp. 1-8, 2016.
- [8] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," Procedia computer science, vol. 98, pp. 461-466, 2016.
- [9] P. Bylica, L. Glen, P. Janiuk, A. Skrzypczak, and A. Zawlocki, "A Probabilistic Nanopayment Scheme for Golem," ed, 2015.
- [10] P. Hurich, "The virtual is real: An argument for characterizing bitcoins as private property," Banking & Finance Law Review, vol. 31, no. 3, p. 573, 2016.
- [11] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 2017: IEEE, pp. 618-623.
- [12] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 983-994, 2017.
- [13] J. Sun, J. Yan, and K. Z. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," Financial Innovation, vol. 2, no. 1, pp. 1-9, 2016.
- [14] X. Xu et al., "The blockchain as a software connector," in 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), 2016: IEEE, pp. 182-191.
- [15] E. Nordström, "Personal clouds: Concedo," ed, 2015.
- [16] J. S. Czepluch, N. Z. Lollike, and S. O. Malone, "The use of block chain technology in different application domains," The IT University of Copenhagen, Copenhagen, 2015.
- [17] D. Shift, "Technology tipping points and societal impact," in World Economic Forum Survey Report, available at: [http://www3.weforum.org/docs/WEF\\_GAC15\\_Technological\\_Tipping\\_Points\\_report\\_2015.pdf](http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf) (last accessed 20.08. 2018), 2015.
- [18] A. Yeow, "Global Bitcoin Nodes Distribution," URL: <https://bitnodes.earn.com/> (accessed 08 November 2018), 2015.
- [19] K. Croman et al., "On scaling decentralized blockchains," in International conference on financial cryptography and data security, 2016: Springer, pp. 106-125.
- [20] B. Obama, "The White House: Office of the Press Secretary," Presidential Studies Quarterly, vol. 39, no. 3, p. 429, 2009.
- [21] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in proceedings of the 1st Workshop on System Software for Trusted Execution, 2016, pp. 1-6.
- [22] S. Park, A. Kwon, G. Fuchsbaauer, P. Gaži, J. Alwen, and K. Pietrzak, "Spacemint: A cryptocurrency based on proofs of space," in International Conference on Financial Cryptography and Data Security, 2018: Springer, pp. 480-499.
- [23] B. Curran, "What is Proof of Elapsed Time Consensus?(PoET) Complete Beginner's Guide," ed: Accessed: Mar, 2019.
- [24] M. Correia, G. S. Veronese, N. F. Neves, and P. Verissimo, "Byzantine consensus in asynchronous message-passing systems: a survey," International Journal of Critical Computer-Based Systems, vol. 2, no. 2, pp. 141-161, 2011.
- [25] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, vol. 107, pp. 841-853, 2020.
- [26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE international congress on big data (BigData congress), 2017: IEEE, pp. 557-564.
- [27] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in proceedings of the 50th Hawaii international conference on system sciences, 2017.
- [28] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, 2014.
- [29] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, "Consortium blockchains: Overview, applications and challenges," International Journal On Advances in Telecommunications, vol. 11, no. 1&2, pp. 51-64, 2018.
- [30] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in Proceedings of the 2017 ACM International Conference on Management of Data, 2017, pp. 1085-1100.
- [31] C. Hammerschmidt, "Consensus in blockchain systems," URL <https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe>, 2017.
- [32] K. Yeow, A. Gani, R. W. Ahmad, J. J. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues," IEEE Access, vol. 6, pp. 1513-1524, 2017.
- [33] A. Baliga, "Understanding blockchain consensus models," Persistent, vol. 4, pp. 1-14, 2017.
- [34] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in Concurrency: the Works of Leslie Lamport, 2019, pp. 203-226.
- [35] N. A. Lynch, M. J. Fischer, and R. Fowler, "A Simple and Efficient Byzantine Generals Algorithm," Georgia Inst of Tech Atlanta School of Information And Computer Science, 1982.
- [36] D. Middleton, "Hyperledger's Sawtooth Lake Aims at a Thousand Transactions per Second," ed, 2017.
- [37] C. Gutierrez, "Hyperledger's Sawtooth Lake Aims at a Thousand Transactions per Second," ed: March, 2017.
- [38] V. Buterin, "What is Ethereum?," Ethereum Official webpage. Available: <http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html>, 2016.
- [39] A. Harðarson, "Can Ripple disrupt the global payments market?," 2018.
- [40] D. Mazieres, "The Stellar Consensus Protocol," A Federated Model for Internet-level Consensus. Version July, vol. 14, 2015.
- [41] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, 2016.
- [42] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," Journal of Information processing systems, vol. 14, no. 1, pp. 101-128, 2018.
- [43] J. Bou Abdo, R. El Sibai, K. Kambhampaty, and J. Demerjian, "Permissionless reputation-based consensus algorithm for blockchain," Internet Technology Letters, vol. 3, no. 3, p. e151, 2020.
- [44] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in International workshop on open problems in network security, 2015: Springer, pp. 112-125.
- [45] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in 2014 IEEE Symposium on Security and Privacy, 2014: IEEE, pp. 475-490.

- [46] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," self-published paper, August, vol. 19, p. 1, 2012.
- [47] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," ACM SIGMETRICS Performance Evaluation Review, vol. 42, no. 3, pp. 34-37, 2014.
- [48] D. Khan, L. T. Jung, M. A. Hashmani, and A. Waqas, "A Critical Review of Blockchain Consensus Model," in 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2020: IEEE, pp. 1-6.
- [49] S. Park, K. Pietrzak, J. Alwen, G. Fuchsbauer, and P. Gazi, "Spacecoin: A cryptocurrency based on proofs of space," IACR Cryptology ePrint Archive, vol. 2015, p. 528, 2015.
- [50] F. Gai, B. Wang, W. Deng, and W. Peng, "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network," in International Conference on Database Systems for Advanced Applications, 2018: Springer, pp. 666-681.
- [51] E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan, "PoRX: A reputation incentive scheme for blockchain consensus of IIoT," Future Generation Computer Systems, vol. 102, pp. 140-151, 2020.
- [52] B. Yu, J. Liu, S. Nepal, J. Yu, and P. Rimba, "Proof-of-QoS: QoS based blockchain consensus protocol," Computers & Security, vol. 87, p. 101580, 2019.
- [53] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. K. Khan, "Proof of X-repute blockchain consensus protocol for IoT systems," Computers & Security, vol. 95, p. 101871, 2020.
- [54] M. T. de Oliveira, L. H. Reis, D. S. Medeiros, R. C. Carrano, S. D. Olabarriga, and D. M. Mattos, "Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications," Computer Networks, vol. 179, p. 107367, 2020.
- [55] A. Biryukov and D. Feher, "ReCon: Sybil-resistant consensus from reputation," Pervasive and Mobile Computing, vol. 61, p. 101109, 2020.
- [56] T. Do, T. Nguyen, and H. Pham, "Delegated proof of reputation: A novel blockchain consensus," in Proceedings of the 2019 International Electronics Communication Conference, 2019, pp. 90-98.
- [57] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo, "Repucoin: Your reputation is your power," IEEE Transactions on Computers, vol. 68, no. 8, pp. 1225-1237, 2019.
- [58] Khursheed, S., Jeoti, V., Badruddin, N., & Hashmani, M. A. (2020, July). Low complexity Phase-based Interpolation for side information generation for Wyner-Ziv coding at DVC decoder. In 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP) (pp. 1-6). IEEE.

# Movement Control of Smart Mosque's Domes using CSRNet and Fuzzy Logic Techniques

Anas H. Blasi<sup>1</sup>, Mohammad Awis Al Lababede<sup>2</sup>, Mohammed A. Alsuwaiket<sup>3</sup>

Computer Information Systems Department, Mutah University, Al Karak, Jordan<sup>1</sup>

Computer Science Department, Mutah University, Al Karak, Jordan<sup>2</sup>

Computer Science and Engineering Technology Department, Hafar Batin University, Hafar Batin, Saudi Arabia<sup>3</sup>

**Abstract**—Mosques are worship places of Allah and must be preserved clean, immaculate, provide all the comforts of the worshippers in them. The prophet's mosque in Medina/ Saudi Arabia is one of the most important mosques for Muslims. It occupies second place after the sacred mosque in Mecca/ Saudi Arabia, which is in constant overcrowding by all Muslims to visit the prophet Mohammad's tomb. This paper aims to propose a smart dome model to preserve the fresh air and allow the sunlight to enter the mosque using artificial intelligence techniques. The proposed model controls domes movements based on the weather conditions and the overcrowding rates in the mosque. The data have been collected from two different resources, the first one from the database of Saudi Arabia weather's history, and the other from Shanghai Technology Database. Congested Scene Recognition Network (CSRNet) and Fuzzy techniques have applied using Python programming language to control the domes to be opened and closed for a specific time to renew the air inside the mosque. Also, this model consists of several parts that are connected for controlling the mechanism of opening/closing domes according to weather data and the situation of crowding in the mosque. Finally, the main goal of this paper has been achieved, and the proposed model has worked efficiently and specifies the exact duration time to keep the domes open automatically for a few minutes for each hour head.

**Keywords**—Artificial intelligence; CNN; CSRnet; fuzzy logic; fuzzy control

## I. INTRODUCTION

Islam is the second largest religion after Christianity in the world, according to a study conducted in 2015 [1], Islam has 1.9 million followers in the world, representing 24.8% of the world's population.

Modern technology has become an influencing factor in our lives and has reached a stage that we cannot do without because it has become a common factor in the affairs of our lives in general. Among the most important aspects of the spread of technology in the modern era are techniques of artificial intelligence that stimulate the process of automating all areas of life to make it easier, faster, and more intelligent in adapting to the tremendous development that we are witnessing from time to time, as it has become an essential element in the field of learning, working, providing services, agriculture, trade, industry, and many others, which helped to improve results desired and achieving great benefits for employers with less time, effort and cost.

Here comes our role as scientists to support the techniques of artificial intelligence to employ them as much as possible, so this paper considered using these technologies to solve the problem of overcrowding in mosques. The Islamic religion is considered the second most widespread religion in the world after the Christianity religion [1], and it is distinguished by special rites distinct from other religions, the most important of which is prayer, especially collective prayer in mosques, which means they need for mosques to spread in line with the large numbers of worshipers and provide a comfortable and clean place to perform the prayer Easily and conveniently. There are four million mosques scattered around the world [2] and it is equipped with the best hygiene and health protocols and this is what makes it one of the cleanest places in the world to perform Muslim prayers. Among the most important of these mosques:

- Al Masjid Al Haram [3]: It has high importance and priority for Muslims, located in Makah Al-Mukarramah/ Kingdom of Saudi Arabia, it is the qibla of the Muslims and there is the honorable Kaaba which Muslims visiting it from all parts of the world to perform the Hajj and Umrah and one prayer in it equal to one hundred thousand prayers in other mosques.
- The Prophet's Noble Mosque [3]: No less important than its predecessor, where the Messenger of the Nation of Islam, Muhammad (peace and blessings of God be upon him) lived and was buried there with two of his companions (Omar and Abu Bakr - may God be pleased with them both) - located in Medina / Kingdom of Saudi Arabia, it is frequented by Muslims from all over the world to visit the tomb of the Prophet and the prayer in it is equivalent to 1000 prayers in others.

In this paper, the focus will be on the Prophet's Noble Mosque as a model that can be converted into a smart mosque, being one of the largest mosques in the world and the second holiest site in Islam after Al-Masjid Al-Haram in Mecca, which is the mosque that the Prophet Muhammad built in Medina after his migration in 1 Hijra next to his house [4]. The mosque has gone through several expansions throughout history, as it now covers 98,327 square meters for the building and 235,000 square meters for the surrounding squares [4], which can accommodate approximately 698,000 worshipers, and its expansion is ongoing to reach a capacity of 2.5 million worshipers [5]. The mosque building has many domes: the

green dome (main dome), 170 gray dome, and 27 moving domes, in addition to 10 minarets.

As noted above, the mosque accommodates a huge number of worshipers, this means that an appropriate environment of moderate temperature and humidity must be provided to help prevent the spread of some viruses such as Coronavirus, especially that the mosque contains carpets, which is an appropriate environment for their transmit, which may cause the transmission of infections to worshipers, and also it can be noted that the mosque contains 27 moving domes, so it is possible to use these domes to achieve the goal of this paper, which is to improve the quality of air and humidity in the Holy Prophet's Mosque by controlling the opening of domes to replenish the air and the sunlight entering the mosque building using Congested Scene Recognition Network (CSRNet) and Fuzzy techniques based on temperature and the number of worshipers in the mosque without the need for human intervention in this process.

The idea came to address a problem in previous research [6], as domes were opened depending on some weather factors, but a problem with temperature was observed so that domes did not open unless the temperature was between ( $16^{\circ}$ - $27^{\circ}$ ), and given the extremely volatile climate in Medina, in case of high temperatures (more than  $27^{\circ}$ ), the domes will remain closed even if the mosque needs ventilation, and also in very cold weather (less than  $16^{\circ}$ ), it will remain closed, but in this paper, the number of worshipers was inserted to improve the work of domes in the required ventilation.

The paper has organized as follows: Section II reviews the related work. Section III describes the materials and methods used to build the proposed model. Section IV discusses the results in detail. Finally, Section V discusses the conclusions and draws the future work.

## II. RELATED WORK

As mentioned earlier, this research is an extension of a previously published paper [6] that aims to solve the problem of ventilation, allow sunlight to enter the mosque, and provide comfort for the worshipers, especially in times of congestion in mosques and the solution was by building a model for smart mosque domes using weather features and outside temperatures. Machine learning algorithms such as k-Nearest Neighbors (kNN) and Decision Tree (DT) were applied to predict the state of domes (open or close). The experiments of this paper were applied to the Prophet's Mosque in Saudi Arabia, which mainly contains twenty-seven hand-moved domes. Each of the machine learning algorithms was tested and evaluated using different evaluation methods. After comparing the results of both algorithms, the DT algorithm achieved 98% higher accuracy compared to 95% accuracy for the k-NN algorithm. The problem with this paper was in the element of temperature, as the domes do not open except in the area ( $16^{\circ}$ - $27^{\circ}$ ), even if the mosque needs ventilation.

In [7] a neural network has been proposed to discover crowded scenes called (CSRnet) as it is one of the deep learning methods that can understand the very crowded scenes and make an accurate estimation of the count, consisting of two layers: a neural network as a front face and an expanded

network for the back end, the authors made experimentations on four groups of images: (Shanghai Tech, WorldExpo 10, UCFCC50, UCSD), the results were so high that they reduced the error by 47.3% while improving by 15.4% compared to the previous methods that were applied to the same group of images.

The author in [8] presented a conceptual model for heating and controlling air conditioning inside the home by applying the principle of fuzzy logic, microprocessors associated with sensors were used to sense the factors affecting ventilation in addition to a compressor and an air circulation fan, all of which were installed inside a building for testing. The proposed model aims to provide comfort and energy-saving by regulating the airflow to different areas of the house depending on the ambient and external temperatures in addition to the relative humidity as parameters according to the rule base, so that the outputs are a compressor speed setting (increase or decrease), adjust the fan speed (Increase or decrease), change the mode of the air conditioner to (hot, cold / off), open or close the ventilation zone. Based on the analysis of the data collected and tested, a comfortable atmosphere was obtained throughout the house with the belief that energy use is very efficient.

The author in [9] is an application of the Fuzzy logic in the field of agriculture and ventilation of greenhouses, the aim of which is to set the appropriate atmosphere for plant growth within greenhouses based on the close relationship between temperature and humidity using a physical model that works to decouple this relation in-between them to manage the internal climate while saving energy as a result of reducing When the engine is running, this system was simulated using a MATLAB so that the temperature was set to 20 Celsius at night and 28 Celsius in the morning with the adopted relative humidity (70%) to complete the ventilation process through entering the more humid air into the greenhouses to maintain the degree of Relative humidity, the study results were similar to the expected results, but more study is needed in detail during operation to verify energy saving.

The authors presented in [10] a prototype of the crowd estimation system in Al-masjid Al-Haram, which helps in guiding the mosque's visitors and managing the crowds in the place through visual representation in the form of a thermal map (i.e., crowd representation as a thermal block), this work was divided into two parts:

- Explore the system's features, aspects, and design stages.
- Preparing a short comparison between two textile-based techniques used to estimate the crowd: LPB & GLCM.

The data used was collected through the mosque's cameras (Sa'i area between Safa and Marwa in particular) to analyze it to estimate the crowd density, then converted it into thermal maps to know the crowded places in the mosque so that it provides the opportunity for users to avoid these crowds or redirect to less crowded areas, for the results, The LPB algorithm yielded comprehensive results of 87.9%, especially for the top and side images.

The [11] aims to develop a logic-based smart ventilation system to control indoor air quality in pharmaceutical sites because indoor air quality affects the pharmaceutical industry, production, and storage, including appropriate temperature, humidity, airflow, and the number of appropriate microorganisms, the proposed system works depending on the fuzzy inference system, where the ventilation system can control airflow and quality according to internal temperature, humidity, airflow and microorganisms in the air. The MATLAB Fuzzy Logic Toolbox was used to simulate the performance of the fuzzy inference system. The results showed that the temperature difference has less effect on controlling the position of the system but has a noticeable effect on air conditioning and fan speed. If the temperature difference corresponds to the "hot" organic function, the air conditioning and fan speed are set to the "medium" organic function, and the higher the temperature difference from "warm" to "hot", the air conditioning and the fan will increase the speed to "very fast" and the system efficiency can be improved by processing input and output parameters according to user requirements.

In fuzzy ventilation control for zone temperature and relative humidity [12] first goal is to use free cooling and drying of available humidity due to the differences in the area and surrounding conditions and this is done by changing the ratio of fresh air that enters the heating, ventilation and air conditioning system and then the controlled area, while the other goal is to maintain the conditions of the region at a preferred control point located between the top and bottom turning points so that the upper and lower turning point boundaries and the preferred set point are adjusted for fuzzy ventilation control purposes to ensure occupant comfort. The HVAC plant becomes active when the fuzzy ventilation control strategy is unable to keep area conditions within the maximum and minimum points of the point. Simulation results were compared using a fuzzy ventilation control strategy with normal plant operation using PID controllers. This standard comparison was used to evaluate the benefits of using a fuzzy ventilation control strategy. The comparisons lasted for 52 weeks based on certain weather data that make sure of exposure to various ambient weather conditions, which result in it the ability of the HVAC station to operate between 05:00 and 17:00 daily.

The author in [13] proposes a physical model of greenhouse used in the Simulink / MATLAB environment to simulate the internal temperature and humidity as a mechanism for controlling air temperature and humidity in greenhouses. A fuzzy logic method was developed to control motors that are installed inside the greenhouse for heating, ventilation, humidification, and cooling to obtain a suitable local climate, the results showed a stable behavior of both temperature and humidity with a low rate of heating, ventilation, and humidification without the need to use a dehumidifier system to reduce energy consumption.

In [14], a hybrid learning algorithm is proposed that represents a general model of the neural network for controlling fuzzy logic and decision systems. This model combines the idea of controlling fuzzy logic, the structure of the neural network, and learning capabilities in an integrated

mysterious logical control system based on the neural network and the decision-making system especially in the speed of learning.

The author in [15] suggested a self-adjusting Fuzzy PI controller in the HVAC air pressure control loop. Fuzzy Self-Adjusting Console (STFPIC) online output measurement factor is modified by vague rules according to the current direction of the controlled process. The base rule is defined to set the resulting measurement factor to error and change the error of the controlled variable. Ziegler-Nichols PI tuner or PID controller works well around normal working conditions but tolerating it to processing parameter changes is highly affected. STFPIC has been used to overcome these shortcomings. Compared with the PID and Adaptive Neural Controls (ANF), simulation results show that STFPIC performance is better under normal conditions as well as when the HVAC system encounters major differences in parameters.

The [16] analyzed the dynamics of the crowd for visitors at the Prophet's Mosque during the most saturated period to describe the most dangerous conditions and suggest technical solutions to accommodate visitors and provide them with a safe passage. The main purpose of the statistical analysis in this study is to investigate the current numbers of visitors to the Prophet's Mosque and prepare administrative plans for future expansion to accommodate the expected number of visitors within specific sites in the mosque. Data was collected by performing an actual count of visitors from the videos and recorded images taken by the legal authority during the holy month of Ramadan and the month of Dhu al-Hijjah and during the busiest hours of the day such as the time of entry from the Peace Gate to the Prophet Mohammed's tomb and from the tomb to the exit from the Baqi Gate. This study provides reasonable information on the crowd dynamics that can be adopted by any responsible crowd management authority aiming to accommodate a large number of visitors during the busiest seasons without causing any harm to visitors. The results of this study are expected to help improve crowd management in the mosque.

### III. METHODOLOGY

In this section, the methods and materials will be described and discussed through showing the implementation of the counting people technique using the Congested Scene Recognition Network (CSRNet) algorithm and build the fuzzy control system by using the data weather [17], also an example for the whole system will be proposed.

This system consists of several parts that connected for controlling the mechanism of opening/closing domes according to weather data and the situation of crowding in the mosque, in general, the following tools and techniques are all we need to build the model that have proposed:

- Camera: First, a camera with high specifications and quality is needed to take pictures from all parts of the mosque to later analyze these images using the algorithm CSRNet and get the desired result which is the approximate number of worshippers, which is available in the Prophet's Mosque and can be used.

- Rainfall Sensor 3864: It should be placed at the top of the dome to predict precipitation accurately and reliably, this type is lightweight, frost-proof, and heat resistant [18], which is good to detect rainfall in real-time and force domes to close.
- DHT22 SENSOR: It is used for measuring temperature and humidity [19]. It uses a capacitive humidity sensor and a thermostat to measure the surrounding air. This sensor is cost-effective, provides low power consumption, good for -40 to 80°C temperature readings with  $\pm 0.5^\circ\text{C}$  accuracy, and up-to 20meter signal transmission is possible.
- ARDUINO UNO: The microcontroller used here is an Arduino UNO [20]. The UNO is a microcontroller board based on ATMEGA 328P. The ATMEGA 328P has 32kB of flash memory for storing code. The board has 14 digital input and output pins, 6 analog inputs, 16 MHz quartz crystal, USB, an ICSP circuit, and a reset button. The UNO can be programmed with the Arduino software.
- Steel Rails: It should have the ability to withstand friction caused by moving the domes, where domes are placed on these tracks to move in one direction to be opened/closed (Fig. 1).

The images have taken from all over the mosque through the cameras distributed inside it. Then these images enter in the worshiper numbers predicting system using the captured images (CSRNet) techniques are applied, and then the congestion percentage in the mosque is calculated by dividing the number of worshipers on the capacity of the mosque. At the same time, rainfall and weather statuses are detected, and if there is rain, the domes are closed, else the weather statuses are entered along with the congestion rate into the fuzzy control system and the rules and relationships between the different data are built and then the dome is opened for a specific period, based congestion rate and weather factors.

#### A. Data Set

For the data of this research, it consists of two groups as follows:

1) *Weather data set*: It represents information about the weather conditions in the Kingdom of Saudi Arabia, obtained from the Kaggle.com website [17], represented by 249024 rows and 15 columns that is contained data for all the cities of Saudi Arabia, the hourly changing weather from 2017 to 2019, the columns are: date, hour, minute, day, temperature, humidity, wind strength, barometer, and visibility.

2) *A set of pictures*: to predict the number of worshipers in the mosque: It is a group of pictures that are taken and analysed through a CSRNet algorithm to predict the approximate number of worshipers at the mosque. A group of images was obtained from the Shanghai Technology Database [21] to train the model on it.

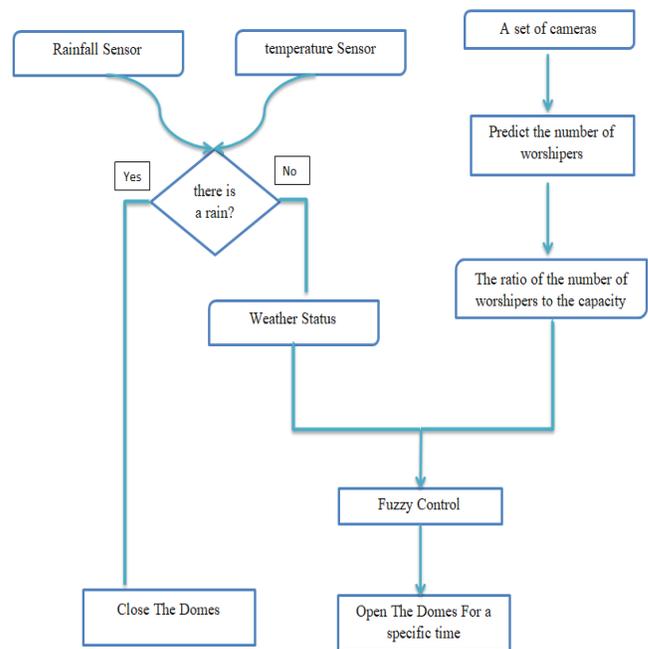


Fig. 1. Proposed Model of Fuzzy Control.

#### B. Building the CSRNET Model

Convolutional Neural Network (CNN) is one of the deep learning techniques and one of the types of the feed-forward neural network, depends on simulating the biological processes occurring in the visual lobe in the brain of living organisms and is used to solve computer vision problems in artificial intelligence and digital image processing and consists of an input layer, hidden layers, and an output layer [22], [23], [24], and to find the optimal solution and larger values of the real results the Back propagation technology is used in calculating the error rate each time and trying to reduce it.

To recognize the number of people in the images, the python programming language will be used to build the crowding detection algorithms using CSRNet algorithm. Where the proposed model firstly predicts the number of worshipers in the mosque by analyzing the group of images that will be taken hourly for the different parts of the mosque and then calculating the approximate total number of worshipers using CSRNet algorithm.

CSRNet algorithm is a technique for crowd counting by estimating the number of people in an image. It is Convolution Neural Networks (CNN) based methods, which are building an end-to-end recession method using CNNs Instead of looking at the spots of an image. Furthermore, it takes the entire image as input and directly outputs the number of crowds. CSRNet publishes a deeper CNN to catch high-level features and produce high-quality density maps without expanding the network complexity. CSRNet uses VGG-16 at the front end because of its strong transfer learning ability [7]. The output size from VGG is  $\frac{1}{8}$  of the original input size. CSRNet also uses dilated Convolution layers in the back end.

### C. Ground Truth Preprocessing

In this part, to achieve the pre-processing step some important libraries like (torch, SciPy) will be used. Also, to build a two-dimensional density map for ground truth, the Gaussian kernel will be used to compute the real values of the people in each image in the dataset [21] bypassing the values, where the dataset contain the values, and these values consisting of the head annotations in that image, and the Gaussian filter and tree with  $k=4$  will be used.

### D. Implementation and Results of CSRnet Algorithm

GPU was used to build the model by using the Cuda function in Python and to build the CSRNet model like [7], the straightforward way and end-to-end structure will be used. Also, a VGG-16 network with only use  $3 \times 3$  kernels will be used for the front-end. For training phase. The accurate weights trained by the authors in [7] will be applied, and to show the accuracy of the results, it will be compared with the ground truth. CSRNet algorithm was tested on the Shanghai dataset [21] and get the results shown in Fig. 2.

Due to the difficulty of obtaining the number of worshippers inside the mosque, the algorithm was applied on the Shanghai Tech dataset (the same mechanism for any images). In Fig. 2, the image on the right shows that the actual number of people is 258, and after applying the CSRNet algorithm with the weights shown previously [7], an approximate number of 267 people was achieved. For the second image, the number of people in the original image is 662 and while an approximate number is 453 was achieved. Since an estimated percentage number of worshippers is needed in the mosque, it does not matter if it is 100% accurate for the proposed system. The previous results can be adopted, and the number of worshippers can be converted to a percentage.

### E. Moving the Domes using Fuzzy Control

Fuzzy logic is a form of knowledge representation used in areas where concepts are difficult to define precisely, and which depend on their context for their understanding [25], where the Fuzzy Logic was introduced by Lotfi Zadeh and Berkely in 1965.

Fuzzy Linguistic Variables are used to represent qualities spanning a particular spectrum. Fuzzy Control combines the use of fuzzy linguistic variables with fuzzy logic. It is represented based on the inputs, outputs, and Disjunction and Conjunctions within specific rules. And it includes several basic steps such as fuzzification: to Calculate Input Membership Levels and fuzzification: to Constructing the Output and Find centroids (when the Location where membership is 100%).

Fuzzy logic is one of machine learning algorithms, which is used in the case of relative data, so that the values are not specified as the terms that humans use [26], so the computer cannot deal with it, as if the data are vague, such as cold, hot, very cold, wet, and very humid, for such values are not considered clear and cannot be determined, so the data are divided into fuzzy sets, for example, it can be described as less crowded, very crowded or moderate crowding. All of them are not specified, but it can be determined by making the category of 5-10 people less crowded and from 30-60 very crowded, in case the area of the place is small and so on.

### F. Building the Fuzzy Model

In this section, the crowding of worshippers in the mosque area has represented using a Linguistic Fuzzy term set of three labels (no crowd, Medium crowd, and crowd). The three Labels were divided into percentage of 0 to 100 as follows (see Fig. 3):

- 0-30% (No Crowd): In this case, the ratio of the number of worshippers is calculated with the capacity of the mosque, and if it is below 30% it is represented that there is no crowding.
- 25-75% (Medium Crowd): In this case, if the ratio of the number of worshippers to the capacity of the mosque is between 25% and 75%, then the case is medium crowding.
- 70-100% (High Crowd): In this case, if the ratio of the number of worshippers to the capacity of the mosque is more than 70% then the case is crowd.

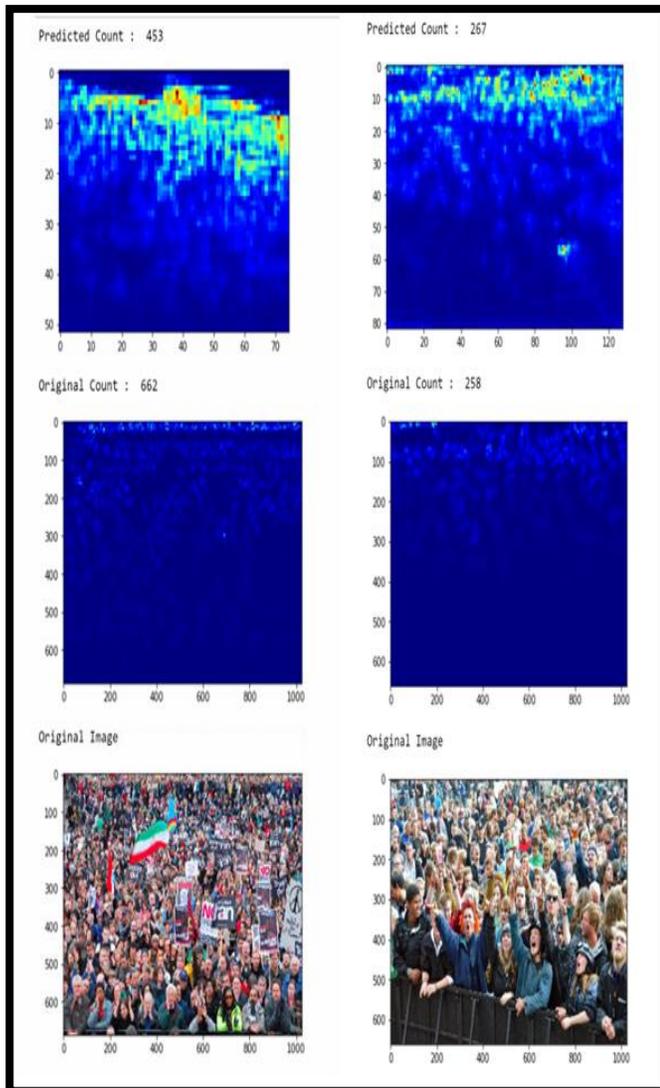


Fig. 2. Result of Counting People using CSRnet Algorithm.

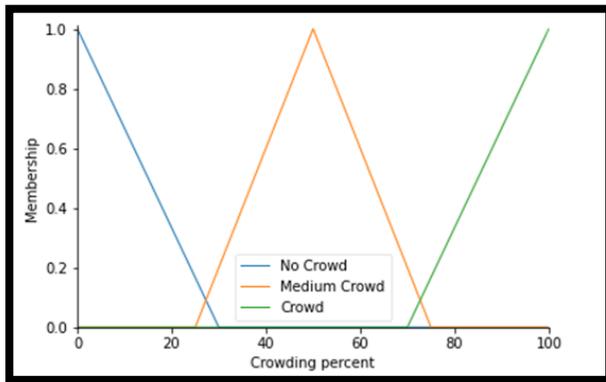


Fig. 3. Linguistic Fuzzy Term Set of Three Labels for Crowding.

As a result of image processing according to the above proportions, the total number of worshippers in the mosque have achieved. Then, the weather and temperature conditions have obtained to determine the appropriate cases for opening the domes. The weather conditions were divided into two labels (Rain and outlook) as follows (Fig. 4):

- (0° and 24°): represents the minimum and maximum temperatures for rainy conditions.
- (7° and 47°): represents the minimum and maximum temperatures for moderate climates.

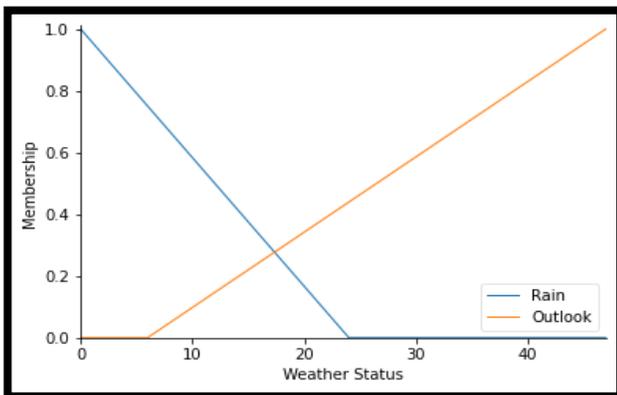


Fig. 4. Linguistic Fuzzy Term Set of Two Labels for Weather Status.

The weather result, combined with the results of image analysis, are inputs that define the state of the dome opening and the time needed per second to conduct the necessary ventilation to the mosque as follows (see Fig. 5):

- State (0): The dome remains closed, and this state working if it was raining.
- State (0-120): The dome opens for a short period, and this state working if the weather was good and there was no crowding.
- State (90-210): The dome opens for a medium period, and this state occurs if the weather was good, and crowding was medium.
- State (180-300): The dome opens for a long time, and this state occurs if the weather was good and there was high crowding.

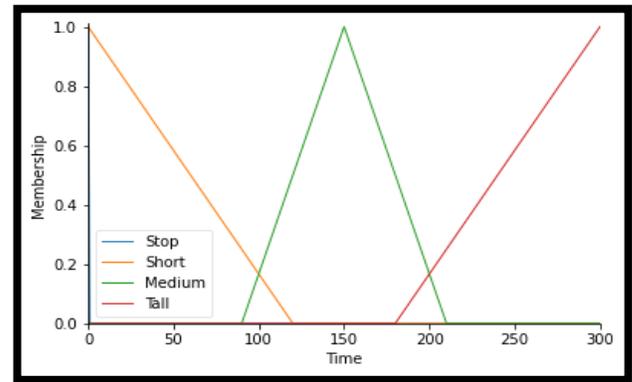


Fig. 5. Linguistic Fuzzy Term Set of Four Labels for Dome's Status.

After train the model according to the inputs from the weather data and the number of worshippers, the following rules have been generated (see Fig. 6):

- Rule 1: in this case, when only if the weather status is "Rain" then we must close the domes (time to open the domes is 0 so the result is "stop").
- Rule 2: in this case, when the weather status is "Outlook" and the status of a crowd is "no crowd" then the time to keep the domes open must be "short".
- Rule 3: in this case, when the weather status is "Outlook" and the status of a crowd is "Medium Crowd" then the time to keep the domes open must be "medium".
- Rule 4: in this case, when the weather status is "Outlook" and the status of a crowd is "Crowd" then the time to keep the domes open must be "Tall".

```
rule1 = ctrl.Rule(weather['Rain'], time['Stop'])
rule2 = ctrl.Rule(weather['Outlook'] & crowd['No Crowd'], time['Short'])
rule3 = ctrl.Rule(weather['Outlook'] & crowd['Medium Crowd'], time['Medium'])
rule4 = ctrl.Rule(weather['Outlook'] & crowd['Crowd'], time['Tall'])
```

Fig. 6. Generated Logical Rules for Dome's Status.

#### IV. RESULTS AND DISCUSSION

The computations involving fuzzy sets, linguistic models, and CSRnet have done using Python programming language. The weather dataset used for the experiments has obtained from Saudi Arabia's weather history on Kaggle website [20]. The detailed description of the dataset, implementation details about the linguistic terms were discussed in the previous sections.

In this section, the results will be discussed in detail. As mentioned in the earlier section, two inputs "weather status and crowding rates", and one output "dome status" have been generated. However, to achieve the aim of this work, the proposed model should be tested by combining the previous inputs with taking into account the proportions for each attribute and linking them with the output.

The following scenario has been tested assuming that the crowding rate of the mosque with the worshippers in the mosque is 72%, and the temperature recorded 30° (see Fig. 7, Fig. 8, and Fig. 9).

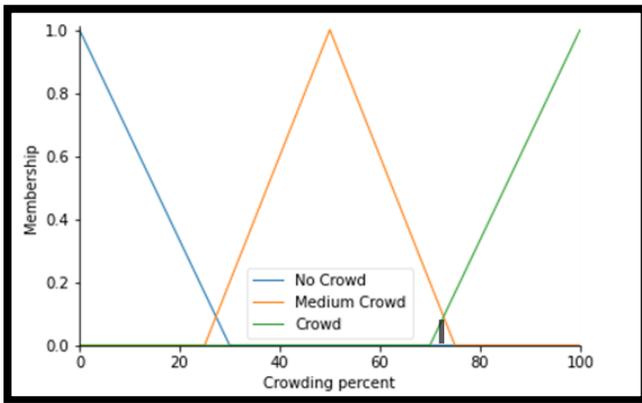


Fig. 7. Crowding Rate of the Mosque with the Worshippers is 72%.

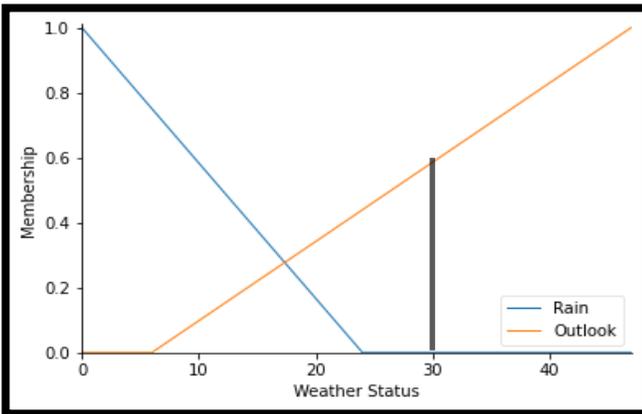


Fig. 8. Weather Status when the Temperature is 30°.

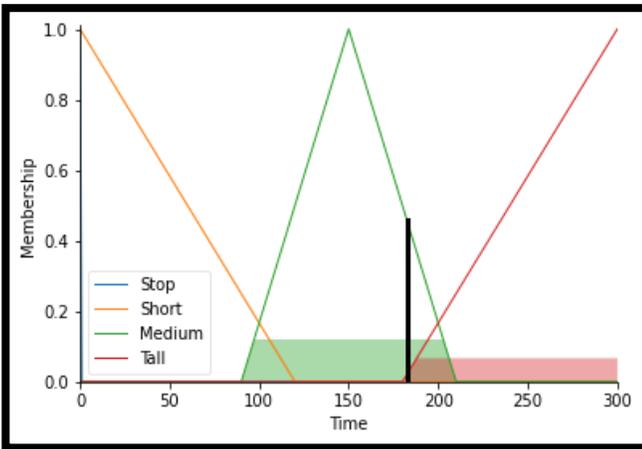


Fig. 9. Testing Scenario for the Proposed Model.

The previous Fig. 7 shows the crowding rate of the mosque with the worshippers when it is 72%, while Fig. 8 shows the weather status when the temperature is 30°. In Fig. 9 both the crowding rate and the temperature degree were combined and represented as inputs, and according to the previously generated rules (see Fig. 6), the exact period during which the domes must be open every hour head can be determined, as in the proposed scenario, this relationship intersected with both the time (medium and tall) so the relationship will be presented in the minutes and according to the inputs the domes will open for 3.04 minutes.

It can be concluded from the previous scenario that the exact time for opening and closing the domes can be specified when the crowding rate and the weather conditions are defined using Congested Scene Recognition Network (CSRNet) and Fuzzy techniques.

## V. CONCLUSION AND FUTURE WORK

Since the spread of mosques is increasing, as well as the technological development in a permanent race over time, it became necessary to coordinate the development of mosques and technological development to match each other, thus the availability of a comfortable environment during worship and approach to Allah. Today we are in the age of using latest technologies in everything, based on this principle a proposed model for the smart dome was presented as the beginning of the computerization of mosques. The Prophet's Mosque was adopted to apply this model, knowing that it can be applied to any mosque provided the necessary materials and techniques.

The proposed model has built by Congested Scene Recognition Network (CSRNet) and Fuzzy techniques using Python programming language to control the domes to be opened and closed for a specific time to renew the air inside the mosque. The proposed model has worked efficiently and specifies the exact duration time to keep the domes open for a few minutes for each hour head. This research came as an extension of previous published research [6] with more modifications and improvements to it, and promising results have been obtained in this work.

As an extension to the model proposed, more factors that affect the dome status might be added to have more accurate results to control the dome movement. Also, different machine learning Algorithms can be applied [27], [28] and deep learning.

## REFERENCES

- [1] Michael Lipka, "Muslims and Islam: Key findings in the U.S. and around the world", PEW Research Center/FACT TANK, August 9, 2017.
- [2] Maryam Ghayyada, "How many mosques are there in the world", Available: mawdoo3.com / Home / Islamic landmarks, 1 July 2019.
- [3] Muhammad bin Abdullah Al-Sabeel, "A brief summary about the architecture of the Two Holy Mosques, since the introduction of Islam to the era of the Custodian of the Two Holy Mosques", 2019.
- [4] Mohammed bin Ali Al-Thobyani Al-Juhani, Sabah Saudi, "The largest expansion in the history of the Prophet's Mosque", 2020.
- [5] Al-Khuzayem, Bandar bin Muhammad, Miller, & Abdul Rahman. "Estimating the crowd density in the Grand Mosque using the bypass neural network". 2019.
- [6] Mohammad Awis Allababede, Anas H. Blasi, Mohammad Alsuwaiket, "Mosques Smart Domes System using Machine Learning Algorithm", International Journal of Advanced Computer Science and Applications (IJACSA) : Vol.11, No.3, 2020.
- [7] Yuhong Li, Xiaofan Zhang, Deming Chen, "CSRNet: Dilated Convolutional Neural Networks for Understanding the Highly Congested Scenes", arXiv : 1802.10062v4 [cs.CV] 11 Apr 2018.
- [8] LEA, Robert N., et al. "An HVAC fuzzy logic zone control system and performance results". In: Proceedings of IEEE 5th International Fuzzy Systems. IEEE, p. 2175-2180. 1996.
- [9] AZAZA, M., et al. "Fuzzy decoupling control of greenhouse climate. Arabian Journal for Science and Engineering", 40.9: 2805-2812, 2015.
- [10] Eldursi, S., Alamoudi, N., Haron, F., Aljarbua, F., & Albakri, G. "Crowd Density Estimation System for Al-Masjid Al-Haram". Int'l

- Journal of Computing, Communications & Instrumentation Engg. (IJCCIE) Vol. 4, Issue 1, ISSN 2349-1469 EISSN 2349-1477, 2017.
- [11] Rahman, S. M., Rabbi, M. F., Altwijri, O., Alqahtani, M., Sikandar, T., Abdelaziz, I. I & Sundaraj, K., "Fuzzy logic-based improved ventilation system for the pharmaceutical industry". J. Eng. Technol, 7, 640-645, 2018.
- [12] GOUDA, Mohamed Mahmoud. "Fuzzy ventilation control for zone temperature and relative humidity". In: Proceedings of the American Control Conference, IEEE, p. 507-512. 2005.
- [13] JOMAA, Manel, et al. "Greenhouse modeling, validation and climate control based on fuzzy logic". Engineering, Technology & Applied Science Research, Vol. 9, Issue 4, P.4405-4410, 2019.
- [14] LIN, Chin-Teng, et al. "Neural-network-based fuzzy logic control and decision system". IEEE Transactions on computers, 40.12: 1320-1336. 1991.
- [15] PAL, A. K.; MUDI, R. K. "Self-tuning fuzzy PI controller and its application to HVAC systems". International journal of computational cognition, 6.1: 25-30, 2008.
- [16] AL-AHMADI, Hassan M., et al. "Statistical analysis of the crowd dynamics in Al-Masjid Al-Nabawi in the city of Medina, Saudi Arabia". International Journal of Crowd Science, 2018.
- [17] Saudi Arabia weather history data. Available: Kaggle Website: <https://www.kaggle.com/esraamadi/saudi-arabia-weatherhistory>. Accessed on: Dec. 10, 2020.
- [18] Shenoy, Arun P., AMEER, P. M. "Anomaly Detection in Wireless Sensor Networks". Conference (TENCON). IEEE. p. 1504-1508. 2019.
- [19] ADHIWIBOWO, Whisnumurti; DARU, April Firman; HIRZAN, Alauddin Maulana. "Temperature and Humidity Monitoring Using DHT22 Sensor and Cayenne", API. Jurnal Transformatika, 17.2: 209-214, 2020.
- [20] Malhotra, M., Aulakh, I. K., Kaur, N., & Aulakh, N. S., "Air Pollution Monitoring Through Arduino Uno". In ICT Systems and Sustainability (pp. 235-243). Springer, Singapore. 2020.
- [21] Shanghai Technology Database. Available: Kaggle Website: <https://www.kaggle.com/tthien/shanghaitech?> Accessed on: Dec. 5, 2020.
- [22] Anas H. Blasi, "Performance increment of high school students using ANN model and SA algorithm". Journal of Theoretical and Applied Information Technology 95(11):2417-2425. 2017.
- [23] Rawabi A Aroud, Anas H. Blasi, Mohammed Alsuwaiket. "Intelligent Risk Alarm for Asthma Patients using Artificial Neural Networks". International Journal of Advanced Computer Science and Applications, Vol. 11 No. 3, 95-100, 2020.
- [24] Anas H. Blasi, Mohammed A. Alsuwaiket. "Analysis of Students' Misconducts in Higher Education Institutions using Decision Tree and ANNs". Engineering, Technology and Applied Science Research. Vol. 10 (No. 6): 6510-6514. 2021.
- [25] Zadeh, Lotfi A., and R. A. Live. "Fuzzy Logic Theory and Applications", World Scientific Publishing Company, 2018.
- [26] Anas H. Blasi, "Scheduling Food Industry System using Fuzzy Logic," Journal of Theoretical and Applied Information Technology, vol. 96, no. 19, pp. 6463–6473, Oct. 2018.
- [27] Mohammed A. Alsuwaiket, Anas H. Blasi, khawla Altarawneh. "Refining Student Marks based on Enrolled Modules' Assessment Methods using Data Mining Techniques". Engineering, Technology and Applied Science Research. Vol. 10(No. 1):5205-5010. 2020.
- [28] Anas H. Blasi, Mohammad A. Abbadi, Rufaydah Al-Huweimel. "Machine Learning Approach for an Automatic Irrigation System in Southern Jordan Valley". Engineering, Technology and Applied Science Research. Vol. 11 (No. 1): 6609-6613. 2021.

# Correlating Crime and Social Media: Using Semantic Sentiment Analysis

Rhea Mahajan<sup>1</sup>, Vibhakar Mansotra<sup>2</sup>

Department of Computer Science and IT, University of Jammu, Jammu, India

**Abstract**—Crimes occur all over the world and with regularly changing criminal strategies, law enforcement agencies need to manage them adequately and productively. If these agencies have prior data on the crime or an early indication of the eventual felonious activity, it would encourage them to have some strategic preferences so that they can deploy their restricted and elite assets at the spot of a suspected crime or even better explore it to the point of anticipation. So, integration of social media content can act as a catalyst in bridging the gap between these challenges as we are aware of the fact that almost all our population uses social media and their life, thoughts, and, mindset are available digitally through their social media profiles. In this paper, an attempt has been made to predict crime pattern using geo-tagged tweets from five regions of India. We hypothesized that publicly available data from Twitter may include features that can portray a correlation between Tweets and the Crime pattern using Data Mining. We have further applied Semantic Sentiment Analysis using Bi-directional Long Short memory (BiLSTM) and feed forward neural network to the tweets to determine the crime intensity across a region. The performance of our proposed approach is 84.74 for each class of sentiment. The results showed a correlation between crime pattern predicted from Tweets and actual crime incidents reported.

**Keywords**—Crimes; social media; Twitter; BiLSTM; semantic sentiment analysis

## I. INTRODUCTION

With the upsurge of online media, the web has become an energetic and enthusiastic domain wherein billions of people all around the globe associate, offer, post and share their daily activities. Data which is generated by Social Networking Sites is an extremely large data which is growing exponentially at an unprecedented pace. Mountains of raw data is generated daily by individuals on these social networking sites [1]. These sites have changed our lives drastically and their impact on society cannot be overlooked. Facebook, Instagram, and, Twitter are the most popular social net-working sites with 2.5 billion, 1 billion and, .336 billion users respectively all over the world and 241 million, 40 million and 37 million users respectively in India. These numbers vary every day and this rapid growth in the volume of users has provided the predictive ability in extensive fields such as personality prediction [2], stock market trends [3], election results [4], the box office performance of movies, etc. [5]. Social media allows its users to share their apprehensions, ideas and daily activities on the web. This shared content by the individuals when joined together provides a rich resource of naturally occurring data. Status updates from Facebook, tweets from Twitter and pictures from Instagram provide information about the social behavior of its users. Our enchantment to social media has grown in the last

decade to the pinnacles which can only be compared to the billions they have been valued for. Its growth and impact is unparalleled, to say the least. While they have developed into different entities, their usefulness and social impact have always been a subject of debate. The influence can be judged from the fact that the fake news travels or gets viral faster than the real and valuable information. This effect has only increased and sometimes does get morphed into something unpleasant and hostile, where these interactions have gravitated towards the unconstructive side of things which includes bullying, trolling, stalking, social media trials etc. This impact is also tipping the scale towards more and more pessimism.

The present crime prediction models commonly depend on relative static highlights including long haul verifiable data, topographical data, and, segment data. This data changes gradually after some time, which means these conventional models couldn't catch the transient varieties in criminal activities [6]. The primary downside of these models is that they diminish the social setting to verifiable criminal records while disregarding information on the social conduct of the users of available on social networking sites including the victim and the criminal as keeping an on eye the social behavior information of an enormous society is a difficult and challenging task [7].

Twitter is picked over other online social media sites because it is one of the most popular micro-blogging sites for its political potential value and transparency and the way that anybody can get to geo-tagged tweets created in a given region or territory. Moreover, people are very vocal about their views and opinions and do not hesitate to express them through their tweets. So, this research is inspired by the fact that the enormous data available on these sites can be used to bring out a significant amount of information for the administration and law authorities which will eventually be used to predict criminal behavioral patterns.

In this paper, an attempt has been made to predict crime pattern using geo-tagged tweets from five regions of India. We hypothesized that publicly available data from Twitter may include features that can portray a correlation between Tweets and the Crime pattern using Data Mining. We have further applied Semantic Sentiment Analysis using BiLSTM and feed forward neural network to the tweets to determine the crime intensity across a region. BiLSTM is a variant of LSTM and is more powerful than LSTM as it overcomes the problem of gradient explosion that occurs in LSTM. The results showed correlation between crime pattern predicted from Tweets and actual crime incidents reported. Fig. 1 shows framework of the proposed research.

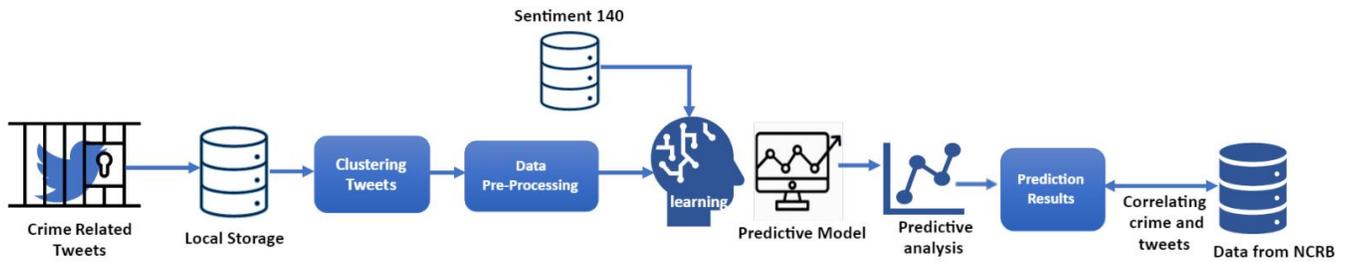


Fig. 1. Framework of the Research.

This paper is organized as follows: After brief introduction in Section I, Section II provides a summary of related works in area of crime Prediction using data from social networking sites. Section III gives the description of the data set and process of data acquisition. Section IV describes the proposed approach, which is followed by Section V, where performance of the classifier on various evaluation metrics is presented. Section VI and Section VII presents correlation analysis and hypothesis testing, respectively. Finally, we have concluded the paper with some future work guidelines in Section VII.

## II. RELATED WORKS

Recent studies have attempted to fit in data from Twitter into their predictive models for crime assessment. The purpose of integrating Twitter data for crime prediction is to take into account significant amount of information available on Twitter about the social conduct and mobility of the users. Geber [8] is the first one to introduce social media content to model crime prediction. To address the use of tweet content in determining the crime pattern of a particular location, Geber used latent Dirichlet allocation on tweets that showed an improvement on models using conventional historic data as crime predictors for stalking, criminal damage and gambling. Even though, it is the foremost study to examine tweet text, Gerber's use of LDA is challenging given that it is an unsupervised technique, which meant correlation between word clusters and the crimes are not driven by previous theoretical insights. This resulted in correlations that seemed comparatively worthless. Wang et al. [9] extracted event-based topics from real time tweets to predict hit-and-run incidents in Virginia. Even though their approach was novel, the source of data was limited to a set of manually selected news portals and the massive amount of information backed by the citizens was neglected.

Chen et al. [10] utilized the sentiment in Tweets together with weather data in KDE for predicting the time and location of the theft. However, their study was restricted to spatial information such as weather data for specific time and location Brandt et al. [11] studied the relationship between mobile populations as recorded by Twitter's geotagging facility and the location of different types of crime. They concluded the absence of tweets was predictive of assaults and thefts. Similarly, Malleon et al.[12] have used a number of geographic analysis methods to model crime risk using tweets

for mobile populations. The main drawback of these studies was that tweet text was not taken in consideration, instead focusing purely on geolocation data. It was also concluded that KDE is a location dependent technique cannot be easily generalized. There may be some type of crime that does not occur in the vicinity of previous locations and incidents and the population of an area can change frequently.

In addition to the above studies, sentiment analysis has also been a key instrument in Crime detection and prevention. Zainuddin et al. [13] applied sentiment analysis to crime related tweets through the use of model that was based on Natural Language Processing techniques and SentiWordNet, the model had the capability to detect the subjectivity of crime and then predicted crime through hate tweets. Machine learning algorithms has also been used to solve the task of sentiment analysis of Tweets [14][15]. Pang et al. [16] performed a comparative study involving algorithms such as Naïve Bayes, Support Vector Machine and maximum entropy to determine sentiment polarity for movies reviews. These studies were effective but ignored the semantics to capture the meaning of the tweets.

In this paper, we have tried to overcome the drawback of above studies by collecting real time tweets for a period of 21 days across five regions of India to capture dynamic movement of the user. Further, we have used combination of BiLSTM and feed forward neural network to find sentiment polarity of the Tweets. The strength of BiLSTM is that it provides extra training by traversing the text twice from left to right and right to left, there by extracting the semantics of the words in context of the information preceding and succeeding it and therefore can capture long term contextual dependencies and global features from the sequential text.

So, keeping in view the various trends of research carried out using social media in particular Twitter, it needs no mention that social media mining is an important area of research and by the application of various data mining techniques can generate very impressive and interesting patterns as well as outcomes which can be analysed, interpreted and can be used for the benefit of the society especially in crime Prediction and detection and in the scenario of evolving protest and riots. Table I lists some of the important works done in area of crime Prediction using tweets.

TABLE I. LISTS SOME OF THE IMPORTANT WORKS DONE IN AREA OF CRIME PREDICTION USING TWEETS

Author	Application	Technique used	Dataset Used	Evaluation results
Geber(2014)[8]	Twitter-based model for crime trend prediction to determine crime rates in the prospective time frame.	Text analysis- filtering including stop word reduction and low-frequency term reduction Predictive analysis-linear support vector classifier	Historic tweets were collected from Chicago city for a period of three years combined with other datasets such as unemployment rates and weather conditions.	Results revealed correlation between features extracted from content as content-based features and the crime trends.
Wang et al. (2012) [9]	Twitter based criminal incident prediction on Hit and Run cases.	Text analysis-Semantic Role Labelling (SRL) and Dirichlet allocation Predictive analysis-linear modelling	Real-time Tweets using Twitter API	F1 score-80%of verbal SRL and 72%of nominal SRL
Chen et al.(2015) [10]	Twitter based model for time and location prediction in which specific type of crime will occur.	Text analysis-Sentiment Analysis by the lexicon-based method Predictive analysis-linear modelling via logistic regression Comparative analysis- hot spot mapping with kernel density estimation(KDE)	GPS tagged tweets from Chicago city of US; combined with weather data and historic crime data from Chicago	Performance measure -Area Under Surveillance Curve(AUC) Predicted AUC-0.67 Actual AUC-0.66 Error-1.5%
Aghababaei et al. (2016) [17]	Twitter based criminal incident prediction on 25 types of crime.	Text analysis-statistical language processing and spatial modelling Predictive analysis-logistic regression Comparative analysis- hot spot mapping with kernel density estimation(KDE)	Geo-tagged tweets from Chicago city of US and historic criminal data.	Of the 25 crime types, 19 showed improvements in Area Under Surveillance Curve (AUC) when adding twitter topics to the KDE-only model.
Almehmadi (2017) [18]	Twitter-based model to predict crime by analysing language usage in Tweets as a valid measure.	Text analysis-WEKA and Ranker algorithm Predictive analysis- SVM classifier was used to classify the data to the proposed class: offensive or non-offensive language	GPS tagged tweets were collected from Houston and New York for three months.	With a binary SVM classifier, 96.19% correct classification accuracy was achieved. Results show accuracy by class for cross-validation with ROC 77%.
Ristea (2018) [19]	Twitter based opinion mining and spatial crime distribution for hockey events in Vancouver.	Spatial clustering, opinion mining and regression analysis was used in order to find meaningful explanatory variables for crime occurrences.	Crime data for Vancouver was obtained from Vancouver Open Data Catalogue. Geo-referenced tweets were obtained using the Twitter Streaming Application for 2014-2016 i.e. for two hockey seasons.	Results showed the influence of social media text analysis in describing the geography of crime along with the importance of additional criminogenic factors
Siriraya et al. (2019) [20]	Twitter based crime investigation tool that provides contextual information about crime incidents by visualizing spatial and time-based characteristics of a crime.	Various tweet vectorization strategies (pre-trained word vectors from the GloVe model4 , Doc2Vec etc.) and classification models (Logistic Regression, SVM etc.) were used to investigate the performance in classifying negative tweets.	Geo-tagged tweets were collected for a period of one year from San Francisco.	The results showed that using the GloVe model to represent the tweet words and the linear kernel SVM to perform binary classification resulted in the best performance (a stratified 5 fold-cross validation showed an F-score of 0.80 as opposed to 0.70 for the SVM-Doc2Vec model)

### III. DATASET DESCRIPTION

We began our research by identification of five regions of India; determined by Nation Crime Records Bureau as per prevailing crime rate. They are Uttar Pradesh, Madhya Pradesh, Maharashtra, Bihar and Delhi-NCR. Then, we collected crime related Tweets from Twitter and crime data from various national and local online news portals and NCRB<sup>1</sup> from 2 December 2019 to 22 December 2019. Crime against women, Crime against children, Murder, Suicide, Cyber Crime and violence due to riots and protests were six categories of crime for which data has been collected.

To extract the data from Twitter, we need to create an account on Twitter. Then, Twitter requires its users to register an application. This application authenticates our account and provides the user a access token and consumer key which then can be used to connect with twitter and download tweets. Crime related and Geo-tagged real-time tweets were collected from above mentioned Indian regions using geo-tag filter of Twitter Streaming API.

We ran the data collection process which resulted in over 30,000 tweets from 512 users in our database shown in Fig. 2. This data contains information such as user ID, the screen name, number of followers, date, the tweet itself, device used to post the tweet source, the user-defined location, coordinates, agender, retweets and user mentions.

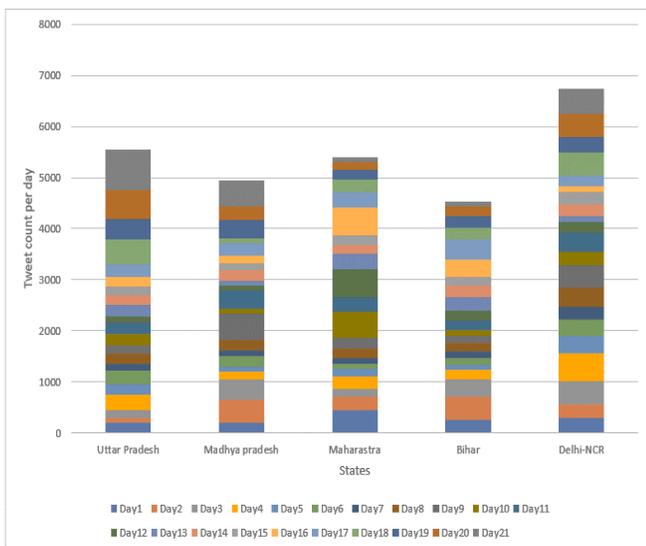


Fig. 2. Distribution of Tweets Day-wise from Five Regions across India.

An English language filter was applied and 29 different keywords were used while streaming real-time Tweets. Tweets were collected using a keyword search strategy [21]. Keywords used to identify a specific crime type were rape, dowry, abduction, kidnapping, child labor, depression, anxiety protest, etc. are listed in Table II. The Tweets were extracted in JSON format imported to a pandas Data frame in Python and were finally downloaded in CSV file format. We extracted the tweets using the geo-tag filter option of Twitter's streaming API and bounding box. Tweets were then clustered on the basis

of similarity i.e. crime type and location using K-means clustering and Jaccard Distance metric to make them organized as shown in Fig. 3.

TABLE II. KEY WORDS

S. No.	Crime Type	Key Words
1.	Crime against women	dowry,rape,assault,abduction,metoo
2.	Crime against children	kidnapping, child labor, minor
3.	Murder	kill, gun, shot, arms, murder
4.	Suicide	Depression, suicide, anxiety mentalhealth
5.	Cybercrime	fraud, stalking, trolling, bullying
6.	Violence due to protest and riots	antiCAA, anti-NRC, hateIndia, protest ,just violence, riots

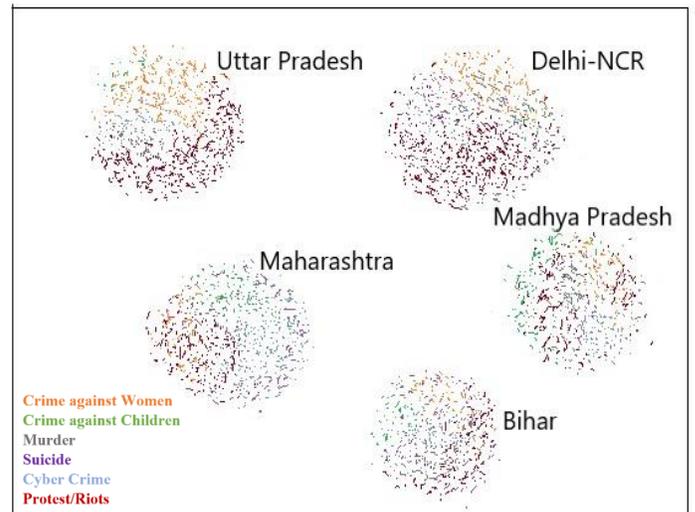


Fig. 3. Tweets Clustered on the basis of Crime Type and Location.

Once the tweets were collected, NLTK<sup>2</sup> package with pip package manager in Python was used for processing text in tweets. The steps include removal of extra places, URL, stop words, tokenization which refers to dividing the text into a sequence of words and lemmatization i.e. reducing different types of words with similar meaning with their root. Tweets were then embedded into vector form using word2vec vectors using Google News vectors for obtaining vector representations of words with Skip-gram architecture.

### IV. SEMANTIC SENTIMENT ANALYSIS

We have used BiLSTM and feed forward neural network as shown in Fig. 5 to determine the sentiment polarity of the tweets. Conventional RNNs can only process the data in one direction and none of the attention is given to process future information. To overcome this limitation, the concept of Bidirectional RNN came into existence. Bi-directional RNN has the ability to traverse the data in both directions with different hidden units acting as forward layers and backward layers. Bidirectional LSTM (Bi-LSTM) was introduced by Graves et al. [22] combining Bidirectional RNN with LSTM

<sup>1</sup>National crime records bureau <https://ncrb.gov.in/en>

<sup>2</sup> <https://www.nltk.org/book/ch01.html>

cell. The output of forward states is not used as an input for backward states and vice-versa in BiLSTM thus, overcoming the problem of gradient explosion.

Sentiment140<sup>3</sup> data set from Kaggle has been used to train our Classifier. It contains 1.6 million tweets extracted using the Twitter API. The tweets have been annotated as negative, positive and neutral with respective sentiment scores and they can be used to detect sentiment of the brand, product, or topic on Twitter .The input to the BiLSTM is set of word vectors  $W=\{w_1, w_2, \dots, w_n\}$ . At each step from  $i \dots n$ , a forward Long Short Memory (LSTM) takes the word embedding of word  $w_i$  and previous state as inputs, and generates the current hidden state. A backward LSTM reads the text from  $w_n$  to  $w_i$  and generates another state sequence. The hidden state  $h_{si}$  for word  $w_i$  is the concatenation of  $h_{si}$  vector forward and  $h_{si}$  vector backward thereby capturing the semantics of the word in context of the information preceding and succeeding it . The output of BiLSTM is fed into the feedforward neural network. Finally, the probability of a tweet  $t_i$  belonging to a sentiment class  $S$  is obtained using Softmax function

$$p(t_i|\hat{\theta}) = \frac{\exp(\beta_i^T \hat{\theta})}{\sum_{j=1}^s \exp(\beta_j^T \hat{\theta})}$$

where  $\beta_i$  (weight vectors) are parameters in SoftMax layer. The activation function for neural network is ReLU. In order to prevent the over-fitting in the training process and co-adaptations of units, dropout of 0.5 is applied.

HYPERPARAMETERS

Epochs	50
Learning rate	$10^{-3}$
Optimizer	Adams
Max length	148
Dropout	0.5
Batch size	64
Nodenum	128
Vector size	300

The output from this sentiment analyser in the form of heat map and corresponding sentiment score is shown in Fig. 4. In the heat map, intensity of blue colour shows the accumulated sentiment of Tweets on a particular day. Tweets that were categorized as Negative (dark blue) were identified as contributing to the crime intensity of that place.

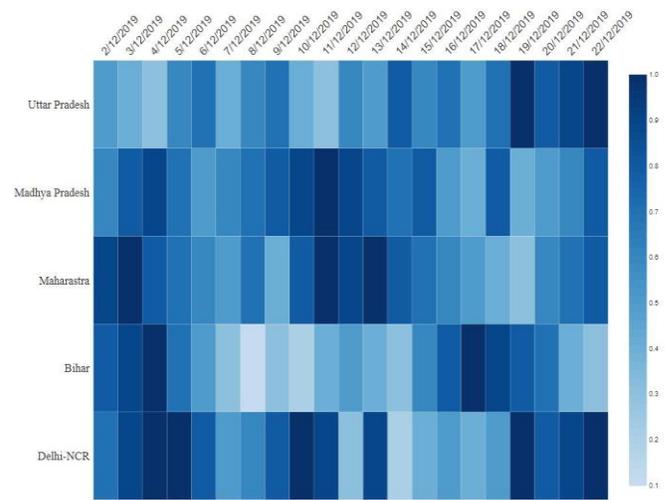


Fig. 4. Heat Map and Corresponding Sentiment Score during Observed Time.

V. EVALUATION METRICES

We have evaluated our classifier on various metrics. Precision, Recall, and F-score have been used for assessing the performance of the proposed model by finding the Confusion Matrix which contains information about actual and predicted classifications done by a classification system. The performance of classifier shown in Table III has been calculated by taking the average of the three metrics for each class of sentiment.

- Precision = True Positive / (True Positive + False Positive)
- Recall = True Positive / (True Positive + False Negative)
- F1-Measure =  $2 * (\text{Precision} * \text{Recall} / (\text{Precision} + \text{Recall}))$

TABLE III. PERFORMANCE OF THE CLASSIFIER

Positive Sentiment			
Precision	Recall	F-Measure	Performance
91.54	92.82	92.18	92.18
Neutral Sentiment			
Precision	Recall	F-measure	Performance
80.70	82.10	81.39	81.39
Negative Sentiment			
Precision	Recall	F-measure	Performance
78.30	83.30	80.72	80.77

<sup>3</sup> <https://www.kaggle.com/kazanova/sentiment140>

---

## Algorithm

---

**Input:** Sentiment140(  $T_{train}$ ), Real-time Crime Related Geo-tagged tweets

**Output:** Probability of Tweet belonging to sentiment class  $s$

**Step 1 :** Install dependencies tweepy, tensorflow, keras

**Step 2:** Import packages os, json pickle, numpy, myplot

**Step 3:** Authentication with twitter using access keys and tokens

**Step 4:** Extract Tweets using Twitter Streaming API using geo-filter and keyword search strategy

**Step 5:** Cluster the Tweets on basis of similarity using Jaccard distance.

**Step 5 :** Obtain the set of word vectors  $t=\{w_1, w_2, \dots, w_n\}$  using word2vec from Google News

**Step 6:** Process the tweets using NLTK package and prepare the data for model fitting

**Step 7:** Initialize BiLSTM model hyperparameters

**Step 8:** For each sentence  $t \in T_{train}$

- Generate expression sequence and output eigenvector  $h_s=\{h_{s1}, h_{s2}, \dots, h_{sn}\}$  through BiLSTM
- The output of BiLSTM is fed to feed forward neural network
- Apply Back propagation algorithm to adjust model parameters and word vectors;
- Apply activation function Softmax to calculate the output probability of Tweet belonging to sentiment class  $S$ .

$$p(t_i|\hat{\theta}) = \frac{\exp(\beta_i^T \hat{\theta})}{\sum_{j=1}^s \exp(\beta_j^T \hat{\theta})}$$

**Step 9:** For each  $t \in T_{test}$

Classify the sentiment polarity of the real time tweets using trained model.

---

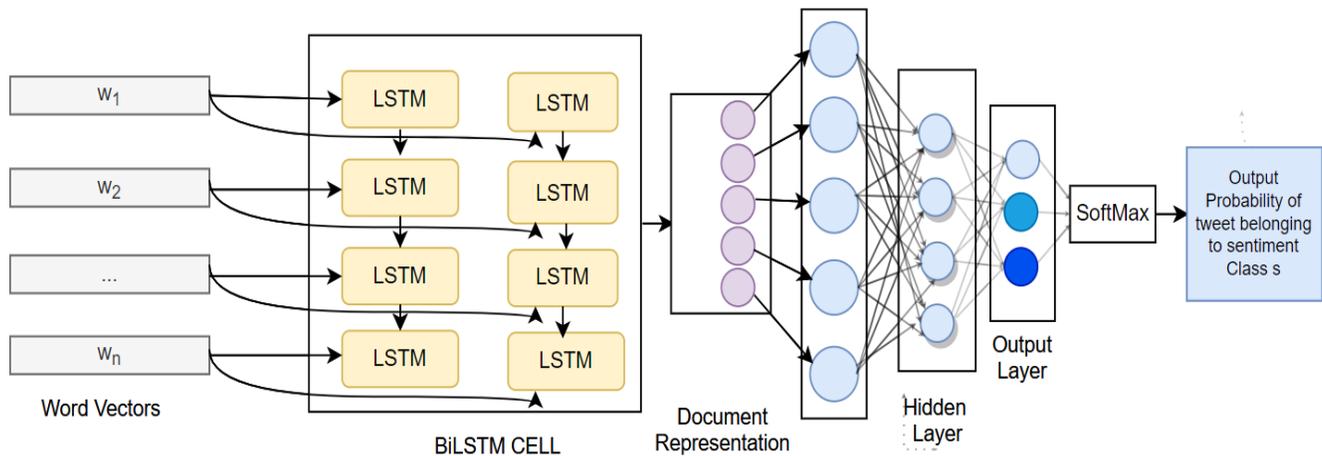


Fig. 5. Working of Sentiment Analyser.

## VI. CORRELATING CRIME AND TWEETS

We have used Pearson’s correlation coefficient (r) as a statistical measure of the strength of a linear relationship between predicted crime pattern (Fig. 7) from tweets and actual crime reported by news portals and media (Fig. 6). The correlation(r) between crime predicted and crime reported is shown in Table IV.

Pearson’s correlation coefficient (r)

$$r = \frac{N\sum xy - (\sum x \sum y)}{\sqrt{[(N\sum x^2 - (\sum x)^2)(N\sum y^2 - (\sum y)^2)]}}$$

$$r^2 = \frac{(N\sum xy - (\sum x \sum y))^2}{\sqrt{[(N\sum x^2 - (\sum x)^2)(N\sum y^2 - (\sum y)^2)]^2}}$$

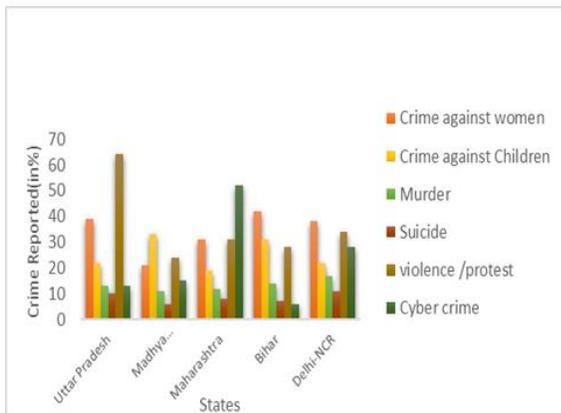


Fig. 6. Crime Incidents Reported from 2 Dec 2019 to 22 Dec 2019 as Per NCRB and News Portals.

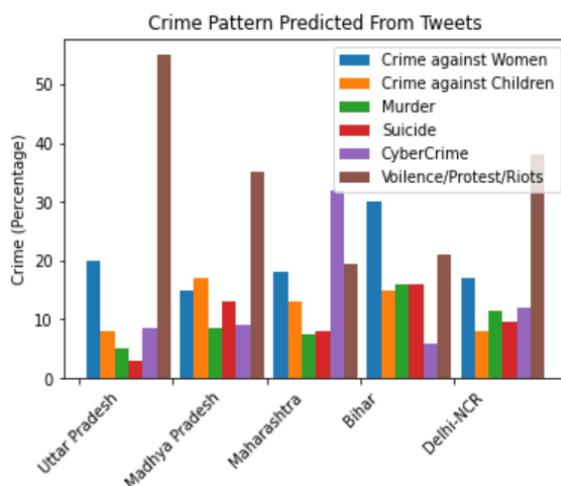


Fig. 7. Crime Pattern Predicted from Tweets from 2 Dec 2019 to 22 Dec 2019.

TABLE IV. HYPOTHESIS TESTING

	r	r <sup>2</sup>	t-test stat	p-value
<b>Crime against Women</b>	0.7927	0.6284	2.2522	0.1079
<b>Crime against Children</b>	0.7978	0.6365	2.2918	0.1057
<b>Murder</b>	0.3722	0.1385	0.6945	0.5372
<b>Suicide</b>	-0.2218	0.0492	-0.3939	0.7209
<b>Cyber Crime</b>	.9499.	0.9023	5.2639	0.1333
<b>Violence protest</b>	0.8068	0.6509	2.3652	0.0989

## VII. HYPOTHESIS TESTING

Null hypothesis Ho: Publicly available data from Twitter do include features that can portray a correlation between Crime pattern predicted from Tweets and the actual Crime incidents reported.

Alternative hypothesis Ha: Publicly available data from Twitter do not include features that can portray a correlation between Crime pattern predicted from Tweets and the actual crime reported.

p-value: The p-value tells us if the result of an experiment is statistically significant (significance level=0.05). The p-value is calculated using a t-distribution, with (n-2) degree of freedom.

$$t\text{-test Statistics} = \left\{ \frac{r \cdot \sqrt{n-2}}{\sqrt{1-r^2}} \right\}$$

Since the p-value is larger than 0.05 as shown in Table IV, we fail to reject null hypothesis and we cannot conclude that a significant difference exists.

## VIII. CONCLUSION

In this paper, we have tried to predict crime pattern using geo-tagged tweets from five regions of India. We hypothesized that publicly available data from Twitter may include features that can portray a correlation between Tweets and the Crime pattern using Data Mining. We have further applied Semantic Sentiment Analysis using BiLSTM and feed forward neural network to the tweets to determine the crime intensity across a region. BiLSTM is a variant of LSTM and is more powerful than LSTM as it overcomes the problem of gradient explosion that occurs in LSTM. The purpose of combining these two approaches was to exploit the strength of BiLSTM and feed forward neural network. The performance of the classifier is 84.74 for each class of sentiment. The results showed correlation between crime pattern predicted from Tweets and actual crime incidents reported. The main limitation of our study was unavailability of geo-tagged tweets as more than half of twitter users prefer to conceal their location due to privacy issues. We hope to further make our research effective by using open mapping from Google. The data used in the research is available on-line on Twitter to support further investigation.

## REFERENCES

- [1] M. A. Russell, Mining the Social Web. OReilly, 2<sup>nd</sup> ed. October 2013.
- [2] M. Suresh, D. Nagendrababu, S. Nakkiran, and K. Vanjinathan, “A Survey on Personality Prediction Using Digital Footprints in Social Media”, International Research Journal of Engineering and Technology, vol. 03, no. 02, pp. 1787–1793, 2016.
- [3] Y. Wang , “Using Social Media Mining Technology to Assist in Price Prediction of Stock Market”, IEEE International Conference on Big Data and Analytics ICBDA, vol. 07, pp.143-147, 2016.
- [4] J. Ramteke and D. Godhia, “Election result prediction using Twitter sentiment analysis,” International Conference on Inventive Computation Technologies (ICICT), pp.122-128 ,2016.
- [5] S. Shim and M. Pourhomayoun, “Predicting Movie Market Revenue Using Social Media Data”, IEEE International Conference on Information Reuse and Integration, vol. 04, no.1, 2017.
- [6] S. Sathyadevan, M. S. Devan, and S.S.Gagadharan, “Crime analysis and prediction using data mining”, International Conference on Soft Computation. ICNSC 2014., vol. 14, pp. 406–412, 201.
- [7] J. Chan and L.B. Moses, “Is Big Data challenging criminology?,” Theoretical Criminology, vol. 20, issue 1, pp. 21-39, 2016.

- [8] M. S. Gerber, "Predicting crime using Twitter and kernel density estimation", *Decision Support System*, vol. 61, no.1, pp. 115–125, 2014.
- [9] X. Wang, M.S. Gerber and D.E. Brown, "Automatic crime prediction using events extracted from twitter posts, in *Social Computing, Behavioral-Cultural Modeling and Prediction*," Springer, 2012, pp. 231–238.
- [10] X. Chen, Y. Cho and S.Y. Jang, "Crime prediction using twitter and weather," *Systems and Information Engineering Design Symposium (SIEDS)*, IEEE, 2015, pp. 63–68.
- [11] T. Brandt, J. Bendler, and D. Neumann, "Information & Management Social media analytics and value creation in urban smart tourism ecosystems," *Information and Management*, vol. 54, no. 6, pp. 703–713, 2017.
- [12] N. Malleson and M.A. Andresen, "The impact of using social media data in crime rate calculations: shifting hot spots and changing spatial patterns," *Cartography and Geographic Information Science*, 42(2), pp.112–121, 2015.
- [13] N. Zainuddin, A. Selamat, and R. Ibrahim, "Improving Twitter AspectBased Sentiment Analysis Using Hybrid Approach," *Intelligent Information and Database Systems*, vol. 9621, N. T. Nguyen, B. Trawiński, H. Fujita, and T.-P. Hong, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 151–160.
- [14] B. Gokulakrishnan, P. Priyanthan, T. Ragavan, N. Prasath, and As. Perera, "Opinion mining and sentiment analysis on a Twitter data stream," 2012, pp. 182–188.
- [15] V. N. Patodkar and S. I.R, "Twitter as a Corpus for Sentiment Analysis and Opinion Mining," *IJARCCCE*, vol. 5, no. 12, pp. 320–322, Dec. 2016.
- [16] B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up?: sentiment classification using machine learning techniques," in *Proceedings of the ACL-02 conference on Empirical methods in natural language processing* vol 10, 2002, pp. 79–86.
- [17] S. Aghababaei and M. Makrehchi, "Mining Social Media content for crime Prediction," *IEEE/WIC/ACM International Conference of Web Intelligence*, vol. 13, pp. 526–531, 2016.
- [18] A. Almealmadi, "Language Usage on Twitter Predicts Crime Rates," *Security of Information and Networks 2017*, pp. 307–310.
- [19] A. Ristea, M. Leitner, and M. A. Andresen, "Opinion mining from Twitter and spatial crime distribution for hockey events in Vancouver," *AGILE 2018*, pp. 1–7.
- [20] P. Siriaraya, Y. Wang, and A. Jatowt, "Witnessing Crime through Tweets :A Crime Investigation Tool based on Social Media," *International Conference on Advances in Geographic Information Systems 2019*, pp. 568-571.
- [21] L. Alfantoukh and A. Durresi, "Techniques for collecting data in social networks", *International Conference on Network-Based Information Systems NBIS*, vol. 20, pp. 336–341, 2014.
- [22] A. Graves and J. Schmidhuber, "Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures," *Neural Networks*, vol. 18, no. 5-6, pp. 602–610, June/July 2005.

# A Hybrid Model for Documents Representation

Dina Mohamed<sup>1</sup>, Ayman El-Kilany<sup>2</sup>, Hoda M. O. Mokhtar<sup>3</sup>  
Faculty of Computers and Artificial Intelligence, Cairo University, Giza, Egypt

**Abstract**—Text representation is a critical issue for exploring the insights behind the text. Many models have been developed to represent the text in defined forms such as numeric vectors where it would be easy to calculate the similarity between the documents using the well-known distance measures. In this paper, we aim to build a model to represent text semantically either in one document or multiple documents using a combination of hierarchical Latent Dirichlet Allocation (hLDA), Word2vec, and Isolation Forest models. The proposed model aims to learn a vector for each document using the relationship between its words' vectors and the hierarchy of topics generated using the hierarchical Latent Dirichlet Allocation model. Then, the isolation forest model is used to represent multiple documents in one representation as one profile to facilitate finding similar documents to the profile. The proposed text representation model outperforms the traditional text representation models when applied to represent scientific papers before performing content-based scientific papers recommendation for researchers.

**Keywords**—Document representation; latent dirichlet allocation; hierarchical latent dirichlet allocation; Word2vec; Isolation Forest

## I. INTRODUCTION

With the rapid growth in the volume of text data and documents over the internet from social media, news articles, scientific papers, and surveys; it becomes a critical issue to find an effective model to represent the text features in the documents before using them in text mining, information retrieval, and recommendation systems. Bag-Of-Words (BOW) model is one of the most popular models for representing documents [1]. It relies on the frequencies of the words within the documents for building the document vector with a fixed length, while it fails to capture the word importance through a collection of documents. Also, BOW doesn't perform well when representing a huge number of documents due to the increasing number of words; which in turn causes a sparse document vector. Term Frequency Inverse Document Frequency (TF-IDF) model has been applied for representing the document as a numeric vector [2, 3]. It measures the importance of the words in a collection of documents, accordingly, the frequent words that appear in many documents such as (if, what, the ...) take a low weight and the rare words that focus on the document purpose take a high weight. TF-IDF model is used in many types of research for information and queries retrieval [4, 5], but it fails to capture the semantics behind words and neglects the order of the words in the documents. With the vital need to capture the semantics of the words to build an effective model for document representation, topic modeling techniques have been proposed for representing documents. Latent Dirichlet Allocation (LDA) is a well-known topic modeling technique [6], in which the documents are represented as a distribution

over a set of latent topics that are generated from a set of documents' words. For deeper representation; hierarchical Latent Dirichlet Allocation (hLDA) which is an extension of the LDA model was developed to learn the hierarchical structure for topics from a collection of documents[7]. Recently, word embedding techniques that represent words and documents (e.g. word2vec and doc2vec) as a numeric vector using neural networks were introduced. Word2vec model builds a representation for words as dense vectors depending on the word's context [8].

In this paper, we aim to build a document representation model that exploits the advantages of hierarchical topic modeling (hLDA) and the word2vec model to represent the document as a hierarchical tree of topics. The proposed model starts with building the hierarchical tree of topics with  $n$  levels from a corpus of a collection of documents. The resulting topics are transformed into numeric vectors using words' vectors resulting from the word2vec model. Then, each document is represented as a hierarchy of topics using the similarity scores between document vector and topic vectors. Once we have a document representation, an isolation forest model is built to represent multiple documents altogether in one representation as a single profile. The resulting profile model is then used to find similar documents to a multiple set of documents that were joint through the profile. The main contributions of this paper are centered around two main points. First, the paper proposes a hierarchy-based representation for a text document that integrates the hierarchical topic modeling and the word2vec model. Second, the paper proposes a unified representation for multiple documents altogether as one profile using the isolation forest model.

We argue that the conjunction between the hierarchical structure of topics and the word vectors would allow a better understanding of the document semantics and consequently a better recommendation. Also, we argue that grouping multiple documents as one profile using the isolation forest model would allow a better representation of the whole set of documents rather than considering each of them individually. To prove our arguments, experiments were conducted using a dataset for scientific papers that contains a set of research papers described by their titles and abstracts, and a set of researchers with their preferred papers. The proposed model was used to represent each paper individually. Then, a subset of each researcher's preferred papers was aggregated as the researcher profile using their representations. Researchers' profiles were used to recommend papers to the researcher where the recommendation results outperform other semantic-based representation models like LDA with word2vec combination [9], and concept-based representation [10].

The paper is organized as follows. In Section II; background about the topic modeling techniques, word2vec model, isolation forest model, and recommendation systems is introduced. Section III discusses the related work while Section IV explains the proposed model. Sections V and VI present the performance evaluation and discussion, respectively. Section VII concludes the paper.

## II. BACKGROUND

### A. Topic Modeling

Topic Modeling is an unsupervised machine learning technique that identifies the latent topics behind the text corpus of a set of documents. Latent Dirichlet Allocation (LDA) [6] is one of the main topic modeling methods. It represents the document as a distribution over a mixture of topics with a certain probability, while each topic is represented as a distribution over a mixture of words. Fig. 1 shows an example for the LDA documents representation, at first, the number of topics  $K$  is defined, and then each word in the documents is randomly assigned to a topic. The assignment process is repeated until all words are assigned to their correct topics. Finally, the documents are represented as a distribution over a mixture of topics with a certain probability.

The LDA graphical representation model is shown in Fig. 2. It shows two boxes “plates”; the outer one is for representing the collection of documents and the inner is for the words in the document associated with the topics where  $M$  denotes the documents number in the collection,  $N$  is the number of words in specific documents,  $w$  is a specific word in the documents,  $z$  is the topic assigned to the word,  $\theta$  is the topic distribution for the document, while  $\alpha$  and  $\beta$  are the parameters of the Dirichlet,  $\alpha$  for a document- topic distribution and  $\beta$  for word-topic distribution. In this graphical model, the gray node represents the observed variables as the only observed variable is the word  $w$ , where the other nodes are latent. The arrows are for representing the dependencies between the variables.

The LDA was later extended for discovering the complex structure of the topics. The hierarchical Latent Dirichlet Allocation (hLDA) model is one of the LDA model extensions while the topics are presented in a hierarchical structure [7] using the nested Chinese restaurant process (CRP) [11]. The hLDA model is used to define the topics for a collection of documents and these topics are organized in a hierarchical structure where more general topics appear near the top levels in the hierarchy and more specific topics appear near the leaves. Given a collection of documents and  $L$  levels of a hierarchical tree where each node in the tree belongs to a topic, the document is represented as a path from the root node of the tree to the leaf node. Then, a vector of topic proportions  $\theta$  is identified in addition to the words of each topic.

### B. Word2vec

Word2vec is one of the word embedding techniques that aim to map words to numeric vectors to capture the syntactic and semantics regularities behind the words [12]. It helps in natural language processing tasks [13], as it represents the words that have a similar meaning, with a similar

representation and similar position in vector so it becomes applicable in finding the relation between the words. The word vectors help answer analogy questions of the form ( $a: b$  as  $c: d$ ) where  $d$  is unknown. For example, the left panel of Fig. 3 illustrates that the relation (man: woman) is as (uncle: aunt) and (king: queen), as it discovers the gender relation between the words [14]. Also, it discovers the singular/plural relations between the words; as illustrated in the right panel of Fig. 3. The words vectors discover the relation between the words through applying algebraic operation between the words vectors for example when subtracting words vectors; vector (“king”) – vector (“man”) + vector (“woman”), its result is closest to the vector (“queen”).

Word2vec learns the distribution of words using neural networks. There are two word2vec models, the Continuous Bag of Words (CBOW) model and the Skip Gram model. CBOW model predicts the current word using its surrounding words in a specific window size. On the other hand, the Skip-gram model predicts the surrounding words using the current word; Fig. 4 illustrates the architecture of the CBOW model and Skip-gram model.

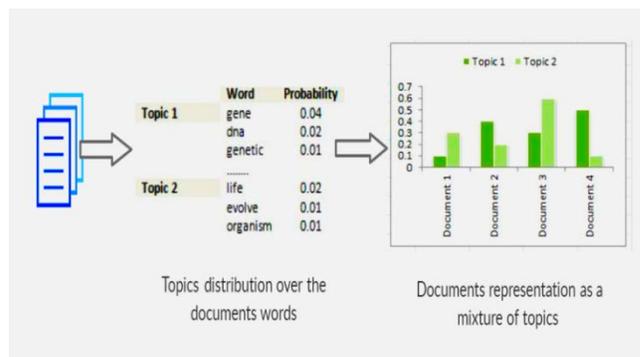


Fig. 1. The LDA Representation for the Documents.

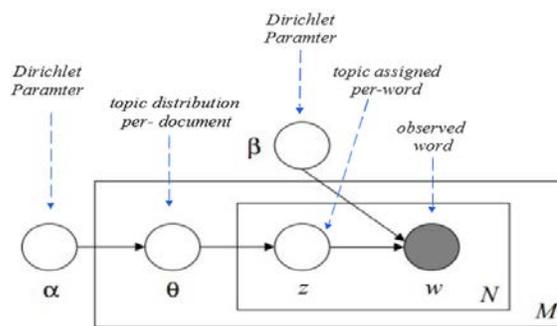


Fig. 2. LDA Graphical Model Representation [6].

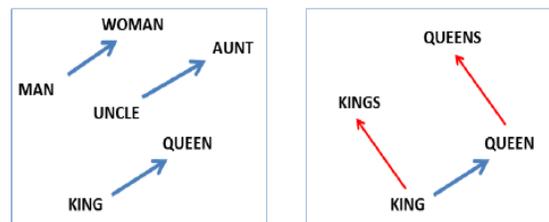


Fig. 3. The Panel shows the different Projection Relation between the Words [14].

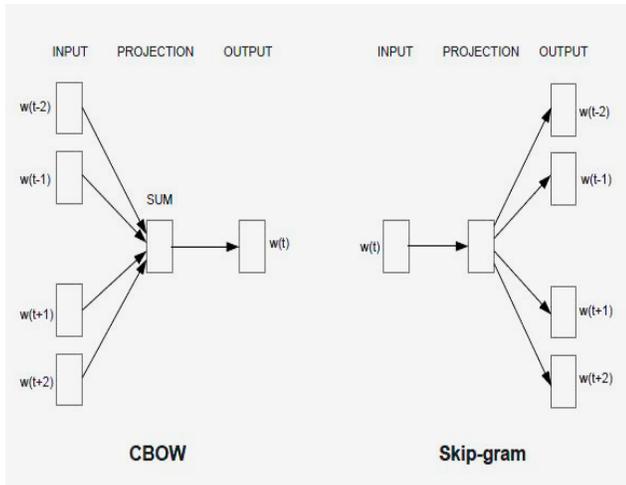


Fig. 4. The CBOW and Skip-gram Word2vec Models [12].

### C. Isolation Forest Model

Isolation forest is a decision-tree algorithm for unsupervised anomaly detection in high-dimensional datasets [15, 16]. In addition, it can be applied for semi-supervised anomaly detection where the dataset has normal instances only. The isolation forest model argues that the normal points are harder to be isolated than the anomalies points. To isolate any point in the data, the isolation forest model randomly selects a feature and a splitting value that lies between the minimum and maximum values for the feature to partition the data and assigns points to each split. Then, the partitioning process is repeated until all the points are isolated. While the normal instances need more partitions to be isolated, the anomaly instances require a low number of partitions. For example, suppose we have a two-dimensional dataset  $X = \{x_0, x_1, \dots, x_n\}$  with  $n$  number of points. Fig. 5 shows that the isolation of the point  $x_1$  which is considered to be a normal point would require more partitions, while the anomaly point  $x_0$  would require few numbers of partitions to be isolated.

In the isolation forest model, the repeatedly partitioning for the data points isolation can be represented in a tree structure (isolation tree). The anomalies would have shorter path lengths in the tree since they are easier to isolate than the normal instances. The isolation tree is constructed through repeatedly partitioning for the data points until all points are isolated or the tree reaches the determined height. The anomaly score is calculated using the average of all path lengths for the data points along with all features of the isolation tree where each path length is obtained by counting the number of edges from the root node to the termination node. The anomaly score for a point  $x$  in a data sample of size  $n$  is predicted by using Equation (1) [16].

$$s(x, n) = 2 \frac{E(h(x))}{c(n)} \quad (1)$$

Where  $E(h(x))$  is the average length of the path  $h(x)$  across all isolation trees for the point  $x$ , and  $c(n)$  is the average length for isolation trees for the given points, which can be calculated as the average path length of the Binary Search Tree (BST) [17]. Fig. 6 illustrates an example of an anomaly detection process using the isolation forest model.

The semi-supervised anomaly detection with the isolation forest model is processed in two stages; the training stage and the testing stage. The isolation trees are built in the training stage while in the testing stage the anomaly score is obtained for each test instance by passing it through the isolation trees to determine the path length in each tree before applying Equation (1).

### D. Recommendation Systems

The recommendation systems are used for suggesting items to users according to their interests, as it tries to predict the most appropriate items for the user's needs. There are three main methods for recommending items, Content-based filtering (CBF), Collaborative filtering (CF), and hybrid [19]. The content-based recommendation method analyzes the items' content to represent the interests of the users [20] and recommends similar items for the user's interests. CBF has widely used for recommending documents and news articles as it depending on analyzing the content of the items and build user profiles. On the other hand, CF recommends the items depending on users who have similar interests with the target user. It predicts the user rates for the unseen items using the rates of his / her correlated users who give a similar rate for the common items. The Hybrid method combines both methods to recommend the items to users.

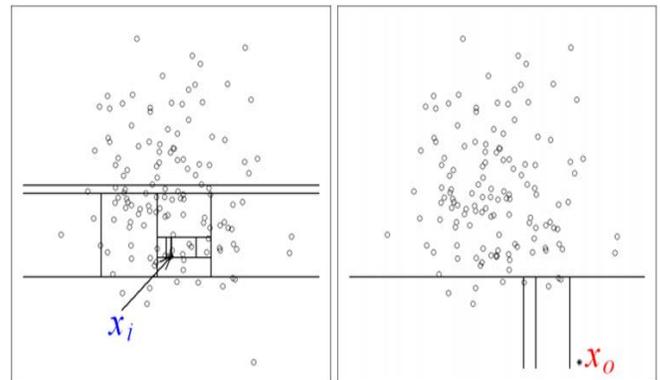


Fig. 5. Isolation for Anomalies Points [15].

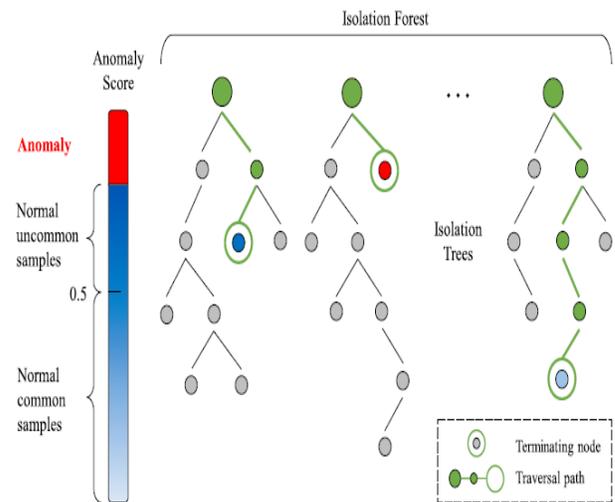


Fig. 6. Anomaly Detection using Isolation Forest [18].

### III. RELATED WORK

Text representation has been studied extensively in the literature, where different methods for representing the text through a variety of domains were proposed. The authors in [4] applied TF-IDF to represent the user's query and documents, to return the relevant documents to the user query. Also in [21] the authors designed a framework for document classification and measuring the similarity between the documents using the TF-IDF method and k-Nearest Neighbor (kNN) algorithm. Another semantic-based method of text representation is topic modeling techniques. For example, the authors in [22] utilized the LDA model to extract the concepts from the source code in software datasets to perform concepts analysis and visualization for software code and to find the similarity between the software programs. In [23] the author builds a topic model for contrastive opinion modeling to find opinions depending on a given topic. The authors in [24] introduced an online course recommendation system that recommends courses to students in a college while combining the content-based recommendation and LDA model, where the LDA model was used to discover the topics from the contents of the course and representing courses as a distribution over the topics. In [25] the authors developed the collaborative topic regression (CTR) model to recommend scientific articles to users by combining the collaborative filtering approach with probabilistic topic modeling that analyzes the latent topics in the content of the articles.

The researchers in [26] applied the hierarchical Latent Dirichlet Allocation (hLDA) model to analyze software program text and generate a feature tree to understand the software system, while the tree includes two hierarchies; feature hierarchy and file structure hierarchy. As the feature hierarchy for displaying the features from abstract to detailed levels and the file structure hierarchy for displaying the classes from whole to part. Also, the authors in [27] used the hLDA model to represent the legal documents as a hierarchy to measure the similarity between them before clustering them.

Recently, the word2vec model was widely used for representing the documents. In [28], the authors applied a multi labels classification for news articles where the word2vec model was applied to build a vector for words in news articles to capture the similarity between the words and then use those words vectors as a classification feature. The authors in [10] proposed a model for representing academic articles to recommend them to researchers. This method generates a set of concepts by clustering the word vectors that are learned from the word2vec model where the words with the same semantic meaning will be grouped in one concept. Then, those concepts are used to represent the articles as a distribution over the concepts.

Another research direction that applies a combination of multiple representation models to build an effective representation method to capture the semantics behind the text., For example, the authors in [9] developed a document

representation model that combines topics of the LDA model and word vectors of the word2vec model.

### IV. PROPOSED MODEL

The proposed model aims to build a document representation model that captures the semantics of the text in the documents. The proposed method starts by extracting the latent topics and the hierarchical relation between those topics using the hierarchical Latent Dirichlet Allocation model (hLDA) from the documents corpus. The latent topics are enhanced with the words' vectors generated from the Word2vec model. The document is represented as a feature vector that refers to how the document relates to each topic in the topics hierarchy. Then, the document representation is utilized to represent multiple documents as one profile. Fig. 7 shows the graphical representation model for the proposed model. Our model builds the documents' vectors through main four phases; text processing phase, topics hierarchy construction phase, document representation phase, and profile construction phase. The four phases are described in more detail as follows.

#### A. Text Processing Phase

In the text processing phase, documents are cleaned for the next phases. Each document is tokenized into words before removing the stop words. Stemming and lemmatization are also performed for each word and they are prepared for the hierarchical topic modeling process. The documents corpus after cleaning are used to train the word2vec model to produce the words' vectors for each word in the documents. The initial document representation vector is calculated as the average of its words' vectors using Equation (2) [9], where each document  $d$  contains  $n$  number of words  $w$  and  $v(w)$  denotes the word vector.

$$v(d) = \frac{\sum_{i=1}^n v(w_i)}{n} \quad (2)$$

#### B. Topics Hierarchy Construction Phase

In this phase, the hLDA model uses the documents' corpus returned from the text processing phase to build a hierarchy of topics where each topic is represented by a set of words and their probability for being related to the topic. While the more abstract topics appear near the root node of the hierarchy tree and the more specific topics in the leaves. Fig. 8 illustrates an example for part of the topic hierarchy generated from a collection of research papers. For topics representation in the hierarchy, we used the words' vectors that are generated from the word2vec model to construct a vector for each topic. The topic vector is calculated using Equation (3) [9], where each topic  $t$  is represented only with the top  $m$  words that have the highest probability associated with the topic. In addition,  $p(w_i)$  refers to the probability of  $w_i$  in topic  $t$  and  $v(w_i)$  is the vector of  $w_i$  that is generated by the word2vec model.

$$v(t) = \sum_{i=1}^m p(w_i) * v(w_i) \quad (3)$$

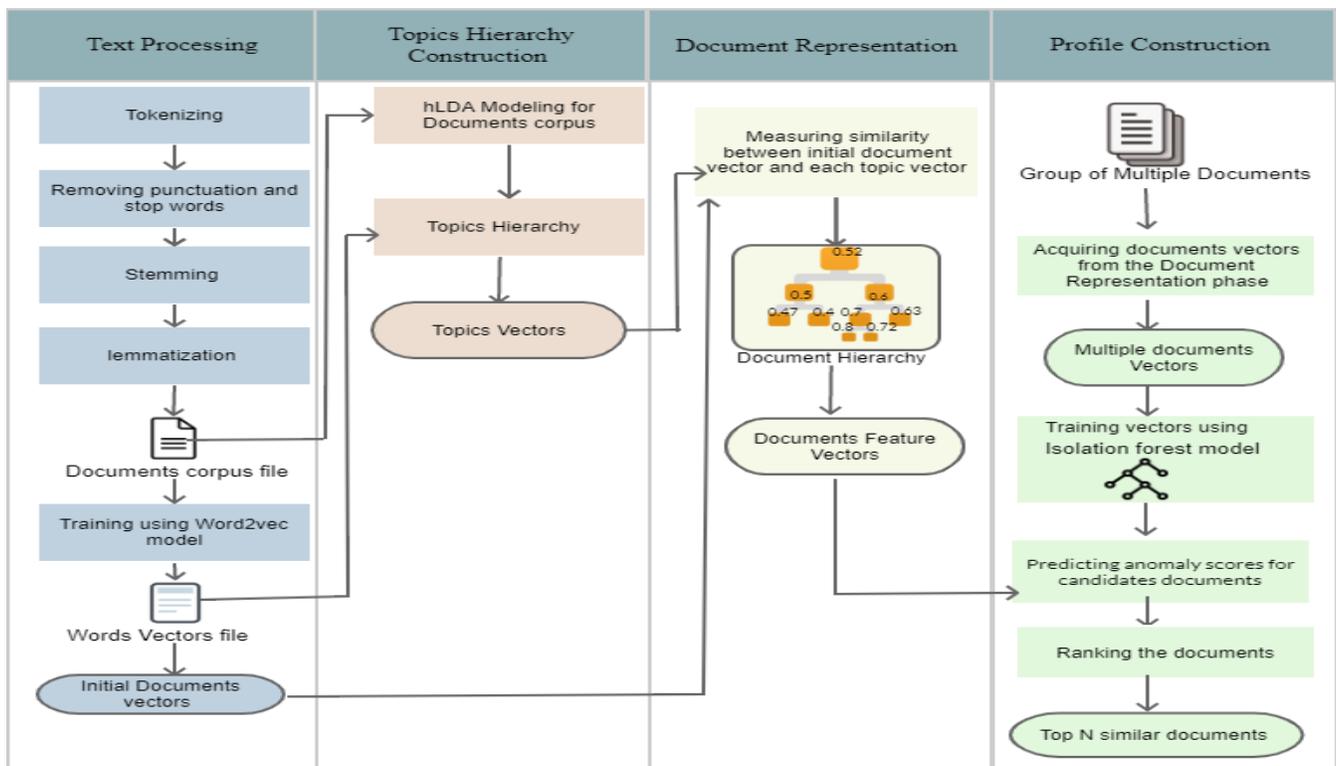


Fig. 7. Graphical Representation of the Proposed Model.

### C. Document Representation Phase

This phase uses the initial documents' vectors that were generated in the first phase and the topics vectors of the hierarchy of topics that were generated from the second phase to build the final document representation as a distribution over the hierarchy of topics. In this phase, we build a single feature vector for each document to use in constructing a profile for multi-documents. We calculate the cosine similarity [3] between the initial document vector and each topic vector in the topics hierarchy. The main advantage of using the cosine similarity is that the cosine similarity can measure the similarity between multi-dimensions vectors based on the orientation rather than the magnitude of the vectors, so it is more suitable for the initial documents vectors and the topics vectors which are multi-dimensional vectors. Equation (4) illustrates the calculation of the similarity between the document vector  $v(d)$  and the topic vector  $v(t)$ . Finally, each document is represented as a feature vector of the similarity scores of the topics hierarchy.

$$sim(v(d), v(t)) = \frac{v(d) \cdot v(t)}{\|v(d)\| \cdot \|v(t)\|} \quad (4)$$

### D. Profile Construction Phase

In this phase, we construct a representation for multiple documents where each group of documents is represented as one profile in order to identify the semantics behind those documents. The multiple documents' profile is constructed through the isolation forest model [15] in its semi-supervised setting. The isolation forest model considers the group of documents as a training dataset and predicts the anomaly score for each document in the testing dataset where the anomaly

score is obtained as described earlier in the background section. The anomaly score is used to indicate the similarity/dissimilarity between each group of documents in the training data and each document in the testing dataset where the high anomaly score would indicate high dissimilarity. Using the isolation forest model allowed the proposed model to represent the multiple documents as one profile and consequently find the similarity/ dissimilarity between each document in the test dataset and the generated profile using the predicted anomaly score.

## V. PERFORMANCE EVALUATION

In order to prove the proposed model's effectiveness, experiments were conducted through a recommendation system where the proposed model was used to represent scientific papers before doing content-based recommendations for the researchers. We used a dataset from CiteUlike<sup>1</sup>; CiteUlike is a site for helping researchers to share scientific papers and finding their preferred papers. This dataset consists of a collection of scientific papers and researchers, while each paper is described by its title and abstract, and each researcher has a list of his/her preferred papers. In the empirical experiments, a random subset of data is selected to measure the performance of the proposed representation model against different representation models. This subset contains approximately 6000 papers and 200 researchers. The proposed model was used to generate vectors' representation for each paper as described in Section IV. First, the text processing phase is performed on the papers. Then, the text generated from the text processing phase is trained using the continuous

<sup>1</sup> www.citulike.org.

bag of words (CBOW) word2vec model through the Gensim<sup>2</sup> library in python with a word vector of size 200. The hLDA model was trained on the paper's text to extract the latent topics and build the topics hierarchy with three levels, which generated 69 topics organized in the hierarchy structure. Fig. 8 shows part of the topics hierarchy that was generated, where each topic is represented by the top 20 words that have the highest probability of being related to the topic. Then, each topic is transformed into its vector representation using the words' vectors generated by the word2vec model. The final vector representation for each document is calculated by getting the similarity between the initial document vector and the topics vectors.

After following the first three phases in the model, a vector for each paper in the dataset is generated with the size of the number of topics in the hierarchy, where each value in the vector represents how the paper is related to the topic. The fourth phase joins each researcher's preferred papers into one profile in order to use it in the recommendation process. The list of the preferred papers for each researcher is divided into two datasets; training and testing, where the training dataset is used for building the profile for the researcher preferences using the isolation forest model [15]. The anomaly score is calculated for each paper in the whole collection of papers to determine the most similar papers to the target profile and how many of them exist in the testing dataset.

The performance evaluation is conducted using the recall evaluation metrics as applied in [29], as the recall function measures the fraction of positive patterns that are correctly recommended [30, 31], while in the dataset we only have the papers that the researchers prefer and there is no information about the papers that aren't preferred by the researchers. The recall is calculated for each researcher, while each researcher has a list of papers that he/she prefers, this list was divided into training and testing datasets. The recommendation system recommends the top N papers for the researcher; N is equal to the length of the testing dataset. The recall [31] is calculated using Equation (5).

$$Recall = \frac{tp}{tp+fn} \quad (5)$$

Whereas *tp* denotes true positive that refers to the number of papers that the researcher prefers from the top N recommend paper and *fn* denotes the false negative that refers to the number of papers that the researcher prefers and not recommended by the recommendation system. The overall recall of the recommendation system is computed by getting the average of all researchers' recall values. While the average recall result is validated with cross-validation technique as the dataset is divided randomly into 5 groups, each time one of the groups takes as a testing dataset and the remaining groups as the training, and the average recall is calculated each time.

We compared our model against the concept-based model [10] and the LDA+Word2vec model [9] given their similarity with the proposed model. Both of concept-based model and the LDA+Word2vec model applied the word2vec model to represent the words. In addition, both combined similar words

into different groups in a way or another. The concept-based model generates a set of concepts by clustering the words vectors that are learned from the word2vec model. Then, it uses the generated concepts to represent each document as a distribution over the concepts. On the other hand, the LDA+Word2vec model combines the LDA model and the Word2vec model and acquires the relationship between documents and topics using Euclidean distance. The proposed model, the concept-based model, and the LDA+Word2vec model are used to represent the scientific papers in the recommendation system to recommend papers to researchers depending on their preferred papers. In this experiment, the vector of size 50 was chosen as the number of topics in the LDA+Word2vec model. Also, the number of concepts in the concept-based model was set to 50. Whereas the vector size 50 is chosen based on the experiments that have been conducted for the concept-based model [10] for different sizes of the dataset with different vector sizes (10,30, and 50), while the best results were achieved using the vector of size 50.

The proposed model was compared against the concept-based model and the LDA+Word2vec model in two settings. In the first setting which we call without researcher profile setting, they were all compared without applying phase 4 of the proposed model where each paper vector was observed using different models and cosine similarity was used to find each researcher's most similar papers to his training dataset. In the second setting, each paper vector was observed using different models, and then the profile construction phase was applied to join the researcher training dataset as one profile in order to find the most similar papers to the profile. Both settings generated a list of recommended papers where recall measures were calculated using the number of papers that the researcher prefers from the list of recommended papers. Fig. 9 shows the results of the average recall for the recommendation system with and without building the profile while using different models for document representation.

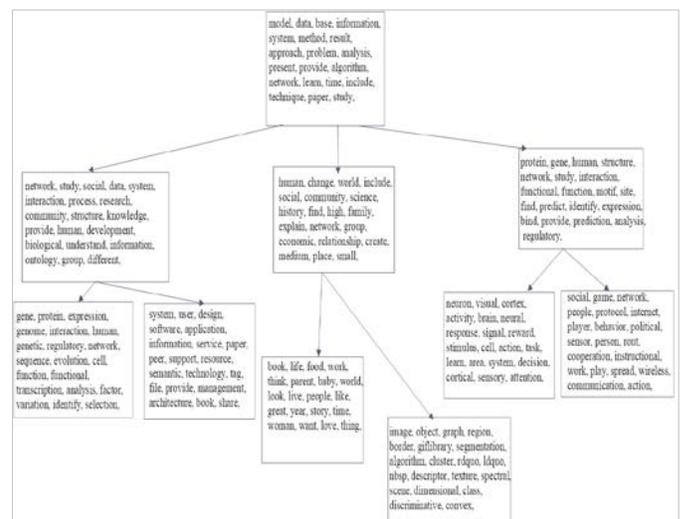


Fig. 8. Part of the Topics Hierarchy that Learned from a Collection of Scientific Papers.

<sup>2</sup> <https://pypi.org/project/gensim/>

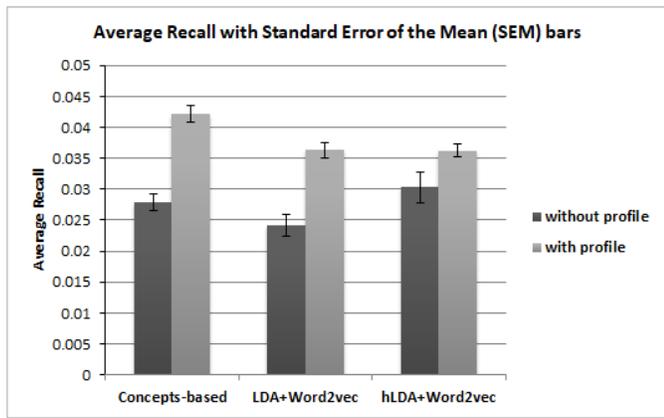


Fig. 9. Profile Effect on Average Recall Value.

Another experiment was conducted for the researchers who prefer a few papers only and the knowledge about their preference is scarce. We selected researchers who have between 10 and 20 preferred papers. The concept-based model, LDA+Word2vec model, and the proposed model were used to represent documents under the same two settings described previously in the previous experiment; once without researcher profile and once with the researcher profile. Fig. 10 shows the average recall results for each way of representation with and without building the profile.

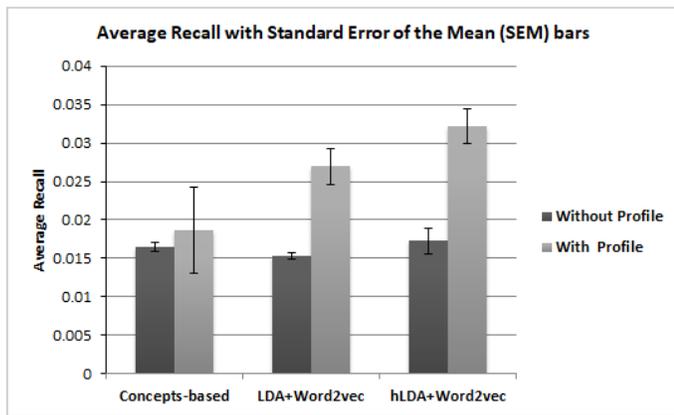


Fig. 10. Average Recall Values for Researchers with Few Preferences.

## VI. DISCUSSION

The previous section shows the experimental results of the performance evaluation for the proposed documents representation model against other representation models that exploit the topics and the concepts behind the documents corpus. The results are shown in Fig. 9 illustrate that without building a researcher's profile, the average recall of the proposed hierarchical document representation model is better than both the concept-based model [10] and the LDA+Word2vec model [9]. The proposed model improves the results of the recommendation systems for the dataset of size 6000 papers with 9% from the results of the concept-based model, and with 25% from the results of the (LDA+Word2vec) model. As the proposed model exploits the topics generated from the document and learns the hierarchical relation between those topics, the hierarchy allows the

representation of the document to contain a more coarse-grained description of the researcher's preferences rather than a fine-grained description. Such a coarse-grained description allows more diversity while generating recommendations.

In addition, Fig. 9 shows that all document representation models while building researchers' profiles perform better than the same models without building researchers' profiles. Profile construction for multiple documents enhances the results of the recommendation system by 51 % and 50 % for the concept-based model [10] and LDA+Word2vec model [9] respectively rather than the models without building a profile, and with 20% for the hLDA+Word2vec model. It also shows that the concept-based model returns the best recommendation results when building researcher profiles but also it is very close to the performance proposed model. By applying the isolation forest model for the collection of papers that are preferred by the researcher to build one profile for them, it becomes possible to capture the researcher's common interests and to decide the most related papers to the interests of the researcher which are considered as normal behavior. On the other hand, the researcher's insignificant interests would be considered as an anomaly behavior.

Another improvement was achieved by the proposed model while doing recommendations for the researchers who have a few numbers of preferred papers. As shown in Fig. 10, the proposed model outperforms other models for the dataset of the researchers that prefer only from 10 to 20 papers. The proposed model without building a profile performs better than the results of the concept-based model by 5%, and also better than the results of (LDA+word2vec) model by 13%. Those improvements show that the hierarchical representation for the topics was successful in capturing researchers' preferences when only a little information was available about them. This illustrates how the coarse-grained description of researcher preferences can be extremely successful in certain situations. In addition, the results presented in Fig. 10 confirm the advantage of building a profile for all recommendation models where the results of the concept-based model, LDA+Word2vec model, and (hLDA+Word2vec) model are enhanced by 13%, 76%, and 86%, respectively when the profile was used to represent researchers preferred papers.

## VII. CONCLUSION

In this paper, a novel document representation model is proposed. The proposed model combines different representation models into a more effective representation of the documents. More specifically, the model exploits the hLDA model to learn a hierarchy of topics that are generated from documents corpus, combined with the word2vec model to capture the semantics behind the document text. The proposed model introduces a representation for the multiple documents as one profile using the isolation forest model, to facilitate finding the similarity between the multiple groups of documents. The evaluation for the proposed model is conducted through different experiments for recommending scientific papers to researchers against similar methods that apply similar techniques; the concept-based model and the LDA+Word2vec model. The experiments show that the proposed model (hLDA+Word2vec) outperforms the concept-

based model with 9%, and the LDA+Word2vec model with 25% as the proposed method exploits the topics behind the documents corpus and the hierarchical relation between them in document representation. In addition, the experiments that are conducted for recommending papers for researchers who like a few numbers of papers show that the representation of papers using the proposed model enhances the recommendation system results from the concept-based model with 5%, and with 13% from the LDA+Word2Vec model. Also, the profile construction for the multiple documents as one profile using the isolation forest model improves the results for the different representation models with 51%, 50%, and 20% for the concept-based model, LDA+Word2vec model, hLDA+Word2vec model, respectively. Therefore, the recommendation system using the proposed model performs better than other methods, especially when using it for constructing a profile.

#### REFERENCES

- [1] Jones, K.S.: A statistical interpretation of term specificity and its application in retrieval. *J. Doc.* (1972).
- [2] Dillon, M.: Introduction to modern information retrieval: G. Salton and M. McGill. McGraw-Hill, New York (1983). xv+ 448 pp., \$32.95 ISBN 0-07-054484-0, (1983).
- [3] Salton, G., Buckley, C.: Term-weighting approaches in automatic text retrieval. *Inf. Process. Manag.* 24, 513–523 (1988).
- [4] Ramos, J., others: Using tf-idf to determine word relevance in document queries. In: Proceedings of the first instructional conference on machine learning. pp. 133–142 (2003).
- [5] Manning, C.D., Raghavan, P., Schütze, H.: Scoring, term weighting and the vector space model. *Introd. to Inf. Retr.* 100, 2–4 (2008).
- [6] Blei, D.M., Ng, A.Y., Jordan, M.I.: Latent dirichlet allocation. *J. Mach. Learn. Res.* 3, 993–1022 (2003).
- [7] Blei, D.M., Griffiths, T.L., Jordan, M.I., Tenenbaum, J.B.: Hierarchical topic models and the nested Chinese restaurant process. *Adv. Neural Inf. Process. Syst.* (2004).
- [8] Mikolov, T., Sutskever, I., Chen, K., Corrado, G.S., Dean, J.: Distributed representations of words and phrases and their compositionality. In: Advances in neural information processing systems. pp. 3111–3119 (2013).
- [9] Wang, Z., Ma, L., Zhang, Y.: A hybrid document feature extraction method using latent Dirichlet allocation and word2vec. In: 2016 IEEE First International Conference on Data Science in Cyberspace (DSC). pp. 98–103 (2016).
- [10] Mohamed, D., El-Kilany, A., Mokhtar, H.M.O.: Academic Articles Recommendation Using Concept-Based Representation. In: Proceedings of SAI Intelligent Systems Conference. pp. 733–744 (2020).
- [11] Blei, D.M., Griffiths, T.L., Jordan, M.I.: The nested Chinese restaurant process and Bayesian nonparametric inference of topic hierarchies. *J. ACM.* 57, (2010). <https://doi.org/10.1145/1667053.1667056>.
- [12] Mikolov, T., Chen, K., Corrado, G., Dean, J.: Efficient estimation of word representations in vector space. *arXiv Prepr. arXiv1301.3781.* (2013).
- [13] Collobert, R., Weston, J.: A unified architecture for natural language processing: Deep neural networks with multitask learning. In: Proceedings of the 25th international conference on Machine learning. pp. 160–167 (2008).
- [14] Mikolov, T., Yih, W., Zweig, G.: Linguistic regularities in continuous space word representations. In: Proceedings of the 2013 conference of the north american chapter of the association for computational linguistics: Human language technologies. pp. 746–751 (2013).
- [15] Liu, F.T., Ting, K.M., Zhou, Z.-H.: Isolation forest. In: 2008 Eighth IEEE International Conference on Data Mining. pp. 413–422 (2008).
- [16] Liu, F.T., Ting, K.M., Zhou, Z.-H.: Isolation-based anomaly detection. *ACM Trans. Knowl. Discov. from Data.* 6, 1–39 (2012).
- [17] Preiss, B.R.: Data structures and algorithms. John Wiley & Sons, Inc. (1999).
- [18] Chen, H., Ma, H., Chu, X., Xue, D.: Anomaly detection and critical attributes identification for products with multiple operating conditions based on isolation forest. *Adv. Eng. Informatics.* 46, 101139 (2020). <https://doi.org/https://doi.org/10.1016/j.aei.2020.101139>.
- [19] Ricci, F., Rokach, L., Shapira, B.: Introduction to recommender systems handbook. In: Recommender systems handbook. pp. 1–35. Springer (2011).
- [20] Pazzani, M.J., Billsus, D.: Content-based recommendation systems. In: The adaptive web. pp. 325–341. Springer (2007).
- [21] Trstenjak, B., Mikac, S., Donko, D.: KNN with TF-IDF based framework for text categorization. *Procedia Eng.* 69, 1356–1364 (2014).
- [22] Linstead, E., Rigor, P., Bajracharya, S., Lopes, C., Baldi, P.: Mining concepts from code with probabilistic topic models. In: Proceedings of the twenty-second IEEE/ACM international conference on Automated software engineering. pp. 461–464 (2007).
- [23] Fang, Y., Si, L., Somasundaram, N., Yu, Z.: Mining contrastive opinions on political texts using cross-perspective topic model. In: Proceedings of the fifth ACM international conference on Web search and data mining. pp. 63–72 (2012).
- [24] Apaza, R.G., Cervantes, E.V., Quispe, L.C., Luna, J.O.: Online Courses Recommendation based on LDA. In: SIMBig. pp. 42–48 (2014).
- [25] Wang, C., Blei, D.M.: Collaborative topic modeling for recommending scientific articles. In: Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining. pp. 448–456 (2011).
- [26] Sun, X., Liu, X., Duan, Y., Li, B.: Using hierarchical latent dirichlet allocation to construct feature tree for program comprehension. *Sci. Program.* 2017, (2017).
- [27] Venkatesh, R.K.: Legal documents clustering and summarization using hierarchical latent Dirichlet allocation. *IAES Int. J. Artif. Intell.* 2, (2013).
- [28] Rahmawati, D., Khodra, M.L.: Word2vec semantic representation in multilabel classification for Indonesian news article. In: 2016 International Conference On Advanced Informatics: Concepts, Theory And Application (ICAICTA). pp. 1–6 (2016).
- [29] Li, Y., Yang, M., Zhang, Z.M.: Scientific articles recommendation. In: Proceedings of the 22nd ACM international conference on Conference on information & knowledge management. pp. 1147–1156 (2013).
- [30] Manning, C., Schütze, H.: Foundations of statistical natural language processing. MIT press (1999).
- [31] Baeza-Yates, R., Ribeiro-Neto, B., others: Modern information retrieval. ACM press New York (1999).

# Predicting Internet Banking Effectiveness using Artificial Model

Ala Aldeen Al-Janabi

Ahmed Bin Mohammed Military College, Doha, Qatar

**Abstract**—This research aims at building a prediction model to predict the effectiveness of internet banking (IB) in Qatar. The proposed model employs the aspect of hybrid approach through using the regression and neural network models. This study is one of the fewest to evaluate the effectiveness of IB through adopting two data mining approaches including regression and neural networks. The regression analysis is used to optimize and minimize the input dataset metrics through excluding the insignificant attributes. The study builds a dataset of 250 records of internet banking quality metrics where each instance includes 8 metrics. Moreover, the study uses the rapidminer application in building and validating the proposed prediction model. The results analysis indicates that the proposed model predicts the 88.5% of IB effectiveness, and the input attributes influence the customer satisfaction. Also, the results show the prediction model has correctly predict 68% of the test dataset of 50 records using neural networks without regression optimization. However, after employment of regression, the prediction accuracy of satisfaction improved by 12% (i.e. 78%). Finally, it is recommended to test the proposed model in the prediction in other online services such as e-commerce.

**Keywords**—Artificial Neural Network (ANN); internet banking (IB); Artificial Intelligence (AI); e-banking effectiveness; regression model; rapidminer

## I. INTRODUCTION

The employment of various technological tools in banking industry can be classified under the umbrella of Electronic Banking (e-banking), and thus, e-banking can be defined as a variety of e-channels for carrying on the banking transactions through various technologies such as telephone, Internet, TV, computer and mobile [1]. Darwish and Lakhtaria [2] indicated that the e-banking transactions and services mainly depend on the information exchange between customers and banking services providers by means of technological methods without face-to-face interaction. Therefore, the technology growth has transformed the method banks deliver the services to customers [3]. The internet technology features add many advantages to e-banking such as fast financial transaction and low service cost, and thus, the Internet technology has a significant impact on e-banking [4]. In Internet banking, the online transaction platform play an important role in supporting several services such as online payment, online shopping, and internet stock trading [5], [6].

Despite of the internet banking advantages such as fast transaction, there are still many customers are not satisfied with the online banking services [7], [8]. Therefore, it is important to develop an assessment model to measure the effectiveness of internet banking in terms of customer satisfaction. Several

researches have explored the assessment of e-banking services quality using data mining methods such as neural, however, especially in Qatar; few have investigated the prediction of internet banking effectiveness in a comprehensive manner through a 2-stage model using prediction and neural models.

So, this research fills the gap in empirical studies because it tests the effect of the inclusion of two prediction model on the accuracy of e-banking evaluation. Additionally, it addresses the gap in literature the prediction using new dataset developed theoretical model derived from two models including TAM and D&M2003.

## II. LITERATURE REVIEW

This section explains the theoretical foundations of e-banking in addition to the study variables derived from D&M 2003 including the quality factors, customer satisfaction and usefulness.

1) *e-Banking*: In the financial industry, the Electronic Finance (e-finance) has recently become as a common trend where the e-finance denotes the use of electronic means and communication to provide the financial services including e-banking, internet banking (IB), electronic trading, and electronic payment [9]. Kumbhar [10] indicated that e-banking often denoted the online banking and some researchers explained that e-banking services has been developed and expanded because most of banking services are conducted via electronic channels such as ATM [11]. The e-banking term is used interchangeably when individuals talk about electronic financial banking services such as: net-banking, Web-banking and phone banking [12].

2) *Internet banking*: The internet banking (IB) is to perform the financial transactions without need for physical contact and it is considered as of the examples in employing technology in banking sector. Moreover, the internet banking is one of the essential parts of e-banking industry [13]. Many researchers identified the internet banking as internet portal that enable the customers to carry out various types of banking transactions and services using the internet [14].

3) *e-Service Quality*: It is pointed by many researchers that service quality is an essential measure for customer satisfaction where it has a significant impact on customer satisfaction and company financial performance as a whole [15], [16].

Service quality is considered as the most common topic in marketing to date as well as it is the pioneering work of

Parasuraman whereas the SERVQUAL has developed as a diagnostic tool for evaluating service quality. Marketing researchers (such as, Parasuraman et al., [17]) defined the service quality as the extent to which the service meets the expectations of customers. Service quality is also defined as the variation in customers' expectations for service performance before and after receiving service [18].

The service quality measures have been discussed by many researchers (such as, Petter et al. [19], Wang et al. [20], Alhendawi et al. [21]) SERVQUAL was developed as an assessment tool to measure service quality and it is widely used within IS Literature in order to measure the gap between customer's expectations and experience. This instrument (i.e. SERVQUAL) have basically consisted of ten measures including tangible, reliability, competence, courtesy, responsiveness, access, credibility, communication, security and knowledge of customers. Later, the researchers Parasuraman et al. [17] filtered these measures and minimized them using factor analysis into five dimensions: tangibles, reliability, responsiveness, assurance and empathy in order to measure the service quality from the customers' point of view. Table I reveals the meaning of service quality's dimensions.

4) *Customer satisfaction*: Many researchers mentioned that customer satisfaction is considered as one of the critical issues for service organizations [22], [23], and also, it is highly important for measuring the quality of bank services [24], [25]. Based on review, it is obvious that the quality improvement has a positive impact on the customer satisfaction level which in turn positively influence the bank profitability [26]. Additionally, it is pointed by several researchers that service quality is the most important factor influencing customer satisfaction [27].

5) *Internet banking usefulness*: In the Web systems, the effective use of information for a given purpose [28]. However, the internet banking usefulness can be defined as the extent to which providers can ease the online services such as the financial transactions, online payment and others through adoption of new technological tools [29].

6) *Interactivity*: For Internet banking, interactivity can be defined as the degree to which the internet banking provides an interactive communication with customers [30], [31].

7) *Security*: The internet banking security means the extent to which the exchanged data is secured or protected from threats [32].

8) *Ease of use*: The ease of use can be expressed as one of Web system features where the users can use the system easily without paying much effort [33]. In Internet banking, ease of use indicates the user view of how easy to learn and use the online banking operations [34]. Thus, decision makers and managers should keep attention to the following metrics: bank services quality, usefulness, security, ease of use, and interactivity, as they are essentials for determining and improving the customer satisfaction. The following section represents the theoretical model which shows the relationships between the input and output data.

TABLE I. SERVICE QUALITY DIMENSIONS (ADAPTED FROM PARASURAMAN ET AL. [17])

No.	Dimension	Meaning
1	Tangible	Physical facilities, equipment and appearance of personnel
2	Reliability	Ability to perform the promised service dependably and accurately
3	Responsiveness	Willingness to help customers and provide prompt service.
4	Assurance	Knowledge and courtesy of employees and their ability to inspire trust and confidence.
5	Empathy	Caring, individualized attention the firm provides its customers.

### III. THEORETICAL FRAMEWORK

Based on the literature review (Alhendawi et al. [35], [36], Petter et al., [37], Delone & Mclean [38]), it is essential to use the quality factors such as service quality, security, privacy and usefulness as a success factors to identify the e-Banking system effectiveness in terms of customer satisfaction. Moreover, Alhendawi [39] indicated that the AI tools such as artificial neural network and regression can be considered as effective methods in predicting the e-Banking effectiveness as output variable (i.e. customer satisfaction). Accordingly, Fig. 1 reveals the proposed conceptual model used in the prediction of the e-Banking effectiveness in terms of customer satisfaction with Internet banking.

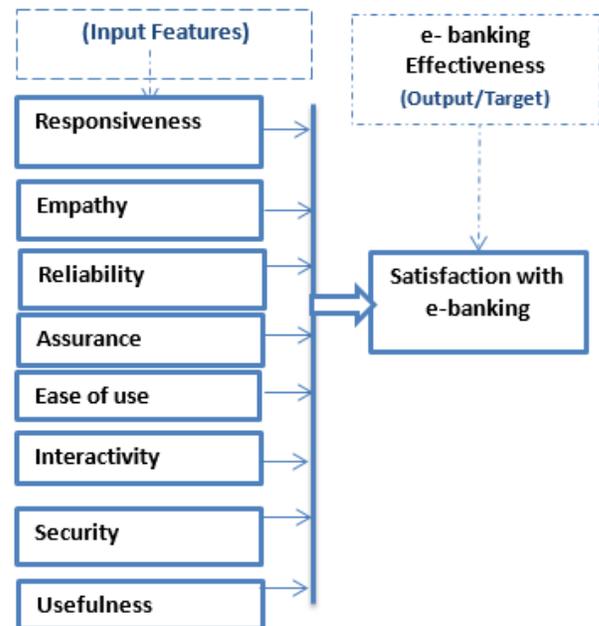


Fig. 1. The Proposed Theoretical Framework.

#### IV. RESEARCH METHODOLOGY

To achieve the research objectives, the authors adopt a methodology of two stages including Dataset and regression stage, and the neural model learning stage. Fig. 2 demonstrates the research methodological steps of the proposed prediction model.

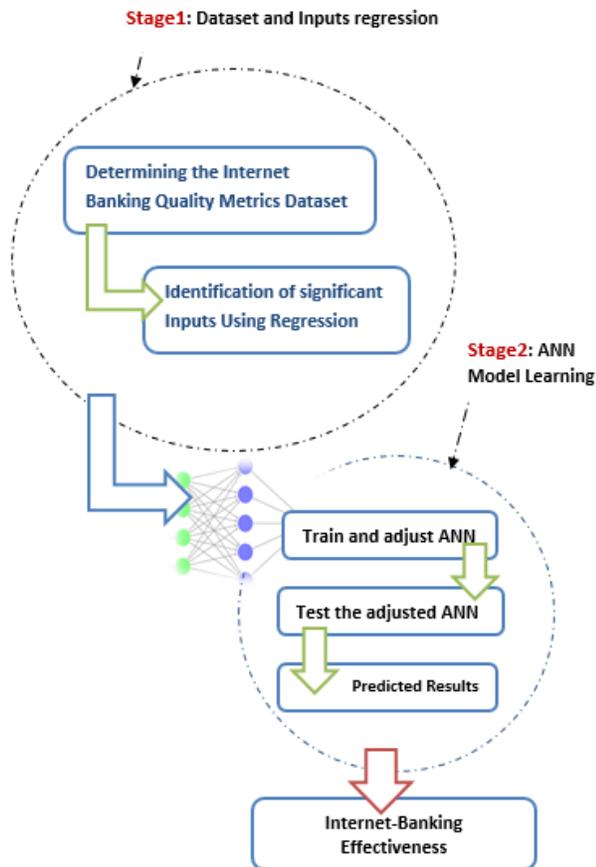


Fig. 2. The Research Methodology.

##### A. Stage 1: Building Data Set and Optimization

In this stage, an instrument or questionnaire of nine variables (i.e. factors) was built to include the service quality, security, usefulness, and interactivity, ease of use and satisfaction metrics of the Internet banking.

1) *Scaling*: A Likert scale of five points is used in order to measure the response of internet banking customers regarding the service quality, interactivity, security, ease of use, usefulness and effectiveness metrics. The metrics are rated by users from strongly agree to strongly disagree.

2) *Data collection*: The research includes the survey of 250 internet banking customers about their satisfaction with the IB system in Qatar. The survey includes the perceptions of IB users regarding nine metrics: four service quality metrics for responsiveness, reliability, assurance and empathy. The remaining five metrics are interactivity, security, ease of use, usefulness and effectiveness.

3) *Reliability*: The result of reliability test shows that the reliability of the research scales was relatively high. The value of Cronbach’s Alpha of the research scales as a whole was 0.90. Based on Table II, the value of Cronbach’s Alpha for the study scales of responsiveness, reliability, assurance and empathy, interactivity, security, ease of use, usefulness and effectiveness were 0.869, 0.918, 0.865, 0.717, 0.866, 0.864, 0.730, 0.881 and 0.916, respectively.

##### B. Building Dataset

Based to previous survey study analysis, there are eight causal factors or determinants (responsiveness, reliability, assurance and empathy, interactivity, security, ease of use, and usefulness) and one target (IB effectiveness). Because we have used a Likert scale of 5 points, we consider the mean of customer satisfaction to evaluate whether the IB system is effective or not.

##### C. Optimization and Regression

Based on the proposed method, the optimization is the final step of stage one in which the regression analysis is used to optimize the input attributes. The regression is employed to identify the significant input attributes in order to optimize the prediction process, and thus, the validation test of the proposed model takes into consideration the results of regression analysis as an input for neural networks prediction. The following chart shows the validation steps of the proposed model.

Fig. 3 shows the flowchart of prediction model validation in order to decide regarding the improvement of prediction accuracy of neural networks. It is clearly seen that the proposed model adopt the aspect of mix approach through using a 2-step prediction.

##### D. Implemented Neural Network Model

Based on the mentioned methodology, first, the Rapidminer is used to build the neural network model with eight input metrics and one output target (i.e. IB effectiveness). Fig. 4 shows the neural model of eight inputs metrics with one output.

Second, we applied the regression model to optimize the input dataset based on the significance of its elements, and then, implement the second neural network model with six significant inputs or metrics.

TABLE II. CRONBACH’S ALPHA OF STUDY VARIABLES

Variable	Cronbach’s Alpha
Responsiveness	0.869
Reliability	0.918
Assurance	0.865
Empathy	0.717
Interactivity	0.866
Security	0.864
Ease of use	0.730
Usefulness	0.881
Satisfaction with IB Effectiveness	0.916

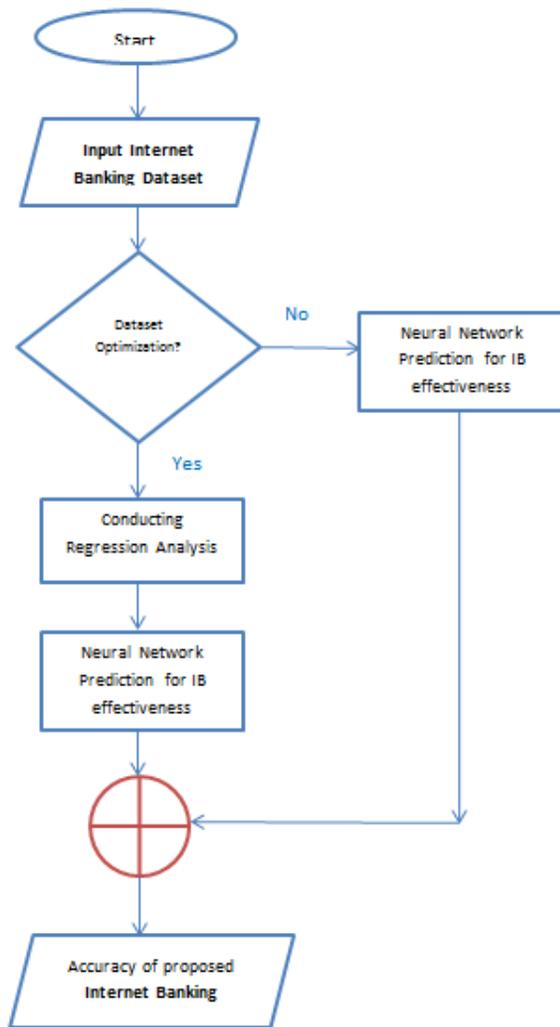


Fig. 3. Validation Process Flowchart.

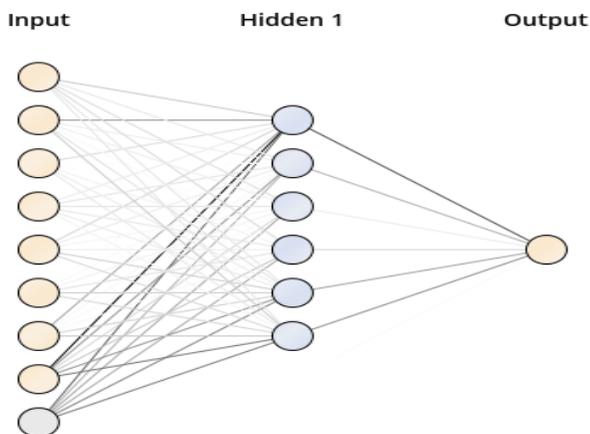


Fig. 4. The Neural Model.

## V. EXPERIMENTAL RESULTS AND FINDINGS

In this research, the regression and neural network models are employed to build the proposed evaluation model in order to gain the features of the two prediction models.

The proposed ANN model is trained by 250 records where the training data set includes 200 records. For validating and testing purposes, the researcher used 50 records as testing data.

### A. Regression

The regression analysis is used to specify the significant input attributes that contribute to the effectiveness of internet banking in term of customer satisfaction. Table III shows the significance of input attributes including: responsiveness, reliability, assurance, empathy, security, and usefulness, and interactivity, ease of use and satisfaction metrics of the Internet banking.

TABLE III. SIGNIFICANCE OF INPUT METRICS

Attribute	Correlation	t stat	Significance (P-Value)
Ease of use	0.009	0.355	0.723
Responsiveness	0.066	2.476	0.014
Assurance	0.078	2.841	0.005
Empathy	-0.029	-1.333	0.183
Reliability	0.051	2.086	0.038
Interactivity	0.096	3.492	0.011
Usefulness	0.069	2.276	0.002
Security	0.718	26.590	0.000
<i>R</i>	0.941		
<i>R</i> <sup>2</sup>	0.885		

Also, based on Table III, it is obvious that the input attributes contributes to the effectiveness of internet banking by 0.885, and therefore, the 8 input attributes contribute to the change in the customer satisfaction by a percentage of 88.5%. Additionally, it is shown that the two metrics ease of use, empathy are insignificant where the P-value for them are 0.723, 0.183; respectively. Generally, the proposed model metrics is suitable to predict the value of IB effectiveness. The following two subsections show the results of prediction before and after regression optimization.

### B. The Predicted Results before Optimization

Practically, 20% of data set are used as test dataset (i.e. 50 out of 200 records). The following shows the prediction accuracy of regression and neural models before optimization (i.e. before removing the insignificant attributes).

1) *The results of regression prediction:* The regression model results show that 32 of 50 effectiveness value can be correctly predicted. Table IV shows the regression prediction statistics where the eight input attribute are counted in the prediction model.

TABLE IV. REGRESSION STATISTICS

	Correctly predicted	Incorrectly Predicted	Prediction Success Ratio	No of input attributes
Regression	31	19	58%	8

2) *The results of neural networks prediction:* The neural model results show that 34 of 50 effectiveness value can be correctly predicted. Table V shows the neural prediction statistics where the eight input attribute are counted in the prediction model.

TABLE V. THE NEURAL PREDICTION STATISTICS WITH 8 ATTRIBUTES INPUTS

	Correctly predicted	Incorrectly Predicted	Prediction Success Ratio	No of input attributes
Neural	32	18	60%	8

Therefore, there is a slight difference in the prediction success ratios where the success ratios of regression and neural are 58% and 60%, respectively.

C. *Predicted Results after Optimization*

Based on the results shown in Table III, there are two insignificant attributes or metrics with p-value > 0.05. The two input metrics are ease of use and empathy. Based on the proposed prediction model, the significant input attributes resulted from regression are used as inputs for neural prediction. Thus, above two metrics are removed from the input attributes, and six significant attributes are used in the new neural prediction model.

Fig. 5 shows the neural network structure after optimizing the input attributes to become six attributes. Table V shows the neural prediction statistics where six-significant input attributes are counted in the prediction model.

Based on Table VI, the success prediction ratio after regression optimization (i.e. using 6 significant inputs) is 78% and this means the prediction is improved by 18%. This means after optimization of inputs, neural model succeeds in predicting 39 out 50 data elements which are obviously seen in Fig. 6.

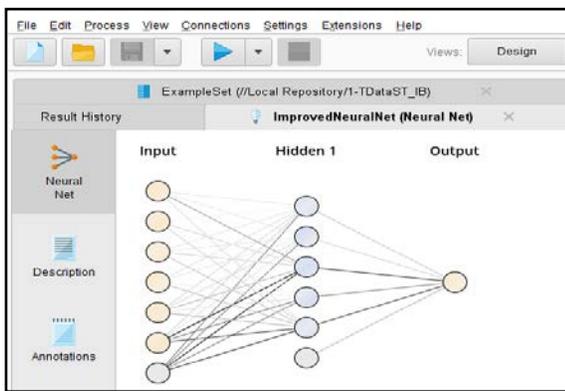


Fig. 5. The Neural Network after Regression.

TABLE VI. THE NEURAL PREDICTION STATISTICS WITH 6 ATTRIBUTES INPUTS

	Correctly predicted	Incorrectly Predicted	Prediction Success Ratio	No of input attributes
Neural	39	11	78%	6

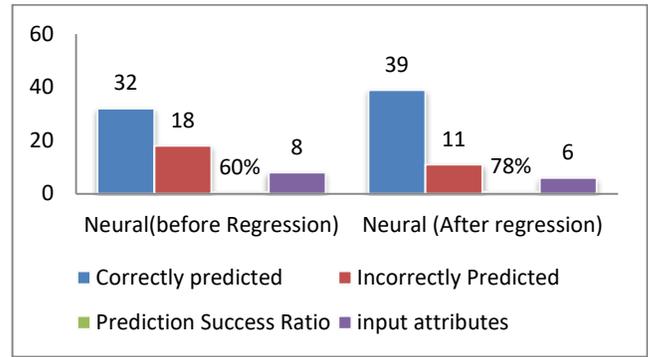


Fig. 6. The Success Ratios of Prediction.

Table VII shows the success status of the tested 50 cases where 1 denotes that the prediction of customer satisfaction succeeds, however, 0 means the proposed model fails to predict the satisfaction with Internet banking.

The following charts in Fig. 7, 8, 9, 10, 11 and 12 demonstrate the relationships between the internet banking effectiveness in terms of customer satisfaction and its predictors including responsiveness, reliability, assurance, empathy, interactivity, usefulness, ease of use and security.

D. *The Relationships between Input Attributes and Predicted Customer Satisfaction*

The x-axis represents the customer satisfaction attribute. In particular, Fig. 7 reveals that the attribute of responsiveness significantly influences the customer satisfaction with Internet banking.

TABLE VII. THE STATUS OF CASES PREDICTION

Case ID	Status	Case ID	Status	Case ID	Status
C1	1	C18	1	C35	1
C2	1	C19	1	C36	1
C3	1	C20	1	C37	0
C4	0	C21	0	C38	1
C5	1	C22	1	C39	1
C6	0	C23	1	C40	1
C7	1	C24	1	C41	0
C8	1	C25	1	C42	1
C9	0	C26	1	C43	1
C10	1	C27	1	C44	1
C11	1	C28	1	C45	1
C12	1	C29	1	C46	1
C13	1	C30	1	C47	0
C14	0	C31	0	C48	0
C15	1	C32	1	C49	0
C16	1	C33	1	C50	1
C17	1	C34	1		

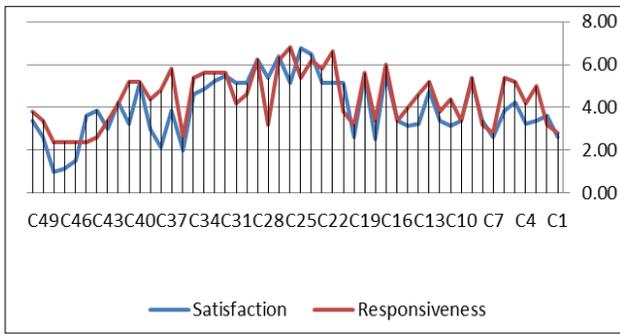


Fig. 7. The Impact of Responsiveness on Internet Banking Effectiveness.

Also, Fig. 8, 9, 10, 11 and 12 demonstrate that the remaining five attributes follow the same pattern, i.e. as the reliability, assurance, interactivity, security and usefulness attributes increased the customer satisfaction increased.

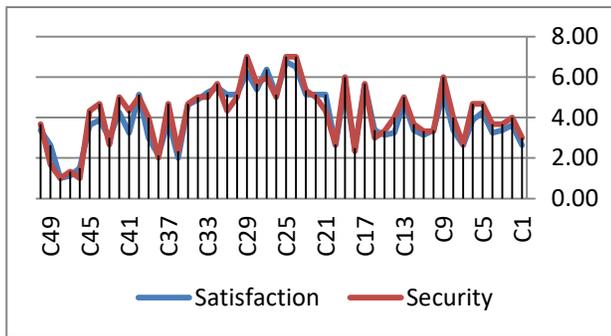


Fig. 8. The Impact of Security on Internet Banking Effectiveness.

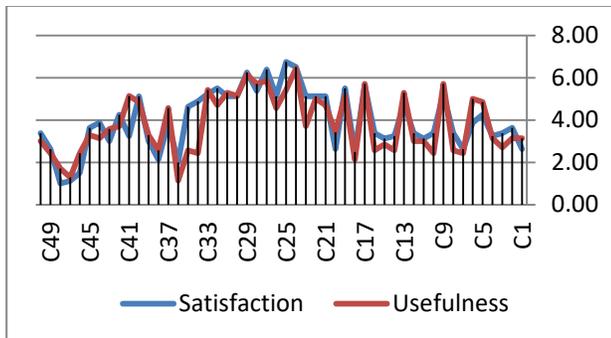


Fig. 9. The Impact of usefulness on Customer Satisfaction with IB.

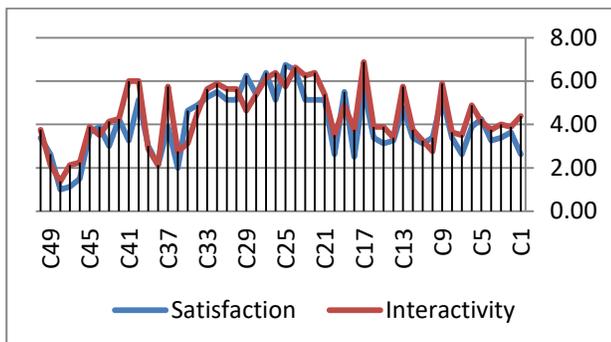


Fig. 10. The Impact of Interactivity on Customer Satisfaction.

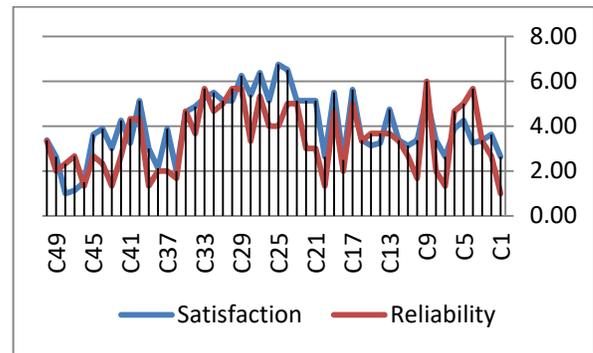


Fig. 11. The Impact of Reliability on Customer Satisfaction with IB.

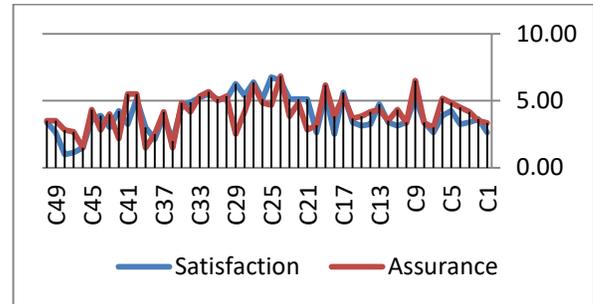


Fig. 12. The Impact of Assurance on Customer Satisfaction with IB.

Based on the correlation analysis of test data set, it is found the six attributes have a relatively high correlations with customer satisfaction with IB (i.e. correlation coefficient  $r > 0.5$ ). The highest four correlations are for the attributes: security, assurance, responsiveness, and usefulness (0.919, 0.696, 0.665 and 0.657), then the last two correlations are for interactivity and reliability (0.596 and 0.563).

## VI. CONCLUSION AND DISCUSSION

This research aims at evaluating the internet banking (IB) effectiveness based on the eight quality attributes: responsiveness, reliability, assurance, Empathy, interactivity, security, usefulness and ease of use. The questionnaire is used for gathering the dataset attributes regarding the internet banking services in Qatar. The dataset has 250 records divided into training and testing datasets by the percentages 80% for training and 20% for testing (i.e. 50 records).

The collected records were used as input dataset for regression model in order to optimize and find the significant input attributes, and then, the optimized 6 attributes are used to train the neural network model. Practically, a new hybrid approach using artificial neural network was proposed for determining the relationships between research variables. In this research, the rapidminer software is used to build the neural model using 8 inputs and one target (IB effectiveness).

The accuracy of the proposed model has been done by using a dataset of 50 records. The obtained results provided an evidence that the results of the proposed prediction model are suitable for handling the nonlinear relationships. Moreover, as the proposed ANN model correctly predicted 39 target values out of 50 (i.e. correct prediction percentage = 78 %), based on the results (i.e. improvement in prediction by 18%), the neural

network is useful in predicting the effectiveness of online services. Furthermore, it is found that the input attributes including responsiveness, reliability, assurance, empathy, interactivity, usefulness, ease of use, and security influence the internet banking effectiveness which is measured in terms of satisfaction. This research is one of the fewest to consider the eight input attributes as IB effectiveness predictors. Second, the research helps the decision makers to decide regarding the improvement of their online services, which in turn increase the customer satisfaction with online transactions such as internet banking services.

One of the major limitations of the research was that the proposed prediction model did not consider all customer satisfaction predictors. Second, the accuracy of prediction is reasonable (i.e. 78%), and thus, more improvement can be applied on the proposed intelligent model through to the other remaining quality attributes such as Technology Acceptance Model (TAM) attributes as predictors in the upcoming research.

#### REFERENCES

- [1] Olga. "Can e-banking services be profitable?." University of Tartu Economics and Business Administration Working Paper 30-2004 (2004).
- [2] Darwish, Ashraf, and Kamaljit I. Lakhtaria. "The impact of the new Web 2.0 technologies in communication, development, and revolutions of societies." *Journal of advances in information technology* 2.4 (2011), pp. 204-216.
- [3] Abd El Kader, Nermine. E-customer relationship management readiness in the banking industry: the case of Egypt. Diss. Middlesex University, 2012.
- [4] Bauer, Hans H., Maik Hammerschmidt, and Tomas Falk. "Measuring the quality of e-banking portals." *International journal of bank marketing* (2005).
- [5] Blut, Markus. "E-service quality: development of a hierarchical model." *Journal of Retailing* 92.4 (2016), pp. 500-517.
- [6] Bell, Emma, Alan Bryman, and Bill Harley. *Business research methods*. Oxford university press, 2018.
- [7] Chin, Wynne W. "Commentary: Issues and opinion on structural equation modeling." (1998), JSTOR.
- [8] Cohen, Jacob. *Statistical power analysis for the behavioral sciences*. Academic press, 2013.
- [9] Ziaee, Morteza. "Research on the internet and check the status of e-banking in Iran." *International Letters of Social and Humanistic Sciences* 10 (2014), pp. 172-180
- [10] Kumbhar, Vijay M. "Determinants of internet banking adoption: an Empirical evidences from Indian banking." *Indian Journal of Commerce and Management Studies* 2.4 (2011), pp.15-25.
- [11] Hussain, Zahoor, et al. "E-banking challenges in Pakistan: An empirical study." *Journal of Computer and Communications* 5.2 (2017), pp. 1-6.
- [12] Shanka, Mesay Sata. "Bank service quality, customer satisfaction and loyalty in Ethiopian banking sector." *Journal of Business Administration and Management Sciences Research* 1.1 (2012), pp. 1-9.
- [13] Oluwatolani, Oluwagbemi, Abah Joshua, and Achimugu Philip. "The impact of Information Technology in Nigeria's banking industry." *arXiv preprint arXiv:1108.1153* (2011).
- [14] Firdous, Sadaf, and Rahela Farooqi. "Impact of internet banking service quality on customer satisfaction." *The Journal of Internet Banking and Commerce* 22.1 (2017), pp. 1-17
- [15] Kadir, Hazlina Abdul, Nasim Rahmani, and Reza Masinaei. "Impacts of service quality on customer satisfaction: study of online banking and ATM services in Malaysia." *International Journal of Trade, Economics and Finance* 2.1 (2011).
- [16] ASHIQULLAH, S. "A relational study on automated service quality, customer satisfaction and financial performance in the context of Bank Asia Ltd available at: [ww.sb.iub.edu.bd/internship/summer2006/0320454.pdf](http://ww.sb.iub.edu.bd/internship/summer2006/0320454.pdf) (accessed January 28, 2016)." Summer internship report submitted to IUB University, Bashundhara (2006).
- [17] Parasuraman, A., Valarie A. Zeithaml, and L. Berry. "SERVQUAL: A multiple-item scale for measuring consumer perceptions of service quality." 1988 64.1 (1988), pp. 12-40.
- [18] Asubonteng, Patrick, Karl J. McCleary, and John E. Swan. "SERVQUAL revisited: a critical review of service quality." *Journal of Services marketing* (1996).
- [19] Petter, Stacie, William DeLone, and Ephraim R. McLean. "The past, present, and future of "IS success"." *Journal of the Association for Information Systems* 13.5 (2012).
- [20] Wang, Yi-Shun, and Yi-Wen Liao. "The conceptualization and measurement of m-commerce user satisfaction." *Computers in human behavior* 23.1 (2007), pp. 381-398.
- [21] Alhendawi, K., & Al-Janabi, A. "An Intelligent Neural Model for Assessing Web Systems Performance". *International Journal of advanced trends in computer science and engineering*, 2020, pp.1854-1860
- [22] Alhendawi, Kamal Mohammed, and Ahmad Suhaimi Baharudin. "The impact of interaction quality factors on the effectiveness of Web-based information system: the mediating role of user satisfaction." *Cognition, technology & work* 16.4 (2014), pp. 451-465.
- [23] Adepoju, Solomon Adelowo, et al. "Multi-Criteria Decision-Making Based Approaches in Website Quality and Usability Evaluation: A Systematic Review." *Journal of Information and Communication Technology* 19.3 (2020), pp.399-436.
- [24] Maranga, Wilfred Nyanusi. *Customer Perception of Electronic Banking Service Quality Provided By KCB Bank Kenya Ltd: A Case Study of UN Gigiri Branch*. Diss. United States International University-Africa, 2017.
- [25] Saha, Sampa, and Zinnatun Nesa. "Measuring service quality: a comparative assessment based on customer service of HSBC and DBBL." *Journal of Banking & Financial Services* 5.1 (2011), pp.111-127.
- [26] Ladhari, Riadh, Ines Ladhari, and Miguel Morales. "Bank service quality: comparing Canadian and Tunisian customer perceptions." *International Journal of Bank Marketing* (2011).
- [27] Megeid, Nevine Sobhy Abdel. "The impact of service quality on financial performance and corporate social responsibility: Conventional versus Islamic banks in Egypt." *International Journal of Finance and Accounting* 2.3 (2013), pp.150-163.
- [28] McKinney, Vicki, Kanghyun Yoon, and Fatemeh "Mariam Zahedi. "The measurement of web-customer satisfaction: An expectation and disconfirmation approach." *Information systems research* 13.3 (2002), pp. 296-315.
- [29] Hair Jr, Joseph F., et al. *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage publications, 2016.
- [30] Palmer, Jonathan W. "Web site usability, design, and performance metrics." *Information systems research* 13.2 (2002), pp.151-167.
- [31] Teo, Hock-Hai, et al. "An empirical study of the effects of interactivity on web user attitude." *International journal of human-computer studies* 58.3 (2003), pp. 281-305.
- [32] Janda, Swinder, Philip J. Trocchia, and Kevin P. Gwinner. "Consumer perceptions of Internet retail service quality." *International journal of service industry management* (2002).
- [33] Hair, Joseph F., et al. "Multivariate data analysis: A global perspective (Vol. 7)." (2010).
- [34] Kline, Rex B. *Principles and practice of structural equation modeling*. Guilford publications, 2015.
- [35] Mohammed Alhendawi, K. A. M. A. L., and A. H. M. A. D. Suhaimi Baharudin. "The assessment of information system effectiveness in e-learning, e-commerce and e-government contexts: a critical review of the literature." *Journal of Theoretical & Applied Information Technology* 95.18 (2017).
- [36] Alhendawi, Kamal Mohammed, and Ala Aldeen Al-Janabi. "An intelligent expert system for management information system failure

- diagnosis." International Conference on Intelligent Computing & Optimization. Springer, Cham, 2018.
- [37] Petter, Stacie, William DeLone, and Ephraim McLean. "Measuring information systems success: models, dimensions, measures, and interrelationships." *European journal of information systems* 17.3 (2008), pp. 236-263.
- [38] DeLone, William H., and Ephraim R. McLean. "The DeLone and McLean model of information systems success: a ten-year update." *Journal of management information systems* 19.4 (2003), pp.9-30.
- [39] Alhendawi, Kamal Mohammed. "Predicting the effectiveness of web information systems using neural networks modeling: framework & empirical testing." *International Journal of Software Engineering and Computer Systems (IJSECS)* 4.1 (2018): 61-74.

# Developing a Framework for Data Communication in a Wireless Network using Machine Learning Technique

Somya Khidir Mohammed Aaelmanan<sup>1\*</sup>, Mostafa Ahmed Hassan Ali<sup>2</sup>

Computer Science Department, College of Computer Engineering & Science

Prince Sattam Bin Abdulaziz University, P.O.Box 422, Alkharj 11942, Saudi Arabia<sup>1</sup>

Communication Engineering Departments, Faculty of Engineering, AL-Neelain University. Khartoum, Sudan<sup>2</sup>

**Abstract**—The emergence of Internet of Things (IoT) has become a huge innovation for utilizing the enormous power of wireless media. The adaptation of smart devices, with intelligent networking, has greatly enhanced the traffic of the IoT environment. The present security mechanism is primarily focusing on specific areas such as content filtering, monitoring techniques, and anomaly detection. A vulnerability reflects the inability of a network that allows an attacker to detect the extent of existing mechanism of security. The existing techniques focused on specific attacks rather than monitoring the whole network. However, there is a demand for a framework to govern and protect data and services in IoT network. Anomaly detection framework is a resource intensive activity to protect data and services of IoT / Wireless Sensor Networks (WSN). It supports application layer of IoT network and traces it frequently to find the existence of malicious activities. In this study, researchers proposed an anomaly detection framework to safeguard against wireless attacks. The proposed framework has employed a machine learning technique to detect the traces of wireless attacks. It supports IoT based networks to monitor the functionalities of the resources. In addition, it discusses the open challenges in IoT networks with possible solutions. Researchers employed a test bed for evaluating the proposed framework. The outcome of the study shows that the proposed framework provides better services with more security.

**Keywords**—Anomaly detection; internet of things; wireless attacks; artificial intelligence; machine learning

## I. INTRODUCTION

The technological developments in wireless communications and Artificial Intelligence (AI) technologies have enabled the design of WSNs, where sensor nodes capture and exchange intelligible data from their surrounding environments in a wireless form and transfer it to the proper destination. According to scientific publications, the total wireless sensor numbers used are projected to exceed 60 trillion at the end of 2022, representing 10,000 wireless sensors for each person worldwide [1]. Thus, all the WSN's problems and challenges will expose the researchers to abundant topics. WSNs have begun to draw interest in academics due to wireless technology and embedded electronics due to wireless technology's rapid technological growth [2]. A typical WSN consists of small devices known as nodes. These nodes are embedded CPUs, minimal CPU power, and smart sensors. WSNs are one of the most promising innovations for the third

millennium and have a broad range of applications globally. WSNs in different applications are commonly used because they have enormously attractive features such as low manufacturing costs, low installation costs, unattended network operations, autonomous operation and long service life [3]. By introducing Internet connectivity potential into sensor nodes and sensing abilities on internet-connected devices, WSNs began blending to the Internet of Things (IoT) [4]. IT will be incorporated into IoT during this time, and countless Sensor Nodes enter the Internet to co-operate with other nodes in order to sense and manage their environment. IoT revolutionizes the IT field and will be the next significant technological leap after the Internet. In the near future, IoT will provide connectivity between people and the world through the WSNs.[5] The WSN will provide IoT with Internet access to an immense quantity of data obtained from the WSNs. Therefore, IoT's safety should begin with securing WSNs before the other components in the first place. The IoT market is anticipated to increase to more than 75 billion in 2025 by over 15 billion devices in 2015[5]. It means on average that every human on Earth has a minimum of 25 IoT devices per person. It is now predicted that IoT will have a significant effect on our lives soon [6]. However, due to the absence of a physical line of defence, i.e. no dedicated infrastructure like gateways for detecting and controlling information flow in the network, security for WSNs and IoT is essential to the scientific community[8][9]. In particular, WSNs and emerging IoT technology can be an open route for attackers in the application domains, where the CIA (confidentiality, honesty, and availability) is primarily relevant. In addition, new integration and joint work between WSNs and IoT would open up new opportunities and security challenges. Regarding scalability, it is often challenging to implement IoT applications, which involve a large number of devices as time, memory, processing and energy constraints are limited [10]. For instance, calculating regular temperature changes across the country could require millions of devices and result in unmanageable data. Furthermore, the hardware used in IoT does have various operational features, such as sampling rates and error distributions, whereas IoT sensors and actuators are often too complex. All these factors are responsible for building up a heterogeneous IoT network in which IoT data are deeply heterogeneous. In addition, it costs a large amount of raw data to be distributed across the diverse and heterogeneous network. IoT requires compression of data and data fusion to

\*Corresponding Author

minimize the data volume. Therefore, it is desired to standardize the understanding of data care for future IoT. Furthermore, hackers, malware and viruses could disrupt data and information in the communication process. IoT is also commonly used in social life applications, such as smart grid, smart transportation and smart home [11]. IoT also contains access cards, bus cards and some other small apps. IoT software can make people more convenient, but private details can be leaked anytime if it cannot provide personal privacy protection. Once the IoT signal is stolen or disrupted, the entire IoT information's security is directly affected. The widespread IoT provides more information and will raise the risk of exposure to such information. On the one hand, IoT does not have the right security solution on the other hand, its innovations would be mostly limited.

WSN and IoT safety is an important problem, especially if commissioned with mission-critical tasks; for example, when a network safety gap leads to casualties for friendly forces on a battlefield in military tactic applications. A recent paper [12] revealed that the majority of the systems currently used fail to embed strong security services which can protect the privacy of patients. None of the patients would be glad if their sensitive health details were exposed to misbehaving nodes and system failures by leakage. The WSN secure algorithms and methodologies shall be applicable for any IoT consisting of one or more sensor networks. As previously reported, WSNs will most likely be implemented in the near future with IoT [13][14]. All cybersecurity problems, in particular attacks, prevention and mitigation are therefore very necessary to create a safe and secure IoT. WSNs are vulnerable to a number of attack methods that could pose essential security threats. These attacks may be linked to two major categories: active and passive [15][16]. In the category of passive attacks, attackers normally are disguised (camouflaged) and either damage the network components or use the connection to gather useful information. Passive attacks can also be classified into types of eavesdropping, disruption of nodes, malfunction of the node, node interrupt and monitoring of traffic. Whereas an attacker affects the roles and activities of the target network in the active attacks group [17][18]. The effect can be the actual target of the intruder and can also be identified by means of protection mechanisms (intrusion detection). For example, as a result of such attacks, network services can be interrupted. Flooding, Denial-of-Service (DoS), Blackhole, Wormhole, Sinkhole and Sybil types are some of the active attacks [19][20][21]. IoT security covers a range of areas, for example, attacks and countermeasures, protection, confidence, key distribution, patch management and access control. Therefore, IoT nodes can be managed via the Internet and sent sensed data (or sensed information data) to internet-based data sinks [21]. Today, IoT networks can also involve or communicate with new concepts like Big Data and Cloud/Configuration, etc.

The objective of the research is as follows:

- To propose an anomaly detection framework for IoT / WSN.
- To develop an interface to monitor the IoT / WSN environment using a machine learning technique.

- To suggest some possible solutions for open challenges in IoT / WSN.

The proposed framework supports IoT based networks to govern the resources and identify the anomalies. In addition, it overcomes the challenges in the existing framework. The existing techniques consider only a specific attack in the wireless network. The emergence of modern technologies leads to the development of new attacks in IoT network. Therefore, there is a demand for effective framework that can adapt to a newer environment and able to detect untraced anomalies.

The remaining part of the paper is structured as follows: Section 1 summarizes the concept of WSN, IoT with its security limitations, effects and future predictions, while Section 2 introduces different types of WSN and IoT attacks. Section 3 provides the proposed framework for secured IoT communications. The outcome of the study is presented in section 4. Section 5 discusses the open challenges and policies for monitoring IoT network. Finally, section 6 concludes the research with its future direction.

## II. RESEARCH BACKGROUND AND RELATED WORKS

WSNs are node arrays, and those nodes are computerized systems, respectively. These sensors usually work together to create centralized network systems [1] [2]. There are some criteria for using nodes such as reliability, multifunctionality and wireless use of these networks. In addition, each node in every network has a defined purpose. For example, if it is intended to gather microclimate information in a densely populated area, the nodes are positioned on a network of buildings or residential area throughout the specific region. In this network, the system for communication and data sharing should be centrally structured and synchronized. IoT not only has security threats similar to sensor networks, mobile communications and Internet however also specializes such like privacy issues, different network configuration authentication and access control issues, storage and administration of information, etc. One of IoT's application challenges is data and privacy security [3]. In IoT, RFID systems, WSN sensor systems are aware of the end of information technology which, with the password encryption technology, protects the integrity and confidentiality of information [7-9]. Many forms of encryption of data and information are available, including random hash lock protocol (hash function), hash chain protocol, infinite channel extract key, Encrypted ID, and so on [11-12]. Authentication of identity and access control can decide the correspondence between the two parties and reiterate each other's true identity, prevent covert attacks to ensure the authenticity, validity of data, and so on [15-17]. The transmission method has two significant security problems. One of the risks is the IoT security, and the other is the related network construction and implementation technology [15]. It should deal with the incompatibilities between various networks that are vulnerable to problems of protection, for instance, it is difficult to create the interconnection between the relationship as the relationship of trust among nodes are constantly changing; however, this can be solved through key management and protocol routing [18-20]. Security issues like DOS/DDOS attacks, forgery/middle attacks, heterogeneous network attacks, ipv6

application risk, and conflicts with the WLAN application also affect IoT's transport security [18][21]. Due to the huge volume of data, it is possible to create network congestion in the core network. The capability and connectivity problems such as space management, redundancy and security requirements in the reference framework should be taken into full account [21]. The security issues of application include access to and user authentication, the privacy of information, data stream destruction, reliability of the IoT network, middleware security, management platform, etc. To ensure technology protection and improve the aspect of basic safety and expectations of human behaviour, IoT usage is strongly tied to contemporary societies. In the meantime, research has also been carried out on people involved in CPS (cyber-physical systems) and overall computer protection. Sensitive IoT layers include Perception layer, transport layer and application layer. Hacker makes all IoT devices vulnerable in the network due to the limited handling capacity of IoT devices because they seemed to have a stronger signal than the actual access point with the same identifiability as the IoT service package. This allowed all network communications to be compromised to eavesdropping and Man in the Middle (MiM) attacks [21]. These scenarios for attacks have created a situation in which IDSs can be used in IoT networks to discover IoT devices vulnerabilities. The concept of IoT focuses on the intelligent incorporation of a specific physical world with the Internet in order to promote interaction; for this purpose, interconnections and dependencies in IoT environments with a number of heterogeneous environments. Any IoT device is therefore exposed to cyber threats in any related environment. Although IoT security threats can be divided widely into cyber- and physical realms, our survey is primarily concerned with cyber-threats, both active and passive attacks. IoT-based environments are subject to a range of physical and virtual dimensions of threat. Passive attacks are distinguished by a lack of changes in data or its flow, thus only affecting communications confidentiality and privacy. Passive attacks in some cases can allow IoT devices to be tracked locally. Active attacks include active change, alteration, and flow of information, but not limited to system settings, software and control messages. The IoT framework is used as a vector to launch large DDoS against Internet networks, and is also an aggressive attack. Since their large number and comparative ease of compromise, poor security standards and weak protection mechanisms, IoT systems are an effective vector for such attacks. Fig. 1 illustrates the user interface and network service attacks on IoT environment.

Most IoT systems use a certain kind of user interface to provide services to users via IoT systems (mobile, desktop or web application). The customer can monitor the case of smart home appliances through mobile applications. The rapid growth of smartphones has provided malicious entities with malware as innocuous mobile apps that they can publish without detection through applications. Often smartphones can also be hacked by bugs in platforms such as Android vulnerabilities. This results in exposure of malware compromise to all information that is stored on the telephone. The attacks allowed by user interface platforms include eavesdropping, location monitoring, DoS/DDoS, and bluejacking.

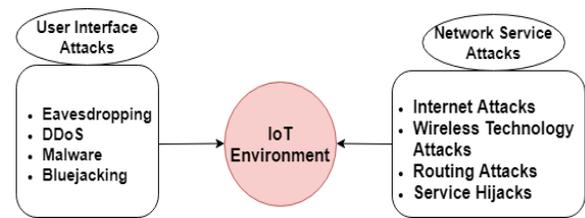


Fig. 1. IoT Attacks.

Network service attacks refer to the attacks targeted to the network configuration of IoT devices[6]. For instance, hackers target IoT devices configuration parameters in order to compromise the device and gain access. Wireless technology attacks are becoming familiar due to the emergence of sophisticated hacking tools. Using these kinds of tools, the IoT network can be hacked by the hackers. Internet and routing attacks means the unauthorized access of protocols of a network whereas the service hijacks indicate the unauthenticated usage of functionalities of IoT devices.

Based on the research background, researchers raised the following Research Questions (RQ).

RQ1 – How to detect anomalies in WSN / IoT network?

RQ2 – How to apply Machine Learning (ML) techniques to prevent attack in data communication in WSN / IoT environment?

RQ3 – What are the criteria for evaluating the performance of anomaly detection methods?

To present a solution for RQ1, authors performed a systematic literature review on methods that detects anomalies in IoT network using ML approaches. The following part of this section will present the outcome of the review.

Abhishek Verma and Virender Ranga[1] developed a ML based approach for detecting anomalies in IoT network. They explored the capability of classification algorithms for machine learning in order to protect IoT against DoS attacks. A systematic study is conducted on classifiers that can further improve intrusion detection systems based on anomalies (IDSs). Classifier performance evaluation is carried out by using familiar evaluation and validation techniques. They employed common datasets such as CIDDS-001, UNSW-NB15, and NSL-KDD.

Authors [2] developed an approach to cyber security, deep learning, to detect attacks in social IoT. The efficiency of the deep model compared to conventional machine learning approaches is evaluated by a distributed attack detection system. The distributed attack detection system had shown to be superior to the centralized detection systems of a deep learning model. It was also shown that the deep model is more efficacious than its shallow counterparts in attack detection.

Authors in [3] considered the integration of the collection of functions, cross validation and classification of the domain, which has not been taken careful into account in current literature. The outcome of this study with recent attacks dataset indicates that the method was capable of effectively detecting cyberattacks. It can detect infected IoT devices that pose a significant challenge in the cloud computing context. The

technique was based on the implementation of a model of training in the distributed fog networks, which can intelligently learn from IoT devices and detect attack or anomaly.

In [4], authors investigated the possibility of using anomaly detection methods based on master learning in vertical wall systems, to boost automation and intelligence in order to achieve predictive climate maintenance. Two types of abnormalities are studied, namely point anomalies and contextual abnormalities. Method of indoor climate anomaly detection, based on forecasts and patterns of recognition were investigated and applied. The results show that in terms of detection points and contextually abnormalities, neural network models, especially the auto encoder (AE), and the long term memory decoder (LSTM-ED), can therefore be deployed to industrial systems in vertical power walls. The results propose a new method of data cleaning and a prediction method is in practice implemented as a proof of concept in the cloud. This study shows the developments in the learning of machinery and the Internet of things that can be completely used to speed up the solution growth.

Authors in [5] discussed different types of attacks and anomalies were suggested and explored in this research based on an intrusion detection method in the IoT. Authors have used the CICIDS data set to detect attacks while assessing the performance of the proposed deep-learning model DBN-IDS framework. Various attacks with several labels and numbers of attacks were presented in this data set. The attack types present in this dataset were DoS/DDoS, Botnet, Brute Force, Web Attack, Invasion, and PortScan, which could cause IoT device failures. They proposed a dedicated, knowledge-based Deep Belief Network (DBN) intrusion detecting system algorithm model in this work. The CICIDS 2017 dataset was used for the performance analysis of their IDS model in relation to attacks and anomaly detection. In all the parameters for accuracy, precision, F1-score, and detection rate, the proposed process generated better performance.

In [6], the author explored similarities between several widely used Support Vector Machine (SVM) classifiers and several other ensemble algorithms, namely, LADTree, REPTree, Random Forest (RF) and MultiBoost, on the other hand. The study was based on a variety of Weka testing methods with the goal of estimating and comparing a selected performance metrics. The results obtained indicate that RF algorithm can be classified as reliable, whereas the REPTree algorithm is the alternative recommendation in the more restrictive timeline cases.

Authors in [7] introduced an ensemble approach that uses the Deep Neural Network (DNN) and LSTM as well as a meta-classifier using the stacking generalization principle. The method used a two-stage approach for the evaluation of network anomalies, with a Deep Sparse AutoEncoder (DSAE) in the first phase, to improve the capabilities of the proposed approach. In the second step, a classification technique was used to stack ensemble learning. The findings of an assessment of the strategy proposed were discussed. The statistical value of network anomaly detection was checked and compared to state-of-the-art approaches. Table I illustrates the features and limitations of the existing literature.

TABLE I. FEATURES AND LIMITATIONS

S.No.	Authors	Features	Limitations
1	Abhishek Verma and Virender Ranga [1]	Application of classification algorithms to predict DoS attacks.	Only Dos attacks were discussed. Authors focussed on the classification of attacks rather than detecting attacks.
2	Diro, A. A., & Chilamkurti, N. [2]	Developed a distributed attack prevention technique based on deep learning approach	The detection speed of the approach was less rather than the learning speed.
3	Md Mamunur Rashid et al. [3]	Suggested a classification algorithm to detect anomalies in IoT devices in fog computing	The focus of the study was on fog computing. Authors employed multiple types of attacks dataset, however, partially related to IoT devices.
4	Yu Liu et al. [4]	Developed a method to detect anomalies in IoT environment. Authors applied LSTM to identify anomalies in IoT networks.	Authors employed limited set of data for evaluating their methods. In addition, they failed to discuss the network performance during the anomaly detection.
5	Manimurugan S et al. [5]	Proposed a DBN based IDS in IoT network.	Authors evaluated the system with a limited set of attacks. No discussion about network performance.
6	Valentina Timčenko and Slavko Gajin [6]	Addressed different kinds of classifiers and its performance on identifying various kinds of IoT attacks.	Authors argued that the performance of RF classifier was better than another classifier. However, they evaluated the classifiers with limited dataset.
7	Vibekananda Dutta et [7]	Authors proposed a LSTM based DNN for identifying IoT attacks.	Multiple datasets were employed for measuring the performance of the IoT detectors. However, authors failed to discuss the network performance of IoT environment.

Based on the outcome of the literature review, researchers selected Yu Liu et al. [4], Vibekananda Dutta et al. [7]. Comparing to the recent studies, the performance of the selected works is better. Both studies employed LSTM as a technique to identify an attack in IoT network.

### III. RESEARCH METHODOLOGY

In this study, the researcher proposed a framework that provides a secure wireless network environment, especially IoT devices. Fig. 2 presents the proposed framework for transmitting data among IoT devices. RQ2 stated that how ML technique can improve the performance of detector to identify / classify attacks in IoT environment. To provide a solution, authors presented studies that addressed the limitations of the wireless networks. Basically, IoT devices operate on top of the

physical layer of wireless networks. The introduction of malicious devices among the existing devices can damage the whole network. In the word "recurring neural network" two large network groups are considered to consist of a similar general structure, one of which is a finite input and the other an infinite input. Both network classes have complexities over time. A repetitive finite impulse is a directed acyclic graph that can roll down and be replaced by a neural network strictly supplied, while a repeating network of endless impulses is a cyclically driven graph that cannot roll down. Long Short-Term Memory (LSTM) is one of the variations of RNN. It contains a dedicated memory to produce an output based on the previous events. The efficiency of LSTM is improved with multiple gates. LSTM eliminates back propagation in contrast to RNN. Each LSTM input produces an output which becomes an input for the next LSTM layer or module. And when major events are delayed over long periods, it can accommodate signals that combine low and high-frequency components. In the proposed framework, the researcher introduced an intelligent interface that governs an IoT network. The development of interface is based on AI-based approach. LSTM in Fig. 2 is applied to identify a malicious node in the network. The researchers employed a supervised learning technique to train the NB classifier, which indicates the vulnerability as a label. They developed a testbed for evaluating the proposed framework.

LSTM models are extremely powerful in handling complex data. It contains five components that allow producing both short - term and long - term data.

Cell state (C) - It indicates the intrinsic memory.

Hidden state (H) - It represents an output state information based on the current input, hidden state, and current cell input.

Input gate (I) - It is used to decide the total number of data that can be passed to the cell state.

Forget gate (F) - It decides the total number of data that can be transferred from current input and previous hidden state to the present cell state.

Output gate (O) - It indicates the total number of data that can be passed from the current cell state to the hidden state.

### A. Input Gate

It figures out which input value for memory modification should be used. The values up to 0,1 are defined by Sigmoid. And the tanh feature tests the transmitted values and assesses their importance from-1 to 1. The input gate and cell status are represented by Equation 1 and 2.  $W_{in}$  is the weight,  $H_{t-1}$  is prior state to the hidden state,  $x_t$  is an input, and  $b_n$  is the bias vector that requires for learning rate in the training phase. The cell state is calculated through tanh function.

$$I = \sigma(W_{in}(H_{t-1}, x_t) + b_n) \tag{1}$$

$$C = \tanh(W_d(H_{t-1}, x_t) + b_c) \tag{2}$$

### B. Forget Gate

It identifies and discards the block information. The sigmoid function is used to define the forget gate for LSTM. Equation 3 includes  $(H_{t-1})$  and input  $(x_t)$  that are examined and the number of outputs among 0 and 1 is verified by each cell state  $C_{t-1}$  number.

$$F = \sigma(W_f(H_{t-1}, x_t) + b_f) \tag{3}$$

### C. Output Gate

For deciding the outcome, the input and the memory of the block are used. Sigmoid defines the values to move between 0 and 1. The tanh function weights the values transferred, which are determined in their value from -1 to 1 and multiplied by Sigmoid efficiency. Equation 4 and 5 represents the output gate and hidden gate to identify an attack in IoT network.

$$O = \sigma(W_o(H_{t-1}, x_t) + b_o) \tag{4}$$

$$H = O_t * \tanh(C_t) \tag{5}$$

Researchers employed IoT attacks dataset [8] to evaluate the performance of the proposed framework. The study focussed to protect IoT network from application and network layer attacks. Authors developed the framework using anomaly-based detection. A testbed is utilized with 10 IoT devices with a ML based interface. Authors applied Long Short-Term Memory (LSTM) version of RNN to train the model to detect the anomalous traces in the network and IoT configuration parameters. Multiple types of attacks such as DDoS, Key Logging, etc., are analysed and traces are utilized as a label for training RNN\_LSTM.

Algorithm 1 presents the data collection processes for IoT attacks detection. Authors intended to develop ML based technique. Researchers employed IoTID20 dataset [8] to train and test the performance of the proposed method. Apart from this dataset, they developed a multiple attack anomaly and applied in the test bed.

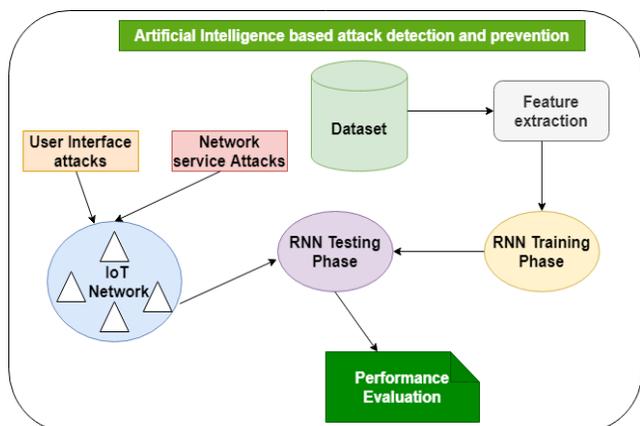


Fig. 2. Proposed Framework for IoT Networks.

#### Algorithm 1 Data Pre-Process

Input: IoTID20, GenID21

Output: Vectors

```
1: Procedure Data Pre- Process
2: while i <- item do
3: D <- RemoveIrrelevant(i)
4: D1 <- RemoveSpacesInString(D)
5: D2 <- TransformAsVector(D1)
6: end while
7: return D2
8: end Procedure
```

Algorithm 2 presents the training phase of anomaly detection in IoT networks. The extracted vectors are treated as an input for training phase and attacks are produced as an output. The LSTMfeed function stores the attack parameters as features and support proposed method (LSTMAD) to identify an attack.

#### Algorithm 2 Training - Anomaly Detection

Input: IoTID20, GenID20- (Vectors)

Output: User Interface / Network Service Attack

```
1: procedure Training phase (vector)
2: while vector <- Vector do
3: if vector = Feature(IoTID20 / GenID20) then
4: attack = Network Service / User Interface Attack found
5: else
6: attack = No Attack
7: if attack = LSTMfeed(feature) then
8: attack = Network Service / User Interface Attack found
9: else
10: attack = No Attack
11: end if
12: end if
13: end while
14: return attack
15: end procedure
```

Algorithm 3 shows the testing phase of LSTMAD which monitors the data communication in the IoT network and identity anomalies in the network. It verifies the device configuration parameters in the network and predicts user interface and network service attacks. Throughput and control overhead criteria show the performance of the network. Thus, these conditions justify the overall performance of the IoT attack detectors. During the testing phase, LSTMAD monitors the IoT network in a specified interval of time during the communication of data among IoT devices.

#### Algorithm 3 Testing Phase - Anomaly Detection

Input: Transmission of data in vulnerable environment

Output: Type of URL

```
1: Procedure Testing phase
2: while D <- Data do
3: if element <- LSTMMemory = Feature (Device configuration / User Interface parameters) then
4: attack = Network Service / User Interface Attack found
5: else
6: attack = No Attack
7: feedback = Environment (suspicious)
8: if element <- LSTMMemory = f<- feedback then
9: attack = Network Service / User Interface Attack found
10: else
11: attack = No Attack
12: end if
13: end if
14: Throughput = Number of packet received / Total time
15: Network overhead = Number of control overheads / Number of received packets
16: end while
17: return attack
18: end procedure
```

Fig. 3 shows the snippets of learning rate to train the IoT attack detectors. Epoch means the frequencies to monitor the IoT network. Both IoTID20 and GenID20 are used in this study to train and test the detectors. IoTID20 contains 625380 attack parameters that represent network service and user interface attacks. In addition, authors generated 23000 attack parameters related to the recent IoT attacks.

```
for IoT_epoch in IoT_range(no of epochs):
    newIoTlr_decay = origIoTlr_decay ** max(epoch + 1 - max__epoch, 0.0)
    attack.assign_lr(sess, learning_rate * newIoTlr_decay)
    current_state = nump.zeros((num_layers, 2, batch_size, attack.hidden_size))
    for step in range(training_input.IoT_epoch_size):
        if num % 75 != 0:
            cost, _current_state = sess.run([attack.cost, attack.train_op, attack.state],
                                           feed_dict={attack.init_state: current_state})
        else:
            cost, _current_state, acc = sess.run([attack.cost, attack.train_op, attack.state, attack.accuracy],
                                                feed_dict={attack.init_state: current_state})
    print("Epoch {}, |accuracy: {:.3f}".format(epoch, step, cost, acc))
```

Fig. 3. Snippets – Training Epoch.

IV. RESULTS AND DISCUSSIONS

In Python 3.0 with support from Sci - Kit Learn and the NUMPY packages, the proposed method (LSTMAD) is developed. In addition, the existing IoT attack detectors are designed for evaluating the efficiency of LSTMAD. The settings for the method parameters during training and test phases are shown in Table II. The learning rate, epoch limit, lot size and decay are the parameters to tell the methods to carry out the results many times. Vocabulary and threshold values are important parameters for the test stage to achieve results through the test dataset.

Authors selected a recent dataset that contains 64.2 million attacks relevant IoT attack in order to answer RQ3. Criteria such as learning rate, accuracy, F1 – Score, Throughput and Control overhead are applied to evaluate the performance of methods. IoT attack detectors are evaluated with a testbed that contains 10 number of IoT devices. Table III presents the learning rate of detectors with IoTID20. The learning rate is increased from 1.0 to 5.0 and number of attacks learnt by each detector is measured. LSTMAD has achieved 93.6 percent of attacks with learning rate of 5.0 whereas Yu Liu et al. [4], and Vibekananda Dutta et al. [7] have achieved 91.5% and 92.4 %, respectively. LSTM is the base technique for all detectors which made detectors to achieve better learning ability. Table IV shows the learning capability of detectors with GenID20 dataset. The dataset contains limited number of attacks rather than IoTID20. Thus, the learning rate of detectors is higher and similar to each other.

Fig. 4 represents the throughput of IoT network. A set of data is communicated between IoT devices in the simulated network. It is evident from the figure that the throughput of the IoT network with LSTMAD is better comparing to Yu Liu et al. [4], and Vibekananda Dutta et al. [7] Throughput is measured in multiple time period with different set of data.

TABLE II. INITIAL SETTINGS OF PARAMETERS (TRAINING AND TESTING PHASES)

Methods	Training phase	Testing phase
LSTMAD	learning_rate=1.0, max_lr_epoch=9, lr_decay=0.73,batch_size=2, num_steps=31, data=train_data	batch_size=20, num_steps=35, data=test_datanum_acc_batches = 30,check_batch_idx = 25,acc_check_thresh = 5,s_training=False, hidden_size=650, vocabulary,num_layers=2
Yu Liu et al. [4]	learning_rate=1.0, max_lr_epoch=9, lr_decay=0.73,batch_size=2, num_steps=31, data=train_data	batch_size=20, num_steps=35, data=test_datanum_acc_batches = 30,check_batch_idx = 25,acc_check_thresh = 5,s_training=False, hidden_size=650, vocabulary,num_layers=2
Vibekananda Dutta et [7]	learning_rate=1.0, max_lr_epoch=11, lr_decay=0.73,batch_size=2, num_steps=31, data=train_data	batch_size=20, num_steps=35, data=test_datanum_acc_batches = 30,check_batch_idx = 25,acc_check_thresh = 5,s_training=False, hidden_size=650, vocabulary,num_layers=2

TABLE III. LEARNING RATE – IoTID20

Learning Rate	LSTMAD	Yu Liu et al. [4],	Vibekananda Dutta et al. [7]
1.0	87.6	89.7	86.4
2.0	88.4	88.4	85.6
3.0	91.6	90.7	89.6
4.0	92.4	90.9	90.8
5.0	93.6	91.5	92.4

TABLE IV. LEARNING RATE – GENID20 DATASET

Learning Rate	LSTMAD	Yu Liu et al. [4],	Vibekananda Dutta et al. [7]
1.0	94.7	90.5	89.6
2.0	96.8	91.6	84.9
3.0	97.5	90.8	90.7
4.0	98.6	90.1	89.7
5.0	98.3	91.4	91.3

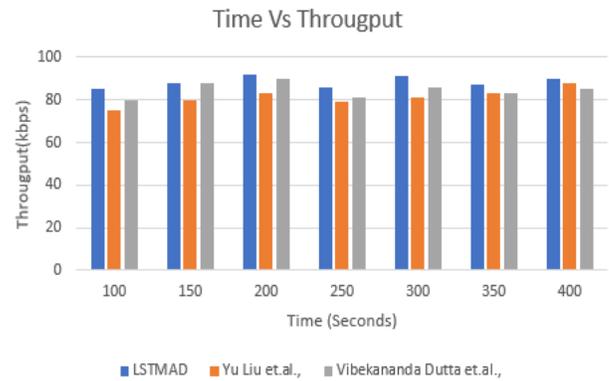


Fig. 4. IoT Network Throughput.

Fig. 5 illustrates the control overhead of IoT network with IoT attack detectors. The control overhead represents the excessive data added with normal data during the communication. The proposed detector required less overhead to govern transmission of data in IoT network. In 400 seconds, the method of Vibekananda Dutta et al. [7] required more than 16000 Bytes of overhead to monitor the network whereas LSTMAD needed only 12000 Bytes of control overhead.

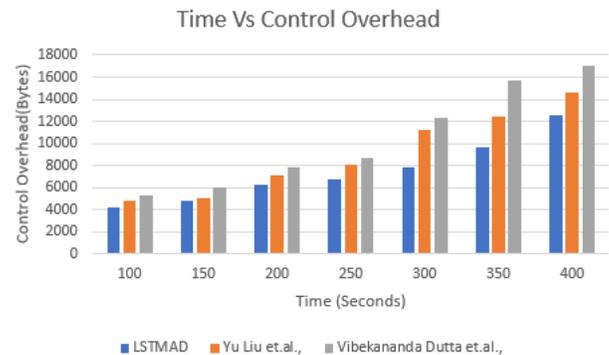


Fig. 5. Control Overhead of IoT Network.

Table V includes the accuracy of each IoT detectors with IoTID20 and GenID20. Accuracy of proposed IoT attack detector is 95.6 % in 450 seconds for IoTID20 dataset whereas Yu Liu et al. [4] and Vibekananda Dutta et al. [7], have achieved 93.8% and 94.6 % in 430 and 520 seconds, respectively. Fig. 6 and Fig. 7 shows the relevant figure of Table V. For GenID20 dataset, LSTMAD has achieved a superior accuracy of 96.3% in 246 seconds which is better than other two detectors.

TABLE V. ACCURACY OF DETECTORS

Methods	IoTID20		GenID20	
	Accuracy (%)	Time (in Seconds)	Accuracy (%)	Time (in Seconds)
LSTMAD	95.6	450	96.3	246
Yu Liu et al. [4]	93.8	430	94.8	301
Vibekananda Dutta et [7]	94.6	520	93.1	432

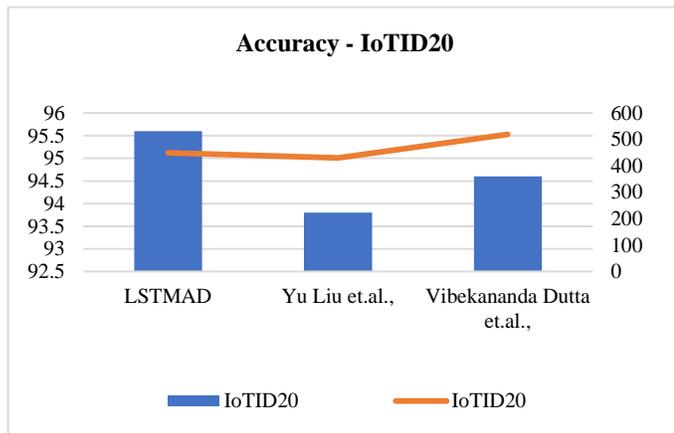


Fig. 6. Accuracy of IoTID20.

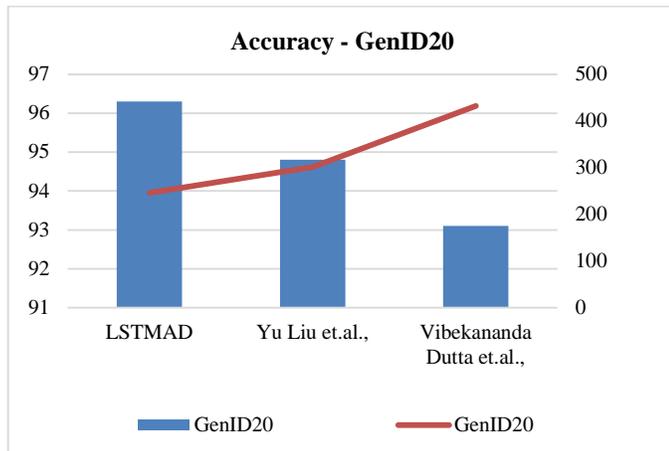


Fig. 7. Accuracy of GenID20.

Table VI presents the F1 – Score of detectors for IoTID20 and GenID20 datasets. F1 – Score represents the retrieving capability of detectors. The retrieving capacity of LSTMAD for IoTID20 is better than Yu Liu et al [4], and Vibekananda

Dutta et al. [7]. The performance of LSTMAD on GenID20 dataset is similar to other methods; however, consumes less amount of time. Fig. 8 and Fig. 9 illustrate the performance of IoT attack detectors. Data pre-process activity of this study supports the classifying process to achieve effective results rather than the other detectors. In addition, it requires limited number of data that improves the throughput of IoT network.

TABLE VI. F1 – SCORE OF DETECTORS

Methods	IoTID20		GenID20	
	F1-Score	Time (in Seconds)	F1 – Score	Time (in Seconds)
LSTMAD	93.4	450	91.8	246
Yu Liu et al. [4]	90.1	430	93.2	301
Vibekananda Dutta et [7]	89.4	520	91.6	432

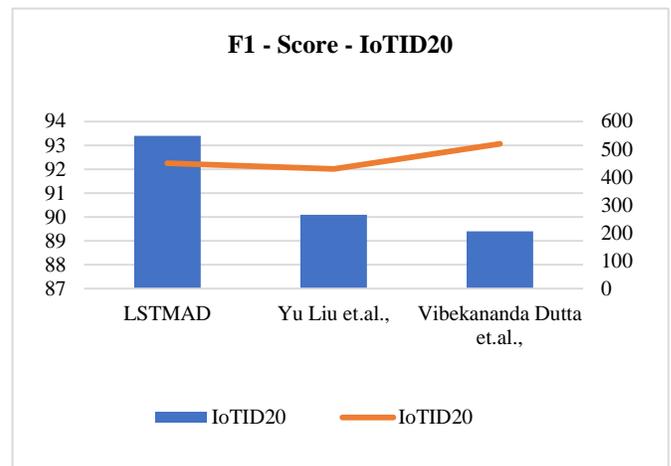


Fig. 8. F1 – Score of IoTID20.

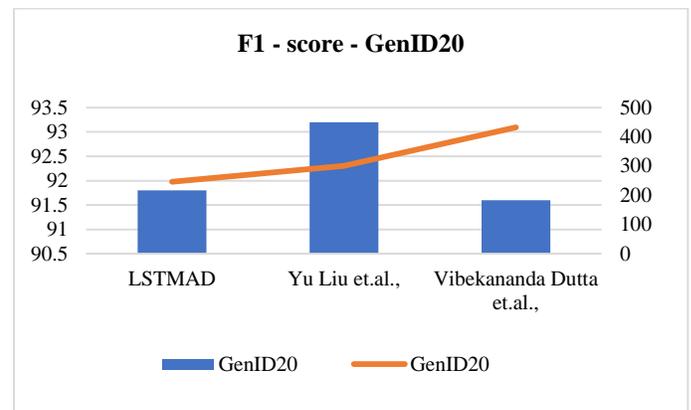


Fig. 9. F1 – Score of GenID20.

## V. OPEN CHALLENGES AND POLICIES

The growing impact of IoT security on the Internet and its users is essential to protect the future of the Internet. In order to protect against Internet threats, IoT-based attacks, IoT manufacturers, IoT service providers, users, SDOs, policy makers and regulators will all be ordered to carry steps. The influence that IoT security has on the trust and online use of

users is also important to understand. Trust is a key component of a sustainable, evolving, global Internet. Users feel vulnerable and excluded without trust and reluctant to take advantage of the many legitimate benefits offered by the Internet. The following part of this section will provide some open challenges and policy requirements for maintaining IoT networks.

#### A. Challenges

A collaborative security approach [11] is essential for the challenges posed by IoT as much as ever. If the IoT Ecosystem expands, the number of connected devices that can be vulnerable may increase. These systems must not be vulnerable. While each actor is responsible for their own tasks, we together need to take steps to reduce the risk that we can generate vulnerable equipment, while reducing the effect of vulnerable devices as they find their way on the network [1][3]. This paper is directed at regulators, policymakers and everyone who is involved in developing and implementing IoT security policy tools.

1) *Weak security*: Competitive pressures for shorter times to market and cheaper products drive many designers and manufacturers of IoT systems, including devices, applications and services, to devote less time and resources to security [6][7]. Strong security can be expensive to design and implement, and it lengthens the time it takes to get a product to market. The commercial value of user data also means that there is an incentive to hoard as much data for as long as possible, which runs counter to good data security practices [9]. Additionally, there is currently a shortage of credible and well-known ways for suppliers to signal their level of security to consumers.

2) *Complex system*: The system's security is as strong as its weakest link. In IoT systems, various components can be operated by different parties in different jurisdictions (for instance, a server in one country may be located and a system may be produced in another country and used in another country), making it difficult to cooperate in the resolution of security issues in IoT and raising problems with cross-border compliance [11]. Complex supply chains challenge security assessments, which require networks to be holistically secured and organized between various parties and parts of the system. IoT systems are increasingly operated and/or controlled by remotely managed cloud providers (or at least strongly interacting with them) rather than being controlled locally. There may also be a specific issue of lack of accountability and control for the end-user.

3) *Limited knowledge*: Consumer knowledge of IoT Protection is limited and affects their safety factor in their shopping habits or the configuration and safeguarding of their IoT Systems [2]. Consumer groups also face financial limitations that make it especially difficult for customers to interact and learn.

4) *Legal liabilities*: It may be difficult to assess the responsibility for damage due to insufficient IoT protection. In order for victims to assign liability or get compensation for

harm, this results in uncertainties. Clear liability may serve as an opportunity to improve protection [5]. Ultimately, in the absence of strong liability regimes, consumers pay for safety violations.

#### B. Policies and Guidelines

Policies to protect from threats to the web infrastructure, such as IoT-based DDoS attacks are all required [17]. The effects that IoT protection has on user trust and online application should also be understood. Trust is a critical element for a sustainable, changing and global Internet. Without trust, users are helpless and oppressed and reject the many valid advantages of the internet.

1) *Data protection*: Data gathered or used by IoT should be protected by privacy and data protection laws, especially the sensor data [18]. Governments will enhance security and safety by clarifying how IoT applies current regulations on the protection of privacy, data protection and consumer protection. In addition, businesses should not make false or disappointing claims about the safety of their goods or services, similarly to the prohibition of misleading statements about food safety [14]. Retailers are also required to share liability and not to sell IoT goods with documented security and security defects [19].

2) *Guiding principles*: Encourage the use, globally, of often checked and widely recognized security best practices and guiding principles for design, implementation and use of IoT devices and services [11].

3) *Regulating industrial sectors*: All industries should be subject to fundamental standards such as data security. IoT systems have however been developed and used in different industries and applications, which can lead to stronger protection outcomes through a sectors-based regulatory approach, complementary to core principles [9]. Strong market incentives or current regulation in some industries could reduce the need for new regulation compared to other industries. In the consumer equipment industry, for example, regulatory tools appropriate to the health sector may not be so useful when qualities such as failure tolerance might not be so critical to producing a healthy product [10].

## VI. CONCLUSION

In this study, authors contributed a method to detect user interface and network service attacks in IoT network. They applied a machine learning approach for classifying the attacks in IoT and WSN. A testbed that contains a number of IoT devices were developed to test the efficiency of the proposed method. A recent dataset IoTID20 which contains 64.2 million of attacks and a total of 63000 attack anomalies were created to measure the performance of IoT attack detectors. Recent approaches in IoT attack detection were compared with the proposed study. Device configuration parameters are the key items to identify an attack in network layers. Usually, attackers modify the configuration in order to launch an attack in IoT environment. In addition, certain policies need to be framed to govern the IoT and WSN. Thus, the proposed study discussed some challenges and necessary policies to monitor the IoT

network. The outcome of the experiment shows that the proposed method capable to detect multiple attacks in IoT and WSN. The future direction of this study is to develop a deep learning-based method to monitor and protect IoT devices from various attacks.

#### REFERENCES

- [1] Verma, A., Ranga, V. Machine Learning Based Intrusion Detection Systems for IoT Applications. *Wireless Pers Commun* 111, 2287–2310 (2020). <https://doi.org/10.1007/s11277-019-06986-8>.
- [2] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761–768.
- [3] Md Mamunur Rashid, Joarder Kamruzzaman, Mohammad Mehedi Hassan, Tasadduq Imam, Steven Gordon, "Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques", *International journal of environmental research and public health*, Vol.17, Issue 9347, 2020 Pp. 1 - 21.
- [4] Yu Liu, Zhibo Pang, Magnus Karlsson, Shaofang Gong, "Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control", *Building and Environment*, Vol. 183, October 2020.
- [5] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan and R. Patan, "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network," in *IEEE Access*, vol. 8, pp. 77396-77404, 2020, doi: 10.1109/ACCESS.2020.2986013.
- [6] Valentina Timčenko and Slavko Gajin, "Machine Learning based Network Anomaly Detection for IoT environments ", *ICIST* 2018.
- [7] Vibekananda Dutta, Michał Chora's, Marek Pawlicki ,and Rafał Kozik, "A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection", *Sensors* 2020, Vol. 20, Iss. 4583.
- [8] Krawczyk, B., Minku, L. L., Gama, J., Stefanowski, J., & Woźniak, M. (2017). Ensemble learning for data stream analysis: A survey. *Information Fusion*, 37, 132–156.
- [9] Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) *Advances in Artificial Intelligence*. Canadian AI 2020. Lecture Notes in Computer Science, vol 12109. Springer, Cham. [https://doi.org/10.1007/978-3-030-47358-7\\_52](https://doi.org/10.1007/978-3-030-47358-7_52) , Accessed: 2020 – 06 – 21.
- [10] P. Ducange, G. Mannara, F. Marcelloni, R. Pecori and M. Vecchio, "A novel approach for Internet traffic classification based on multi-objective evolutionary fuzzy classifiers", 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 1-6, July 2017.
- [11] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques", *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2671-2701, 2019.
- [12] M. F. Elrawy, A. I. Awad and H. F.A. Hamed, "Intrusion Detection Systems for IoT-based Smart Environments: A Survey", *J. Cloud Comput.*, vol. 7, no. 1, pp. 123:1-123:20, December 2018.
- [13] V. L. L. Thing, "IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach", 2017 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6, March 2017.
- [14] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System", *IEEE Access*, vol. 7, pp. 41525-41550, 2019.
- [15] Soe, Yan N.; Feng, Yaokai; Santosa, Paulus I.; Hartanto, Rudy; Sakurai, Kouichi. 2020. "Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture" *Sensors* 20, no. 16: 4372. <https://doi.org/10.3390/s20164372>.
- [16] S. Ioffe and C. Szegedy, "Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift", *Proc. 32nd Int. Conf. on Machine Learning - Vol. 37 ICML'15*, pp. 448-456, 2015.
- [17] 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):1153–1176, 2016.
- [18] T. Hurley, J. E. Perdomo, and A. Perez-Pons. HMMbased intrusion detection system for software defined networking. In *Machine Learning and Applications (ICMLA)*, 2016 15th IEEE International Conference on, pages 617–621. IEEE, 2016.
- [19] U. S. R. K. Dhamodharan and R. Vayanaperumal. Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal*, 2015:7, 2015.
- [20] A. A. Diro and N. Chilamkurti. Distributed attack detection scheme using deep learning approach for internet of things. *Future Generation Computer Systems*, 2017.
- [21] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng. Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, 21(2):34–42, 2017.

# Floating Content: Experiences and Future Directions

Shahzad Ali

Department of Computer Science  
Jouf University, Tubarjal, Kingdom of Saudi Arabia

**Abstract**—Floating content is a promising communication paradigm based on pure ad hoc communications. It has a huge usage potential for various context-aware applications. In this paper, recent research related to floating content communication paradigm is presented. This paper focuses on some of the vital experiences ranging from analytical models to simulations to the real-world implementations. Some important results on the performance of floating content based on analytical models, simulations, and real-world implementations are presented. These results not only show the usefulness of the existing analytical models but also explain the ways of extending these existing models for incorporating new communication technologies and mobility models. This paper also highlights the energy consumption of smartphone applications based on floating content and explains how new communication technologies impact the feasibility of using floating content as a communication service for different applications. Based on the experiences, new future directions are highlighted that can prove to be very beneficial for researchers investigating this area.

**Keywords**—Floating content; opportunistic communications

## I. INTRODUCTION

A massive growth in mobile computing and an abundance of smart devices are consistently driving applications toward context-awareness [1]. Location is the most common type of context used in such applications. Mostly such context-aware applications deal with data having spatial and temporal constraints. For example, a location-aware parking finding application makes use of information about a free parking slot that is available for a limited time and is of interest to the people searching for parking location nearby. Opportunistic communications due to their specific characteristics can prove to be very beneficial for such applications. Several opportunistic communication paradigms are available in literature under different names [2] [3] [4]. They all aim at making a piece of information available over a restricted geographic area. The term “floating content” was introduced in [3]. Fig. 1 illustrates the basic working of floating content service. For the implementation of floating content service, it is assumed that all nodes rely on pure ad hoc communications (Bluetooth, WiFi-Direct, etc.) for content transfer and there is no fixed infrastructure like WiFi or cellular network availability. As the first step for floating content, a node creates a piece of content and defines a range called “Anchor Zone” for that content. Anchor zone refers to a geographical area in which the content is replicated using ad hoc communications whenever two nodes come in communication range of each other. Therefore, nodes within an anchor zone keep on replicating the generated content and in this way that content “floats” within the anchor zone. Once a node goes out of the anchor zone, it deletes the content. This mechanism is

illustrated in Fig. 1. In this way a new node entering the anchor zone has an opportunity for getting the content if it comes in contact of a node already possessing the content. This is called the success ratio and it is one of the fundamental performance metrics for floating content. Formally, success ratio can be defined as the average fraction of nodes getting content before leaving the anchor zone. The second important performance metric is called availability. It is the fraction of nodes within an anchor zone possessing a piece of content. The success ratio depends on availability and increases in availability leads to increase in the success ratio.

In [4], the authors introduced a new zone called the Range of Interest (ROI). ROI is different from the anchor zone. Anchor zone acts as a replication zone for the content items; on the other hand, ROI is used to calculate different performance parameters like success ratio. The anchor zone can be much larger than ROI. The size of the anchor zone affects the success probability and availability. For example, the advertisement related to a special offer at a supermarket might be of interest to the people nearby so ROI can be set to let’s say 300 meters. However, for achieving a high success probability, the anchor zone might be set much larger compared to ROI. Therefore, ROI can always be less than or equal to the size of the anchor zone.

The rest of the paper is organized as follows. Section II explains the latest related work regarding floating content. Section III presents some of the existing analytical models and simulation results that provide us with a deep insight about the performance evaluation of the floating content. In Section IV vital observations and discussions are presented. Section V concludes the paper.

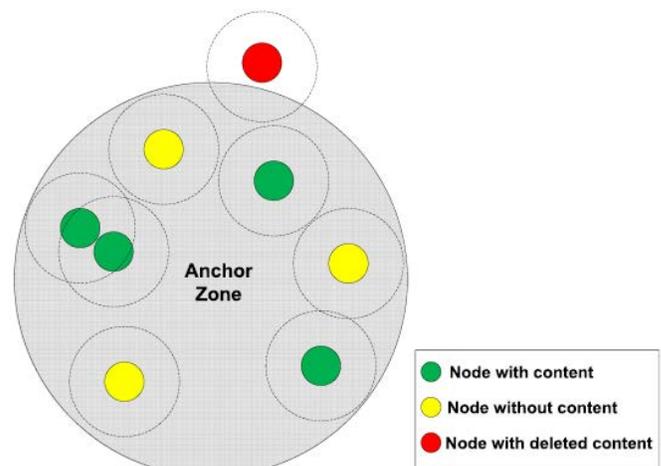


Fig. 1. Floating Content Replication Mechanism.

## II. RELATED WORK

After the first appearance of floating content in [3], various works have focused on different aspects of floating content. In [5], the authors confirmed that the analytical model presented in [4] can predict the success probability for Manhattan Grid Mobility model; however, for more complex models like Reference Point Group Mobility (RPGM) model and realistic vehicular traces, estimates were not quite accurate. As success probability is highly dependent upon the mobility characteristics of the users, therefore, analytical model capturing such characteristics was needed.

The first implementation of floating content as a communication service for a real-world application was done in [6]. An android based application called “Floaty” was developed and tested in an office environment. Bluetooth technology was used for communication among users. The experimental results confirmed the suitability of using floating content as a communication service in an office environment.

In [7], a modified version of the application used in [6] was used in an experiment in a university campus environment. It was shown that the mobility model in a university campus environment was quite different from the one that was observed in [6]. However, the results highlighted that a relatively low user density is enough to guarantee content persistence over time. This was contrarily to the predictions from the models presented in [3]. The experiment showed that even under a low user density, the content floats for a substantial time.

In [8], the authors proposed a new mobility model called Poisson Jumps mobility model. In this work the authors presented a new analytical model for the Poisson Jumps mobility model in a campus environment. The authors proved that Poisson Jumps mobility model can emulate the mobility patterns observed in a campus environment. The presented analytical model also captured the key performance metrics such as success probability and availability.

The performance of floating content is also investigated for VANETs. In [9], an analytical model was proposed for prediction of performance of the floating content in VANET environment. Instead of considering the road geometry, the analytical model was based on a modified version of the Random Waypoint mobility model. The proposed analytical model was evaluated under both synthetic and real-world vehicular traces. The model could predict performance accurately under both settings. The authors also conducted the performance analysis for floating content in a VANETs setting by proposing a new synthetic mobility model called District Mobility Model (DMM). An analytical model was developed based on DMM and performance of the floating content was evaluated under different mobility patterns and traffic conditions. The results proved the effectiveness of floating content under a wide range of traffic conditions.

In recent related work, it can be observed that the early works focused on the conditions under which a piece of content floats in an area. Later on, works focused on different

analytical models and simulations for calculating different performance metrics. After confirming the persistence of the floating content from the analytical models, research focused on the real-world implementation of few applications using floating content as a communication service. Different analytical models were also developed for capturing the mobility characteristics in different environments like university campus and vehicular networks.

## III. ANALYTICAL MODELS AND SIMULATIONS

Various analytical models are presented in the literature regarding different performance parameters for floating content. These models vary based on the mobility of nodes ranging from simple mobility models [4] to relatively complex mobility models [7] [3] [8] incorporating synthetic traces and real-world mobility traces for the users. For this paper, a simple analytical model is considered, which is capable of predicting the performance of floating content for various parameters. Though this model was originally proposed for a simple mobility model called Random Direction mobility model, in [5] it was proven that despite its simplicity, it is capable of predicting performance for various relatively complex mobility models.

The analytical model presented in [4] provides an equation (equation 1) for calculating the success probability  $P_s$  under Random Direction Mobility model. Equation (1) has two parts. The first part represents the probability of meeting  $k$  nodes along a trajectory within an anchor zone. This part is essentially dependent on the pure geometry and can be altered for different mobility models. The second part represents the probability that one of the  $k$  nodes meets another node having the content and content replication take place.

$$P_s(\tau) = \int_0^{2R} \frac{l^2}{\pi R^2 \sqrt{4R^2 - l^2}} \cdot \sum_{k=1}^{\infty} \left[ 1 - \left( 1 - \frac{Q\bar{n}}{(\bar{m} + \bar{n})} \right)^k \right] \frac{(2r\lambda(l^{\wedge}v\tau))^k e^{-2r\lambda(l^{\wedge}v\tau)}}{k!} dl \quad (1)$$

The contribution of this analytical model is novel because it provides a simple (in that it uses few primitive system parameters) analytical model for computing success probability. This model was based on a simplistic mobility model called Random Direction mobility model. By extensive simulations, it was proven that the analytical model was capable of predicting the success probability for a wide range of system parameters.

The analytical model presented in [4] can be used to determine the size of the anchor zone required for getting 90 percent success probability for a given ROI. For instance, Fig. 2 presents the value of anchor zone required for a ROI equals to 300 meters for getting a success probability of 90 percent. It can be observed that a time comes when the anchor zone radius becomes equal to the radius of ROI for achieving a success probability of 90 percent. This is the condition under which the anchor zone radius and ROI are equal and anchor zone radius is sufficient for achieving 90 percent success probability.

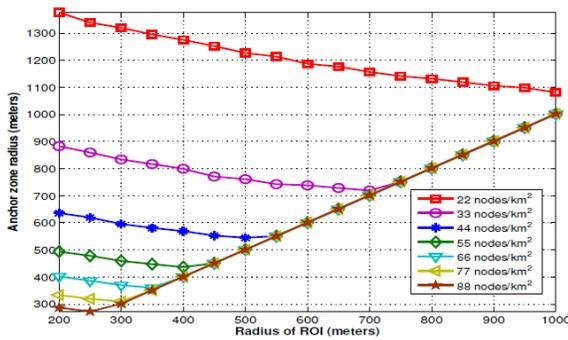


Fig. 2. Anchor Zone Radius for Achieving 90 Percent Success Probability.

Despite the simplicity of the analytical model, by doing extensive simulations in [5], it was observed that the approximates provided by the analytical model are close to a variety of mobility models including Manhattan Grid Mobility Model (MGMM), Reference Point Group Mobility (RPGM), and synthetic vehicular traces from Cologne city as shown in Fig. 3.

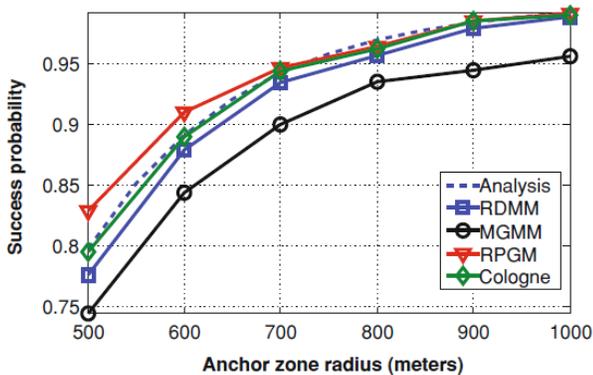


Fig. 3. Success Probability for different Mobility Models.

It is worth explaining that the communication model used by the model presented in [4], includes a parameter called ‘Q’ representing the probability of a successful transfer between two nodes when they communicate with each other.

The value of Q equals to 1 means that there is a 100 percent success rate for an exchange of messages between two nodes. This parameter allows more complex communication models to be incorporated in the analytical model. This is one of the possible ways to extend the existing analytical model for different communication technologies such as Wifi-Direct and Bluetooth.

#### IV. OBSERVATIONS AND DISCUSSION

This section presents some of the important observations that were observed during the course of this work.

##### A. Impact of Communication Technologies on the Performance

It is worth noting that for real-world implementation and performance evaluation of floating content, Bluetooth was used [6] [7]. One of the more prominent communication technologies based on pure ad hoc communication is WiFi-Direct. It offers much longer communication range and much higher data transfer rates compared to Bluetooth [10].

Alternatively, for VANETs, a different standard known as 802.11p is available [9].

The bottom-line is that each communication technology has its own specific characteristics (like communication range, data transfer rate, etc.).

Therefore, first from the analytical model’s perspective, it is very important to incorporate the specific characteristics of the communication technology into the model.

Second, from the practical (real-world implementation) perspective, it is important to utilize these different communication standards for developing the applications for doing the performance evaluation.

##### B. Applications based on Floating Content

Previously, the applications developed using floating content as the communication service [7] [6] [8] were experimental in nature and were restricted to different environments such as an office or a university campus.

The potential of floating content was realized recently in a few killer applications that surfaced particularly for post-disaster management and emergency situations [9].

In this paper, I would like to mention a recent application called “Tabaud” [11]. It is an application for both Android and Apple platforms and is initiated by the government of Saudi Arabia as a measure to contain the Corona virus (COVID-19).

This application utilizes Bluetooth for sending notifications to people if they are in the vicinity of an infected COVID-19 person. By using this application, a person can take essential precautions if he is in the vicinity of an infected person with COVID-19. This application has more than 2 million downloads on Android platform alone.

This application utilizes the communication service similar to floating content for exchanging messages among users who are within the vicinity of each other. The benefit of using Tabaud application is that even if a user is not connected to a fixed network like 4G or Wi-Fi, still he/she is able to receive alert notifications about a COVID19 infected person near him/her.

Similarly, applications based on the concept of Geo Fencing are also getting common. Geofencing is a concept in which a user is notified about an event/alert if he/she is in the vicinity of a particular location. Applications such as Checkmark 2, Geo Alert: location reminder, etc. are based on this concept.

There is a huge potential for using floating content as a communication service for communicating with users in the vicinity without relying on 3G/4G networks.

Similarly, there is a huge potential for using floating content as a communication service for the applications related to geographically restricted advertisements. For example, advertisements or special offers at a shopping mall might be of most interest to the people nearby. Floating content can prove to be very beneficial for such geographically restricted information dissemination.

### C. Energy Consumption

A crucial consideration while designing and implementing any application for smart devices is energy consumption due to the operation of that particular application.

As using floating content as a communication service requires periodically scanning for compatible devices within the vicinity, therefore it is important to investigate the energy consumption aspect as well.

An experiment was performed by running Floaty application developed in [8] and the results are shown in Fig. 4. In the experiment a total of 12 smartphones belonging to three different companies, i.e., HTC, Sony, and Samsung were present in the vicinity of each other.

All the smartphones were running the Floaty App, and Fig. 4 shows that on average each smartphone consumed between 3.5 and 4 percent battery per hour.

It is worth noting that optimizations for the application can be made by tuning in the different parameters like scan interval, message generation interval etc. However, for a normal user, this energy consumption seems high because after 12 hours of operation, the application would have consumed roughly 40 to 50 percent of battery.

Similarly, as Bluetooth was used by the Floaty app, therefore use of different communication technologies like Wifi-Direct is another open question that can be addressed in future work.

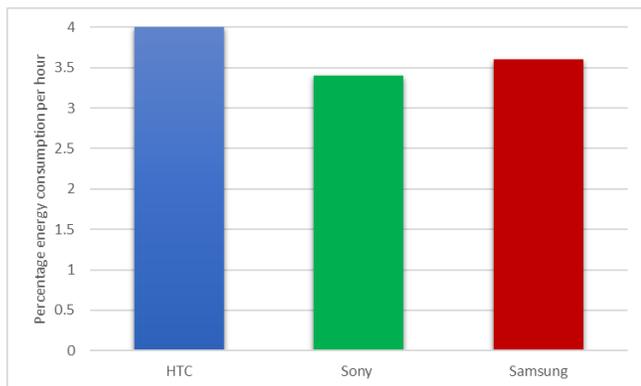


Fig. 4. Energy Consumption by an Application using Floating Content as Communication Service.

### V. CONCLUSION

In this paper, the experiences learned from the recent research in a communication paradigm called floating content is presented. This work considered a simple analytical model and focused on the ways of extending this model for incorporating different communication technologies and mobility models. This paper also highlighted the impact of different communication technologies on the performance of floating content. Some of the existing applications using floating content were also illustrated and results related to the energy consumption of the smart devices running applications based on floating content were also discussed. Based on the discussions, new future directions were highlighted that can prove to be very beneficial for the researchers investigating in this area.

#### REFERENCES

- [1] P. Rosenberger and D. Gerhard, "Context-awareness in industrial applications: definition, classification and use case," *Procedia CIRP*, vol. 72, pp. 1172-1177, 2018.
- [2] A. A. V. Castro, G. D. M. Serugendo and D. Konstantas, "Hovering Information - Self-Organising Information that Finds Its Own Storage," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, Taichung, 2008.
- [3] E. Hyttiä, J. Virtamo, P. Lassila, J. Kangasharju and J. Ott, "When does content float? Characterizing availability of anchored information in opportunistic content sharing," in *IEEE INFOCOM*, Shanghai, 2011.
- [4] S. Ali, G. Rizzo, B. Rengarajan and M. A. Marsan, "A simple approximate analysis of floating content for context-aware applications," in *MobiHoc '13*, Bangalore, 2013.
- [5] S. Ali, G. Rizzo, V. Mancuso and M. A. Marsan, "Impact of Mobility on the Performance of Context-Aware Applications Using Floating Content," in *International Conference on Context-Aware Systems and Applications*, Viet Tri City, 2013.
- [6] S. Ali, G. Rizzo, V. Mancuso, V. Cozzolino and M. A. Marsan, "Experimenting with floating content in an office setting," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 49-54, 2014.
- [7] S. Ali, G. Rizzo, V. Mancuso and M. A. Marsan, "Persistence and availability of floating content in a campus environment," in *IEEE Conference on Computer Communications (INFOCOM)*, Kowloon, 2015.
- [8] G. A. Rizzo, V. Mancuso, S. Ali and M. A. Marsan, "Stop and forward: Opportunistic local information sharing under walking mobility," *Ad Hoc Networks*, vol. 78, pp. 54-72, 2018.
- [9] G. Manzo, M. A. Marsan and G. Rizzo, "Performance Modeling of Vehicular Floating Content in Urban Settings," in *International Teletraffic Congress (ITC 29)*, Genoa, 2017.
- [10] S. Iskounen, T. Nguyen, S. Monnet and L. Hamidouche, "Device-to-Device communications using Wi-Fi direct for dense wireless networks," in *7th International Conference on the Network of the Future*, Buzios, 2016.
- [11] Tabaud. [Online]. Available: <https://play.google.com/store/apps/details?id=sa.gov.nic.tabaud>. [Accessed 07 February 2021].

# A Collision-aware MAC Protocol for Efficient Performance in Wireless Sensor Networks

Hamid Hajaje<sup>1</sup>

Zine El Abidine Guennoun<sup>3</sup>

Department of Mathematics  
University Mohammed V  
Rabat, Morocco

Mounib Khanafer<sup>2</sup>

Department of Electrical and  
Computer Engineering  
College of Arts and Sciences  
American University of Kuwait  
Safat, Kuwait

Junaid Israr<sup>4</sup>

Mouhcine Guennoun<sup>5</sup>  
Cisco Systems  
Ottawa, Canada

**Abstract**—Both IEEE 802.11 and IEEE 802.15.4 standards adopt the CSMA-CA algorithm to manage contending nodes' access to the wireless medium. CSMA-CA utilizes the Binary Exponential Backoff (BEB) scheme to reduce the probability of packet collisions over the communication channel. However, BEB suffers from unfairness and degraded channel utilization, as it usually favors the last node that succeeded in capturing the medium to send its packets. Also, BEB updates the size of the contention window in a deterministic fashion, without taking into consideration the level of collisions over the channel. The latter factor has a direct impact on the channel utilization and therefore incorporating it in the computation of the contention window's size can have positive impacts on the overall performance of the backoff algorithm. In this paper, we propose a new adaptive backoff algorithm that overcomes the shortcomings of BEB and outperforms it in terms of channel utilization, power conservation, and reliability, while preserving the fairness among nodes. We model our algorithm using Markov chain and validate our system through extensive simulations. Our results show a promising performance for an efficient backoff algorithm.

**Keywords**—Wireless sensor networks; beacon-enabled IEEE 802.15.4; binary exponent backoff; adaptive backoff; fairness; power consumption; reliability; channel utilization

## I. INTRODUCTION

The Binary Exponent Backoff (BEB) is an ingenious algorithm employed by both IEEE 802.11 and IEEE 802.15.4 standards to manage the wireless medium access among multiple competing nodes. BEB has been under the scope of extensive studies and have been shown to suffer from several performance pitfalls [1]-[5], [21]-[28], [65], [66] and [67]. Basically, [21], [22], and [23] provided detailed analysis of the MAC protocol, which implements BEB, in IEEE 802.11 to investigate its performance in terms of critical parameters, like throughput. The important conclusion drawn from these studies is that BEB suffers from a major shortcoming in terms of achieving high throughputs. It was proven that the practical performance, in terms of throughput, falls far behind the theoretical one and it is highly dependent on the number of nodes available. This observation motivated important research contributions that targeted enhancing BEB in IEEE 802.11-based networks (for example, see [53], [68], [69] and [70]). The same problem occurs in IEEE 802.15.4, which adopts a slightly modified version of BEB. IEEE 802.15.4's

performance received a strong attention and many studies devised modified versions of BEB to achieve higher throughputs while preserving more power [6], [9-15], [18-19], [29]-[31], [35], [52], [54], [71], [72], [80]. In this paper we focus on the performance of BEB in IEEE 802.15.4-based wireless sensor networks (WSNs). We introduce changes into BEB that can overcome the limitations it experiences. The changes form a foundation for the new Adaptive Backoff Algorithm (ABA) that we model using Markov chain. We also conduct a simulation study to validate our proposed theoretical model. Our results are promising and pave the way for further improvements in future work. The rest of the paper is organized as follows. Section II overviews the BEB algorithm and highlights the problematic aspects of its functionality. In Section III we review the literature for contributions that targeted improving BEB in IEEE 802.15.4. In Section IV we describe ABA and model it mathematically using Markov chain. Section V describes the simulations we conducted to validate the developed mathematical model for ABA and compares the performance of ABA with a number of backoff algorithms proposed in the literature. Finally, Section VI concludes our work and envisions future research directions.

## II. OVERVIEW OF BEB IN IEEE 802.15.4 STANDARD

The IEEE 802.15.4 standard defines the specifications of the PHY layer and the MAC sub-layer for low-rate personal area networks (LR-WPANs) [7], [8], [11], [13] and [32]. This standard suits the functionality of WSNs as it conforms to their distinguished requirements (like the need to preserve the resources of the sensor nodes [59]). The standard supports both star and peer-to-peer topologies. In the star topology, communications among nodes should go through a designated controller node called the PAN coordinator (or the *coordinator* for simplicity). In the peer-to-peer topology, however, direct communication between nodes is possible (and a coordinator still exists). The standard can operate in a beacon-enabled or a nonbeacon-enabled mode. The beacon-enabled mode utilizes a superframe structure to control the communications over the wireless medium in a manner that reduces packet collisions. In Fig. 1, we depict the general structure of the superframe. As shown in the figure, the superframe is delimited by beacons that the coordinator sends periodically to synchronize the nodes. The superframe is constituted by active and inactive portions. The active portion

consists of two main periods, namely, the contention access period (mandatory) and the contention free period (optional). The inactive portion, however, is used by the coordinator to conserve more power by conducting no activities. In this paper we ignore both the contention free period (CFP) and the inactive portion of the superframe.

During the CAP, nodes contend among themselves to secure an access to the wireless medium. The slotted CSMA-CA mechanism, that employs the BEB algorithm, is utilized here. In the rest of the paper, we focus on the beacon-enabled mode of IEEE 802.15.4.

The basic functionality of BEB is explained as follows. Before any transmission attempt, the backoff exponent ( $BE$ ) is initialized to  $macMinBE$ , a MAC attribute defined in the IEEE 802.15.4 standard with a default value of 3. Then, the node backs off for a duration (i.e., contention window) chosen randomly from the range  $[0, 2^{BE}-1]$ . Once the backoff period expires, the node proceeds for two clear channel assessments (CCAs). These assessments are needed to check whether the wireless medium is clear for commencing a transmission. Packet transmission starts only if the medium is found to be clear during the two CCAs. However, if either of the CCAs results in finding the medium busy, the value of  $BE$  will be increased by one (up to a maximum of  $macMaxBE$ ) and the node backs off again (the maximum number of allowed backoffs is  $macMaxCSMABackoffs$ ). The idea behind incrementing  $BE$  is to find its appropriate value that better adapts the duration of backoff to the level of activity over the communication medium. If  $BE$  reaches its maximum, it cannot change unless successful/failed packet transmission occurs, or packet retransmission commences. In that case,  $BE$  is reset to  $macMinBE$ . The packet will be dismissed if  $macMaxCSMABackoffs$  is crossed, and the CSMA-CA mechanism will start the BEB process over. Upon succeeding in transmitting a packet, an acknowledgement (ACK) packet is sent back by the receiver node. If the ACK packet is not received, the node attempts (up to a maximum of  $macMaxFrameRetries$ ) to retransmit the packet. With every retry, the complete BEB procedure is re-applied. If  $macMaxFrameRetries$  is crossed, the packet will be dismissed. It should be mentioned that basic time unit used by CSMA-CA is the  $aUnitBackoffPeriod$ , which we refer to it as  $time slot$  or  $time unit$  in the rest of the paper. Fig. 2 shows the CSMA-CA mechanism, including the BEB algorithm, with more details (the flow chart is taken from [32] with slight simplifications that do not affect the overall mechanism).

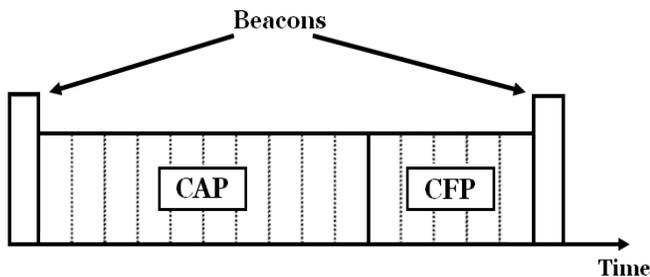


Fig. 1. Superframe Structure (Redrawn from [32]).

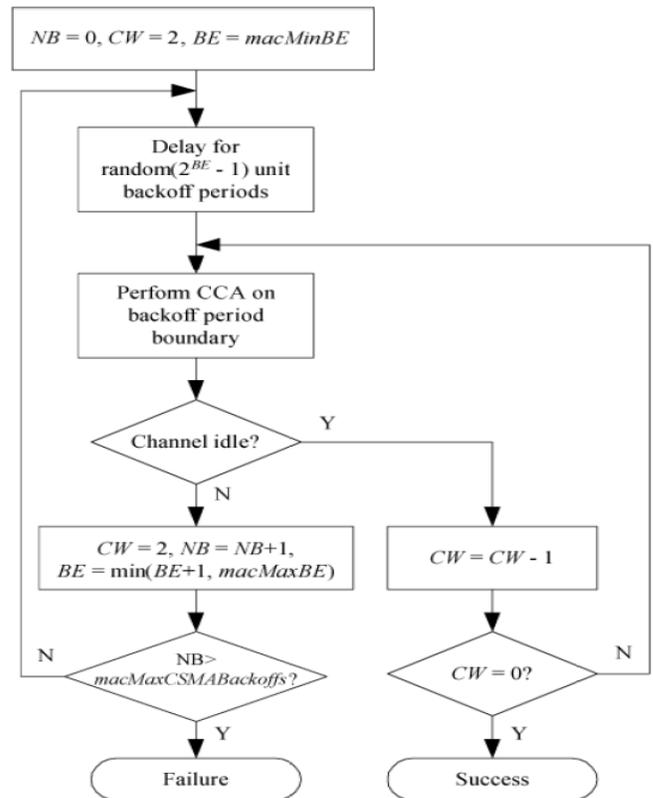


Fig. 2. CSMA-CA Mechanism [32]. NB Refers to the Number of Backoffs Done by the Node and CW is a Counter for the CCAs.

From the description of the BEB algorithm we can identify the reasons behind the degradation of the throughput in its performance evaluation. Clearly, BEB keeps on choosing the contention window randomly without taking into consideration the number nodes available in the network, the level of communication activity occurring on the medium, and the likelihood of packet collisions. A node increases  $BE$  gradually, in steps of 1, in attempts to transmit a packet and then resets  $BE$  to its minimum, as explained before, without incorporating any information about its failed trials of transmissions or the intensity of the traffic in the medium. In other words, BEB is “memory-less” [24] as it keeps no information about the network status or conditions. On the other hand, BEB may have a problem of unfairness under saturation conditions [20][25]. This can be seen from noticing that a node that fails to access the medium tends to backoff for longer periods (because  $BE$  keeps increasing as mentioned earlier), reducing its opportunity of sending its packets. However, a node that has just finished its successful transmission will reset its  $BE$  to its minimum, which results in shorter backoff periods and thus higher chances of accessing the medium. That is, the last successful node is favored on the account of other nodes [26]. Clearly, under saturation conditions we will face a high rate of packet collisions, which leads to excessive power consumption and degraded throughput [33]. Furthermore, this behavior raises serious security concerns. A selfish node may deliberately tune its  $BE$  such that it always achieves the minimum backoff period among the nodes. That way, the selfish node will access the

medium much more frequently than the other nodes in the network (for more details on this misbehavior and how to mitigate it, see [55]-[58]). On the other hand, a node may act maliciously by tuning *BE* to be at its maximum. This way, the node refrains from accessing the medium, which discourages other nodes from using this node as their next hop while forwarding packets. These functionality issues in BEB are far from being acceptable in WSNs. The next section focuses on the efforts proposed in the literature to modify BEB and enhance its performance in IEEE 802.15.4-based WSNs.

### III. RELATED WORK

Research efforts proposed various methodologies to improve BEB. In the following we review some of these proposals.

Minooei and Nojumi studied improving BEB in the context of IEEE 802.11 [34]. Lee et al. investigated the performance of the algorithm in [34], which they call the Non-Overlapping BEB (NO-BEB), in IEEE 802.15.4 networks [29]. NO-BEB modifies the way BEB selects the length of the contention window after an access failure. Basically, in order to reduce the level of contention over the medium, the contention window ( $W$ ) is randomly selected from the range  $[W_{i-1}, W_i]$  rather than  $[0, W_i]$ , where  $W_i$  is the contention window of the  $i$ th backoff stage [34]. This change guarantees that no overlapping with the previous range (that is,  $[0, W_i]$ ) occurs. As a result, nodes experiencing different number of medium access failures have better chances of acquiring different contention windows from the non-overlapped regions. NO-BEB is modeled using Markov chain in [29] and shown to outperform BEB in terms of throughput, probability of collisions and average access delay. While NO-BEB introduces a creative methodology to incorporate the communication medium's status in the computation and selection of  $W$ , it still resets the latter to its minimum after each successful packet transmission. We mentioned in Section II that this behavior is problematic.

Woo et al. proposed the Knowledge-based Exponential Backoff (KEB) algorithm in [30]. The main target of KEB is to improve the throughput depending on the channel state information as collected by each node. Each node uses the Exponential Weighted Moving Average (EWMA), with a smoothing factor  $\beta$ , to compute locally the collision rate after each successful transmission. Based on that computation, the value of *BE* is adjusted to achieve higher throughput. In other words, as the collision rate increases beyond a predefined collision threshold  $\alpha$ , *BE* will be increased and thus nodes backoff for longer periods of time (in order to reduce the level of communications over the medium, which reduces the collisions). In contrast, as the collision rate remains below  $\alpha$ , nodes backoff for shorter periods of time, which improves the utilization of the communication channel. KEB has been modeled using Markov chain and then simulated to validate the analytical model. The provided results show that KEB outperforms BEB in terms of throughput. The main drawback of KEB is that its performance is mainly dependent on the value of  $\alpha$ . The authors provide a simulation study to find out the optimal values of these parameters that achieve the best throughput performance. However, this indicates that KEB

cannot operate in an adaptive fashion and its performance will be governed by the targeted application.

Khan et al. introduce the Improved BEB (IBEB) algorithm in [31]. In IBEB each node, after specifying its *BE*, randomly selects an Interim Backoff (*IB*), which is restricted to be 10% to 40% of the specified backoff delay. The authors argue that this approach tends to reduce packet collisions since the probability of having two nodes randomly selecting the same *BE* and *IB* is quite low. The authors provided a simulation study to examine IBEB's performance in terms of latency, channel utilization, goodput, and average number of collisions. The results showed that IBEB outperforms BEB in terms of these parameters. We highlight that IBEB may suffer from major degradation as the number of nodes increases in the network. This is because the pool of *IBs* is so narrow that many nodes will happen to select the same *IB*, which contributes to higher packet rates of collisions.

Zhu et al. in [39] modify the CSMA-CA algorithm and propose the Linear Increase Backoff (LIB) scheme to enhance the performance in term of packet delay. The idea of LIB is that the backoff counter, upon sensing any of the two CCAs busy, increases linearly instead of exponentially (which is the case in BEB). The authors analyze the behavior of LIB using a comprehensive Markov model. Using this model, they extract formulas to describe the packet delay, energy consumption and throughput of unsaturated, unacknowledged traffic. Simulations of LIB show that it achieves a superior performance in terms of delay, throughput, and energy conservation. LIB is mainly designed for time-critical monitoring and detection applications, and therefore, minimization of the delay is the main target of this scheme.

In [73], the authors have proposed a backoff algorithm, named Waiting Backoff Algorithm (WBA), in order to enhance both the delay and the throughput performance of IEEE 802.11 MAC protocol. The main idea behind this algorithm is to observe the waiting time of each station during the backoff stage and then estimate the size of the contention window in the network. The authors have conducted some simulation experiences to show WBA enhances the basic backoff algorithm for some specific number of stations.

J. Sartthong and S. Sittichivapak have employed the mathematical optimization function theory to propose another backoff algorithm called Contending Stations Backoff Algorithm (CSBA) [74]. This paper includes a comparison results with BEB and other backoff algorithms and shows some improvements in term of saturation throughput efficiency. The same authors have extended this work to achieve more performance by this time by introducing [75] both a Binary Exponential Increment Half Decrement backoff algorithm and a discrete Markov chain model called the Fixed Backoff stages and Fixed Contention windows, named BEIHD and FBFC respectively.

In [68], Q. Liu and A. Czylik have tackled the collision problems in WSN by proposing a collision-aware backoff mechanism (CABEB). Their main idea consists of involving a collision aware module that captures the channel state and adapts the MAC layer based on the collision probability to control the length of backoff period.

In [76], R. TejaChekka et al. have proposed an Adaptive Binary Exponential Backoff algorithm to handle multiple channel access issue by avoiding the collision at the sender side and the buffer overflow at receiver side without degrading channel utilization and throughput efficiency.

In [69], M. Shurman et al. have analyzed the three backoff algorithms BEB, I-BEB and E-BEB and highlighted their limitations. Then, they proposed the New Binary Exponential Backoff (N-BEB) algorithm to improve channel access fairness while preserving the channel throughput. It consists of improving contention window configuration, based on the number of successful and unsuccessful transmissions.

In [77], the authors have tackled the BEB problems by providing two main contributions. First, they proposed an adaptive backoff mechanism through which nodes can dynamically adjust the backoff period according to the actual status of the network. Second, they proposed a priority-based service-differentiation mechanism to provide multi-levels differentiated services in order to meet different QoS requirements.

In [78], the authors have tackled the 802.15.4 performance issues by proposing a backoff mechanism in which the backoff duration is adaptively chosen, when WiFi transmissions are detected during the clear channel assessment. They also consider erroneous decisions regarding the type of packet detected during the CCA and prove that the proposed algorithm remains efficient. Some simulation experiences have been conducted with 10 nodes to demonstrate the feasibility of such technique.

In [70], X. Liu et al. have addressed BEB drawbacks by using a different approach. They proposed a backoff algorithm, which adopts a retransmission counter to measure the network congestion situation. The proposed algorithm also divides the contention window interval into small intervals, and in different intervals, it leverages different backoff strategies. They measured the performance of this approach that showed slight improvements in throughput rate for some specific cases.

In [79], Y. Huang et al. have proposed a Synchronized Contention Window-based backoff algorithm, named SCW. In SCW algorithm, each station actively tracks the transmissions and when the channel state is changed, resetting the CW value synchronizes the CW of each station, which participates in the competition. This way, it makes each station get the medium access grant with the same probability in next channel contention. The experimental results of this technique show some improvement in the case of large number of stations.

#### IV. ADAPTIVE BACKOFF ALGORITHM

Based on the discussions outlined in Sections II and III, we now introduce the new Adaptive Backoff Algorithm (ABA). The pivotal objective behind ABA is to improve the channel utilization ( $U$ ) in the WSN. ABA achieves higher levels of channel utilization than is possible with BEB while keeps the power consumption at the lowest possible level (which is a primary requirement to prolong the lifetime of the WSN). Preliminary to designing/modifying any backoff algorithm, it is essential to understand the factors that play the role of

degrading  $U$ . From one side, whenever the nodes select long backoff periods, the wireless medium is forcibly kept idle for a long duration of time and thus  $U$  is affected. From another side, as the rate of packet collisions rises, the useful communication activities over the medium are affected and  $U$  is reduced as a result. Failing to consider these two factors results in partially effective backoff algorithms.

The problem with BEB is that it provides a *deterministic* solution that keeps on updating the length of the contention window based on predefined steps. This is the main shortcoming of BEB. We need a *probabilistic* solution that can involve the status over the wireless medium in the computation of the contention window. Based on that, ABA proposes that the probability of collision ( $P_c$ ) be used in updating the value of the contention window. This approach guarantees that the contention window will be adapted to conditions over the communication channel. Stated differently, the value of the contention window will be updated as follows:

$$W(t) = P_c(t)W_{max} \quad (1)$$

where,  $W(t)$  is the selected contention window at time  $t$  ( $W(t)$  and  $W$  will be used interchangeably in the rest of the paper),  $W_{max}$  is IEEE 802.15.4's maximum contention window (set to  $2^{macMaxBE}$ ), and  $P_c(t)$  is the probability of collisions at time  $t$  (In the rest of the paper,  $P_c(t)$  and  $P_c$  will be used interchangeably).  $P_c$  is computed locally at each node by knowing the proportion of packets that suffered from collisions. This proportion is computed as  $n_c/(n_s + n_c)$ , where  $n_c$  and  $n_s$  are, as observed by any node, the total number of collided packets and the total number of successfully transmitted packets, respectively (note that in case of unacknowledged traffic, we assume that a mechanism at higher layers is available to advise the MAC of a collision after a certain timeout). According to (1), upon having a packet to send, the node backs off for a duration that cannot exceed  $W_{max}$ . In case that CCA1 or CCA2 reveal that the medium is busy, the backoff process is repeated *macMaxCSMABackoffs* times before discarding the packet. On the other hand, upon experiencing an idle medium after the two CCAs, the packet is sent. In case of a packet collision, the node updates its  $W(t)$  based on the number of collisions it faces and resends the packet. If the packet continues to collide more than *macMaxFrameRetries* times, the packet will be discarded. Equation (1) indicates that, as the rate of collisions increases (decreases), the node utilizes an extended (a shortened) backoff period. This is anticipated to significantly reduce (increase) the contention among nodes, and also allows them better chances of successful transmission.

The overall result is enhanced channel utilization in the network. ABA requires no hardware upgrades and requires simplified computations that requires low power consumption (as we demonstrate in Section V) and can be easily implemented in sensor nodes' platform. In Fig. 3 we show the flow diagram of ABA.

We now develop the mathematical model for ABA based on Markov chain (see [41]-[51] for extensive studies on how to model IEEE 802.15.4's BEB using Markov chain). The

model covers saturated traffic under both acknowledged and unacknowledged traffic conditions. We should mention that saturation conditions are typical in important research areas, like Wireless Body Area Networks (WBAN) (see [63] and [64] for examples).

In Fig. 4 we illustrate a two-dimensional Markov chain that covers all the states a node goes through to access the medium, using ABA, while working under saturated traffic conditions. The latter means that the node has always a packet to send. Each state in our Markov model is distinguished by a pair  $(i, j)$ , where  $i$  can be 0, -1, or -2, to refer to the backoff/CCA states, successful transmission states, or collision states, respectively. The  $j$  index will be clarified in the following. States  $(0, j)$ , where  $j \in [1, W - 1]$ , refer to the duration of backoff during which the node is involved in no activity, waiting for its backoff counter to expire. States  $(0, 0)$  and  $(0, -1)$  correspond to CCA1 and CCA2, respectively. States  $(-1, j)$ , where  $j \in [0, L_s - 1]$ , correspond to the duration spent to successfully transmit a packet. Finally, States  $(-2, j)$ , where  $j \in [0, L_c - 1]$ , correspond to the time wasted due to a packet collision. The probability of finding the medium busy during CCA1 (CCA2) is denoted as  $\alpha$  ( $\beta$ ) (an explanation on the difference between  $\alpha$  and  $\beta$  is detailed in [38]).

The state transition probabilities of our Markov chain are as follows:

$$P(0, j - 1 | 0, j) = 1 \text{ for } 0 < j \leq W - 1 \quad (2)$$

$$P(0, j | 0, 0) = \frac{W-j}{W} \text{ for } j \geq 0 \quad (3)$$

$$P(0, -1 | 0, 0) = 1 - \alpha \quad (4)$$

$$P(-1, j | 0, 0) = (1 - \alpha)(1 - \beta)(1 - P_c) \text{ for } 0 \leq j \leq L_s - 1 \quad (5)$$

$$P(-2, j | 0, 0) = (1 - \alpha)(1 - \beta)P_c \text{ for } 0 \leq j \leq L_c - 1 \quad (6)$$

$$P(0, j | -1, j \text{ or } -2, j) = \frac{1}{W} \text{ for } j \geq 0 \quad (7)$$

Equation (2) captures how the backoff counter decrements before attempting any packet transmission. Equation (3) describes the probability of backing off given that the medium was found busy during CCA1 or CCA2. Note that  $W$  in this equation will be updated according to (1). It is important to point out that deriving (3) is attained by summing all the transition probabilities starting from state  $(0, 0)$  and ending at any of the states  $(0, 0), \dots, (0, W-1)$ . The summation includes the probabilities:  $(\alpha + (1 - \alpha)\beta)/W$  (to transit from state  $(0, 0)$  to any of the backoff states  $(0, j)$ , where  $j \in [0, W-1]$ ),  $(1 - \alpha)(1 - \beta)(1 - P_c)/W$  (to transit from state  $(0, 0)$  to any of the backoff states, after a successful transmission),  $(1 - \alpha)(1 - \beta)P_c$  (to transit from state  $(0, 0)$  to any of the backoff states, after a packet collision), and the probability of being at the state preceding the selected backoff state (so, if backoff state  $(0, 1)$  was randomly selected, we should include the probability of being at backoff state  $(0, 2)$  in our summation, and so on). Equation (4) states the probability of initiating CCA2 given that CCA1 was successful. Equation (5) is the probability of successfully sending a packet after two successful CCAs while Equation (6) is the probability of

having a packet collision after those CCAs. Finally, Equation (7) describes the even probability of choosing a contention window after packet transmission/collision. Assuming that  $s(t)$  and  $c(t)$  are the stochastic processes representing the backoff stage and the state of the backoff counter, respectively, we now write the stationary distribution of our Markov chain to be  $b_{i,j} = \lim_{t \rightarrow \infty} P(s(t) = i, c(t) = j)$ ,

where  $i \in [-2, 0]$  and  $j \in [-1, \max(W - 1, L_s - 1, L_c - 1)]$ . We now derive the closed form expressions for this distribution.

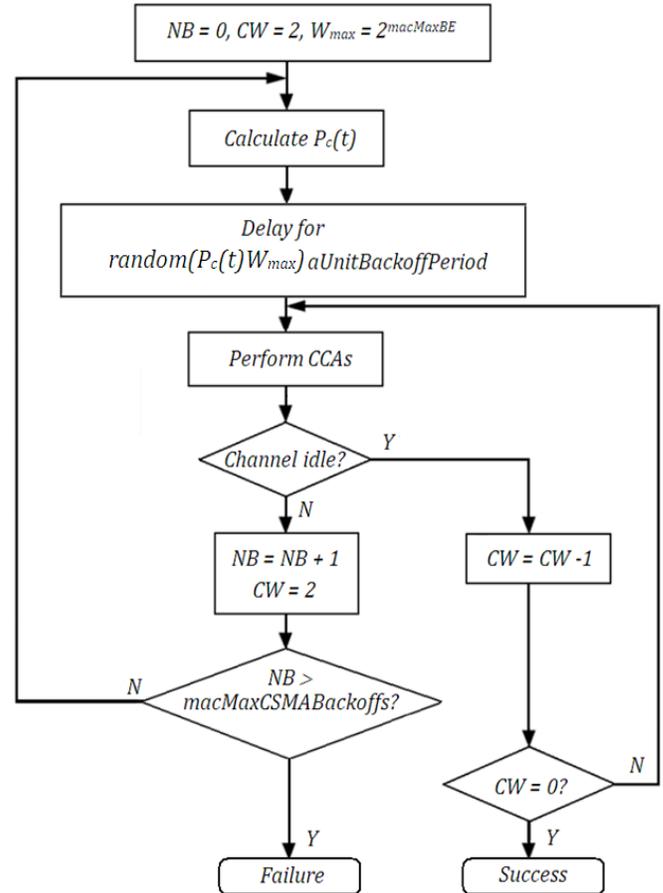


Fig. 3. ABA Algorithm.

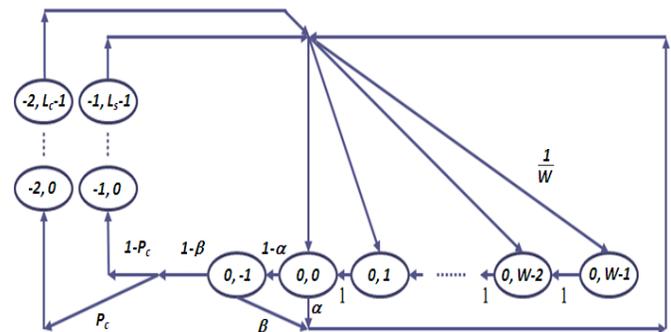


Fig. 4. Markov Chain of ABA Algorithm Under Saturated Traffic Conditions.

By the normalization condition, we have the following formula:

$$\sum_{j=1}^{W-1} b_{0,j} + \sum_{j=0}^{L_s-1} b_{-1,j} + \sum_{j=0}^{L_c-1} b_{-2,j} + b_{0,0} + b_{0,-1} = 1 \quad (8)$$

The first term in (8) refers to the backoff states, the second term refers to the packet transmission states, the third term refers to the packet collision states, and the fourth and the fifth terms refer to the CCA1 and CCA2 states, respectively. We depend on the Equations (2)-(7) to find the mathematical expression for each of these terms. The latter will be expressed in terms of  $b_{0,0}$ , for which a closed form expression will be derived later. Based on (2), (3), and (7) we can write:

$$\sum_{j=1}^{W-1} b_{0,j} = \sum_{j=1}^{W-1} \frac{W-j}{W} b_{0,0} = \frac{W-1}{2} b_{0,0} \quad (9)$$

Next, based on (5) and (6) we have:

$$\sum_{j=0}^{L_s-1} b_{-1,j} = L_s(1-\alpha)(1-\beta)(1-P_c)b_{0,0} \quad (10)$$

$$\sum_{j=0}^{L_c-1} b_{-2,j} = L_c(1-\alpha)(1-\beta)P_c b_{0,0} \quad (11)$$

Finally, based on (4) we obtain the following formula:

$$b_{0,-1} = (1-\alpha)b_{0,0} \quad (12)$$

The probability of collision,  $P_c$ , is formulated in [16] and [17] as follows:

$$P_c = 1 - (1-\tau)^{N-1} \quad (13)$$

Equation (13) is formulated based on the observation that a collision will not happen if, out of  $N$  nodes, only one node is at CCA1, while the remaining  $N-1$  nodes are at any state other than CCA1. Assuming that the probability that a node initiates CCA1 is  $\tau$ , the probability of having no collisions in the network will be  $(1-\tau)^{N-1}$ . Therefore,  $P_c$  will be the complement of the latter term, which gives Equation (13). We point out, however, that when a certain node is initiating its CCA1, it is not quite accurate to assume that the remaining  $N-1$  nodes can be at any state other than CCA1. These nodes can only be in the backoff states. They cannot be, for example, in the state  $(-2, 0)$ . Otherwise, the original node, at the CCA1 state, cannot send out its packet in the first place. Therefore, we accept that Equation (13) provides a reasonable approximation of  $P_c$  in the network, but we expect that it may cause some deviations from the actual behaviour, as we demonstrate later in Section V.

The abovementioned definition of  $\tau$  indicates that it is equal to  $b_{0,0}$ . Therefore, we can now substitute Equations (9)-(13) into (8) and solve for  $\tau$ . The substitution results in the following formula:

$$\tau = \frac{2}{3-2\alpha+2(1-\alpha)(1-\beta)[L_s+P_c(L_c-L_s)]+W} \quad (14)$$

Both  $L_s$  and  $L_c$  are defined in the IEEE 802.15.4 standard (see [32]).  $W$  and  $P_c$  has already been defined in (1) and (13), respectively. Therefore, we need to find mathematical expressions for  $\alpha$  and  $\beta$  to solve for  $\tau$ . These expressions strongly depend on whether the communicated traffic is acknowledged or not. Pollin et al. have provided in [37] (also, see [39]) a detailed study in this direction and we adopt their

findings in this paper. In case of unacknowledged traffic, we have the following expressions:

$$\alpha = L(1 - (1 - \tau)^{N-1})(1 - \alpha)(1 - \beta) \quad (15)$$

$$\beta = \frac{1-(1-\tau)^{N-1}}{2-(1-\tau)^{N-1}} \quad (16)$$

where,  $L$  in (15) refers to the length of the packet to be sent. On the other hand, for acknowledged traffic we have the following expressions:

$$\alpha = P_c(1 - \alpha)(1 - \beta) \left( L + L_{ack} \frac{N\tau(1-\tau)^{N-1}}{1-(1-\tau)^N} \right) \quad (17)$$

$$\beta = \frac{1-(1-\tau)^{N-1}+N\tau(1-\tau)^{N-1}}{2-(1-\tau)^N+N\tau(1-\tau)^{N-1}} \quad (18)$$

where,  $L_{ack}$  in (17) refers to the length of the ACK packet. We should mention that Equations (16) and (18) are approximated for large  $N$  (see [37] and [39] for details).

Equation (14) along with Equations (15)-(16) (or Equations (17)-(18)) for unacknowledged (or acknowledged) traffic form a nonlinear equation system of three variables, namely,  $\tau$ ,  $\alpha$ , and  $\beta$ . This system of equations can be solved using numerical methods to find the operating point of the network.

It is worth mentioning that the Markov model depicted in Fig. 4 is much simpler than the one provided in [36], [37], [38], and [39]. In these studies, the authors show all the backoff and packet transmission retries stages to study the functionality of the MAC layer in IEEE 802.15.4. However, although our model shows these stages augmented as one stage, yet, as we show later, we are able to capture the main characteristics of the MAC layer and derive all the formulas that describe its functionality. We will see in the next section that showing the backoff and retries stages is just needed for the sake of computing the reliability of the system. We will follow a methodology that helps in deriving a mathematical formula for the reliability without undermining the validity of the model in Fig. 4.

#### A. Channel Utilization Under ABA

The Channel Utilization ( $U$ ) parameter measures how efficiently we are utilizing the wireless medium to successfully transmit packets. In an unacknowledged traffic situation,  $U$  refers to the probability that a node sends a packet successfully. However, in an acknowledged traffic situation, the node should receive back the ACK packet in order to consider the transmission successful. By examining the model in Fig. 4, we notice that channel utilization is defined as follows:

$$U = NL\tau(1-\alpha)(1-\beta)(1-P_c)$$

which reduces to:

$$U = NL\tau(1-\alpha)(1-\beta)(1-\tau)^{N-1} \quad (19)$$

where,  $N$  is included in the computation in order to find the total  $U$  achieved from the successful transmissions of all the nodes in the network.

### B. Power Consumption Under ABA

It is essential to study the performance of ABA in terms of power consumption. This is because sensor nodes are battery-powered and any proposed algorithm for WSNs should not deplete the nodes' power resources at a high pace.

Under ABA, a node can be in any of the following states: backoff states, CCA states, packet transmission (with either success or collision) states. The power consumed at a node, denoted  $E_{total}$ , is the total summation of the power consumed at each of these states:

$$E_{total} = E_{idle} + E_{CCA} + E_{tx} + E_{rx} \quad (20)$$

$E_{idle}$  is the total power consumed during the backoff states:

$$E_{idle} = P_{idle} \sum_{j=1}^{W-1} b_{0,j} = P_{idle} \frac{W-1}{2} b_{0,0} \quad (21)$$

$E_{CCA}$  is the total power consumed during the two CCA states:

$$E_{CCA} = P_{CCA} (b_{0,0} + b_{0,-1}) = P_{CCA} (2 - \alpha) b_{0,0} \quad (22)$$

where,  $P_{idle}$  and  $P_{CCA}$  to refer to the average power consumed during a backoff state and a CCA state, respectively.

We should pay a careful attention to  $E_{tx}$ , the total power consumed during packet transmission. The value of  $E_{tx}$  depends on the type of traffic assumed, whether it is acknowledged or not. According to IEEE 802.15.4 [32], if the traffic is acknowledged, the node, after sending a packet (thus,  $P_{tx}$  is considered), becomes idle for a period of one time slot (thus,  $P_{idle}$  is considered) before it starts sensing the ACK packet. If the ACK packet is sensed, we should consider the average power consumed during reception ( $P_{rx}$ ). If the ACK packet is not sensed after a period of  $L_{ack}$ , or in case of having a collision, the node becomes idle for an extra time slot (thus,  $P_{idle}$  is considered) before proceeding to sending the next packet. Therefore, as already noted in [36], to compute the total power consumed while sending acknowledged traffic, we have the following formula:

$$E_{tx} = P_{tx} \left( \sum_{j=0}^{L_s-1} b_{-1,j} + \sum_{j=0}^{L_c-1} b_{-2,j} \right) + P_{idle} (b_{-1,L_s} + b_{-2,L_c}) + P_{rx} \sum_{j=L_s+1}^{L_s+L_{ack}} b_{-1,j} + P_{idle} \sum_{j=L_c+1}^{L_c+L_{ack}+1} b_{-2,j} \quad (23)$$

The first term in Equation (23) considers the transmission of the packet, whether it is successful or not. The second term corresponds to the additional time slot in waiting for the ACK packet. The third term evaluates the average power consumed while receiving the ACK packet. Therefore, the summation starts at  $L_s + 1$  which takes into consideration that we wait for  $L_s$  time slots and then one extra time slot before receiving the ACK. Finally, the fourth term corresponds to the time slot waited in the cases of having a collision or losing the ACK packet.

In case of unacknowledged traffic, only the first term of Equation (23) is considered.

Finally,  $E_{rx}$ , the average power consumed during reception of packets, for both acknowledged and unacknowledged traffics, is expressed as follows:

$$E_{rx} = P_{rx} \sum_{j=0}^{L_s-1} b_{-1,j} \quad (24)$$

### C. Reliability Under ABA

Reliability ( $R$ ) is defined in [36] as the probability of achieving a successful packet reception. In other words,  $R$  provides us a measure of how efficient ABA is in improving the possibility of transferring a packet to its destination. Under ABA, a packet is dismissed if we exceed either *macMaxCSMABackoffs* or *macMaxFrameRetries*. That is, a node goes through multiple backoff stages, in case of busy CCAs, and/or multiple transmission retries, in case of repeated collisions, before dismissing a packet. Therefore, formulating  $R$  depends on finding the probability of avoiding the dismissal of a packet. As the likelihood of dismissing a packet diminishes, it means that the system is more reliable. Therefore, the reliability is defined as follows:

$$R = \frac{\pi_s}{\pi_s + \pi_f} \quad (25)$$

Where,  $\pi_s$  is the probability of having successful transmissions and  $\pi_f$  is the probability of having failed transmissions. Note that *failed* transmissions include both collided packets and discarded packets. While  $\pi_s$  is known from Equation (5), special attention is needed to formulate  $\pi_f$ . We develop the finite-state machines (FSMs) shown in Fig. 5 and use them to accomplish that. The FSM in Fig. 5(a) shows that a node, as it goes from state  $(0, 0)$  and ends back at it, may encounter a successful transmission (S), a packet collision (C), or a busy channel (B). Fig. 5(a), however, does not show the multiple backoff stages and packet transmission retries a node may experience while attempting to send a packet. In other words, the B and C states are in fact constituted by multiple stages. These stages are shown in Fig. 5(b) and 5(c). Note that these two FSMs can be merged to show the complete system, but we avoid that to simplify our derivations. Based on Equations (3)-(6), we can directly see that  $x = \alpha + (1 - \alpha)\beta$ ,  $y = (1 - \alpha)(1 - \beta)P_c$ , and  $z = (1 - \alpha)(1 - \beta)(1 - P_c)$ . These equations can be also inferred by noticing the transitions in Fig. 5(a). The FSM in this figure is interpreted as follows. As a node finds the channel busy, it has a probability of  $x$  to find the channel busy again. On the other hand, it may succeed to send its packet or face a packet collision with probabilities  $z$  and  $y$ , respectively. After succeeding in sending a packet, a node may be successful in sending the next packet with a probability of  $z$ . Otherwise, the node may find the channel busy with probability  $x$  or suffer from a collision with probability  $y$ . Finally, as the node experiences a collision, it may encounter another collision with probability  $y$ , succeed in sending the packet with probability  $z$ , or find the channel busy with probability  $x$ .

In Fig. 5(b) and 5(c) we capture the fact that, during a single cycle, a node may go through *macMaxCSMABackoffs* (denote as  $m$  in Fig. 5(b)) backoff stages and *macMaxFrameRetries* (denote as  $n$  in Fig. 5(c)) collisions before discarding a packet (note that  $\pi_{C_i}$  denote the probabilities to suffer from a collision after finding the

channel busy for  $i$  times). Therefore, in order to find  $R$ , we need to find the probability that the system backs off for  $m+1$  times or experiences a collision for  $n+1$  time. If we assume  $A$  to be a random variable that denotes the number of backoff stages the node has gone through, and  $B$  to be a random variable that denotes the number of collisions occurred, then Equation (25) can be rewritten as follows:

$$R = \frac{\pi_S}{\pi_S + P(A=m+1) + P(B=n+1)} \quad (26)$$

$P(A = m + 1)$  and  $P(B = n + 1)$  can be found using the FSMs in Fig. 5(b) and 5(c), respectively. Towards that end, if we have the transition matrices  $P_1$  (for Fig. 5(b)) and  $P_2$  (for Fig. 5(c)), then there exist the stationary distributions  $\pi_1$  and  $\pi_2$ , such that  $P_1 \times \pi_1 = \pi_1$  and  $P_2 \times \pi_2 = \pi_2$ . The latter relationships are expanded, respectively, as follows:

$$\begin{matrix} S & B_1 & B_2 & \dots & B_m & B_{m+1} & C \\ S & z & z & z & \dots & z & z & z \\ B_1 & x & 0 & 0 & \dots & 0 & x & x \\ B_2 & 0 & x & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ B_m & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ B_{m+1} & 0 & 0 & 0 & \dots & x & 0 & 0 \\ C & y & y & y & \dots & y & y & y \end{matrix} \times \begin{bmatrix} \pi_S \\ \pi_{B_1} \\ \pi_{B_2} \\ \vdots \\ \pi_{B_m} \\ \pi_{B_{m+1}} \\ \pi_C \end{bmatrix} = \begin{bmatrix} \pi_S \\ \pi_{B_1} \\ \pi_{B_2} \\ \vdots \\ \pi_{B_m} \\ \pi_{B_{m+1}} \\ \pi_C \end{bmatrix} \quad (27)$$

$$\begin{matrix} S & C_1 & C_2 & \dots & C_m & C_{m+1} & B \\ S & z & z & z & \dots & z & z & z \\ C_1 & y & 0 & 0 & \dots & 0 & y & \pi_{C_1} \\ C_2 & 0 & y & 0 & \dots & 0 & 0 & \pi_{C_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ C_m & 0 & 0 & 0 & \dots & 0 & 0 & \pi_{C_m} \\ C_{m+1} & 0 & 0 & 0 & \dots & y & 0 & \pi_{C_{m+1}} \\ B & x & x & x & \dots & x & x & x \end{matrix} \times \begin{bmatrix} \pi_S \\ \pi_{C_1} \\ \pi_{C_2} \\ \vdots \\ \pi_{C_m} \\ \pi_{C_{m+1}} \\ \pi_B \end{bmatrix} = \begin{bmatrix} \pi_S \\ \pi_{C_1} \\ \pi_{C_2} \\ \vdots \\ \pi_{C_m} \\ \pi_{C_{m+1}} \\ \pi_B \end{bmatrix} \quad (28)$$

In (27) the stationary distribution  $\pi_1$  is defined as  $[\pi_S \ \pi_{B_1} \ \pi_{B_2} \ \dots \ \pi_{B_{m-1}} \ \pi_{B_m} \ \pi_C]$ , where  $\pi_{B_k}$  is the probability of being in the  $k$ th backoff stage. On the other hand,  $\pi_2$  is defined as  $[\pi_S \ \pi_{C_1} \ \pi_{C_2} \ \dots \ \pi_{C_{n-1}} \ \pi_{C_n} \ \pi_B]$  for (28), where  $\pi_{C_r}$  is the probability of experiencing the  $r$ th collision.

Based on (27) and (28), we can write the following formulas (see Appendix A for the detailed derivations):

$$P(A = m + 1) = \pi_{B_{m+1}} = \frac{x^{m+1}(1-x)}{1-x^{m+1}} \quad (29)$$

$$P(B = n + 1) = \pi_{C_{n+1}} = \frac{(1-x-y)y^{n+1}}{(1-x)^{n+1}-y^{n+1}} \quad (30)$$

Finally, with the knowledge of Equations (26), (28), and (29), we can now formulate the reliability as follows:

$$R = \frac{1}{1 + \frac{(1-x)x^{m+1}}{(1-x)^{m+1}(1-x-y)} + \frac{y^{n+1}}{(1-x)^{n+1}-y^{n+1}}} \quad (31)$$

#### D. Channel Collision Time Under ABA

An efficient backoff algorithm should prove effectiveness in reducing the rate of collisions in the wireless medium. This is essential because not only it improves the utilization of the communication channel, but also reduces the consumption of power due to useless activities.

We aim in this subsection at investigating the percentage of time the channel is getting busy due to collisions. This is

different from what Equation (13) reflects. Equation (13) describes the probability of collision from each node's perspective. In other words, this equation describes the *average* probability of collision that *any* node will face when communicating over the medium. However, that equation does not consider the *channel's* perspective. The latter recognizes the fact that a collision involves at least two nodes, and therefore, even if three or more nodes send their packets at the same instant, the channel will experience a busy period of only  $L_c$  time units. Stated differently, by examining Fig. 4, we notice that the proportion of time a node spends in the collision state is  $L_c(1-\alpha)(1-\beta)P_c\tau$  (recall Equation (11)). Then, if  $N_c$  nodes (out of  $N$ ) have collided at the same instant, the channel collision time,  $T_{cc}$ , is the *non-overlapping* period of time during which the channel is busy with a collision situation. The latter is defined as follows:

$$T_{cc} = \frac{L_c N \tau (1-\alpha)(1-\beta) P_c}{N_c} \quad (32)$$

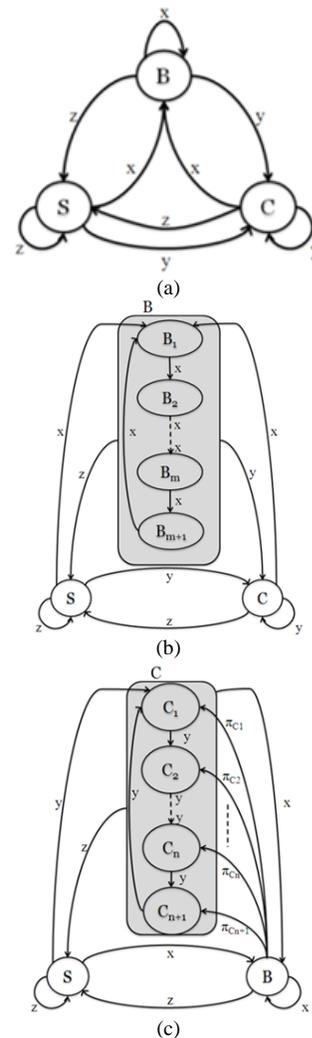


Fig. 5. (a) States Encountered During One Complete Cycle, (b) Break Down of the B State into Multiple Backoff Stages, and (c) Break Down of the C State into Multiple Packet Transmission Retries.

where,  $N_c$  is the *expected* number of collided nodes. To determine the value of  $N_c$ , we should calculate the expected

number of collided nodes, given that a collision has happened. This is a conditional probability that we compute as follows. The probability of having  $k$  nodes involved in a collision requires that while a node is at CCA1,  $k-1$  nodes should also be at CCA1 while the remaining  $N-k$  nodes should be in any state other than CCA1. This probability is expressed as  $\tau^{k-1}(1-\tau)^{N-k}$ . The problem of selecting  $k-1$  nodes out of  $N-1$  nodes under the conditions just mentioned is a typical binomial distribution. Given all of these facts, and by noticing that we may have from 2 to  $N$  nodes that are colliding at the same time, we can formulate  $N_c$  as follows:

$$N_c = \frac{1}{P_c} \sum_{k=2}^N \binom{N-1}{k-1} k \tau^{k-1} (1-\tau)^{N-k} \quad (33)$$

Note that we divide by  $P_c$  because we have a condition that a collision has already happened.

Equations (32) and (33) imply that if  $k$  nodes have collided at the same time, the channel will be busy for only  $L_c$  time units and not  $kL_c$ .

An effective backoff algorithm should be able to achieve reductions in  $T_{CC}$ .

### V. SIMULATIONS AND MODEL VALIDATION

In this section we conduct extensive simulations in order to validate the mathematical model developed in Section IV. Our simulations also provide a comparative study between ABA, from one side, and both BEB and NO-BEB from the other side. In this comparison, we evaluate the performance of ABA in terms of channel utilization, power consumption, reliability, and channel collision time. Furthermore, the fairness of ABA is studied to ensure that the nodes in the network are sharing the communication medium equally.

We wrote a C-based simulator to simulate ABA and the other three algorithms mentioned above. The network under study is of a peer-to-peer topology. The network operates in the beacon-enabled IEEE 802.15.4 mode. We omit both the CFP and the inactive periods from the superframe and assume that it is constituted only by the CAP in the active period.

We use the average power consumption of different wireless network interface cards (NICs) [60], [61], and [62]. The parameters considered in our simulations are summarized in Table I<sup>1</sup>. Also, we always assume, except when stated differently, that  $L_s = L_c = L$ . In the following sub-sections, we present our simulations results along with discussions and comments.

#### A. Model Validation

In this subsection we validate our theoretical Markov model by comparing the behavior it predicts to the behavior extracted from simulations. For each parameter studied, we compute the *coefficient of variation of the root-mean-square deviation RSMD* ( $CV(RMSD)$ ), which is a measure of the accuracy of our mathematical model. In other words,  $CV(RMSD)$  measures the differences between the

mathematical model and the simulations.  $CV(RMSD)$  is defined as follows:

$$CV(RMSD) = \frac{\sqrt{\frac{\sum_{i=1}^n (V_{theo} - V_{sim})^2}{n_{sample}}}}{\bar{V}}$$

where,  $V_{theo}$  is the predicted theoretical value,  $V_{sim}$  is the simulated value,  $\bar{V}$  is the average of the observed values, and  $n_{sample}$  is the total number of the sample values used. An accurate theoretical model should achieve low values for  $CV(RMSD)$ .

1) *Channel utilization*: We validate the mathematical expression that we derived for  $U$  in Equation (19). Fig. 6 compares the theoretical behavior with the simulated behavior under unacknowledged traffic conditions while Fig. 7 shows the comparison under acknowledged traffic conditions. We can clearly see that Equation (19) is very accurate in predicting the behavior  $U$  of as the network's size increases. We do see, however, a discrepancy for small networks ( $N \leq 20$ ). In fact, we explain this discrepancy by recalling that Equations (16) and (18) are approximated for large  $N$  (see Section IV), and therefore, as the network gets smaller the model, we provided, may become less accurate.

TABLE I. SIMULATION PARAMETERS

Power Consumed (mW)	Rx	30
	Tx	40
	CCA	30
	Sleep	0.8
Durations	1 timeslot	0.32 ms (80 bits)
	Packet Length ( $L$ )	14 or 28 timeslots
	ACK Packet Length ( $L_{ACK}$ )	2 timeslots
	Simulation Time	320 s
802.15.4 Parameter Settings	<i>macMinBE</i>	3
	<i>macMaxBE</i>	8

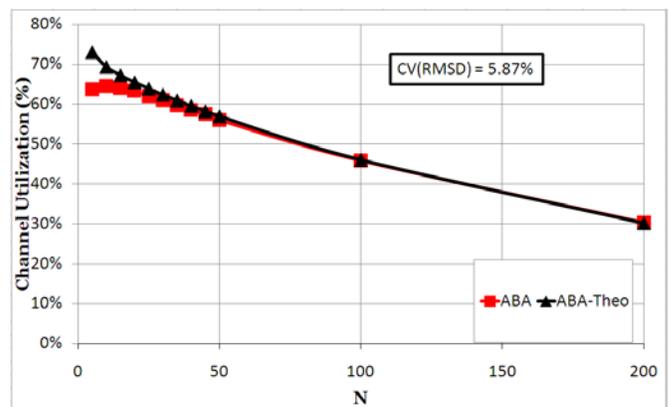


Fig. 6. Channel Utilization of ABA Under Unacknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

<sup>1</sup> CCA power in this table refers to the power consumed during either of the clear channel assessment periods.

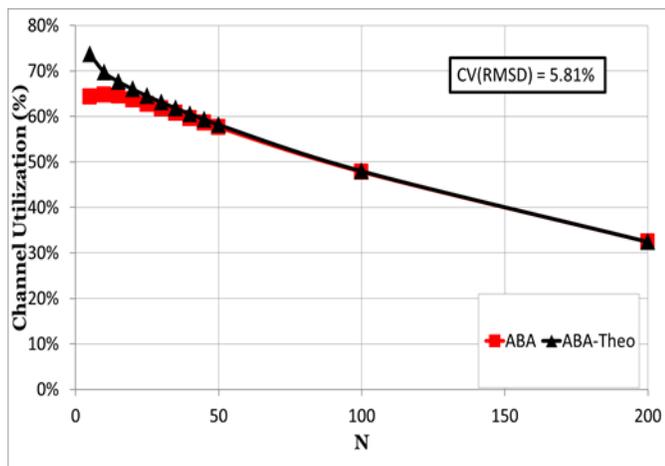


Fig. 7. Channel Utilization of ABA under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

2) *Power consumption*: Fig. 8, for unacknowledged traffic, and Fig. 9, for acknowledged traffic, show a perfect match between our mathematical expressions and the simulations for the total power consumption under ABA.

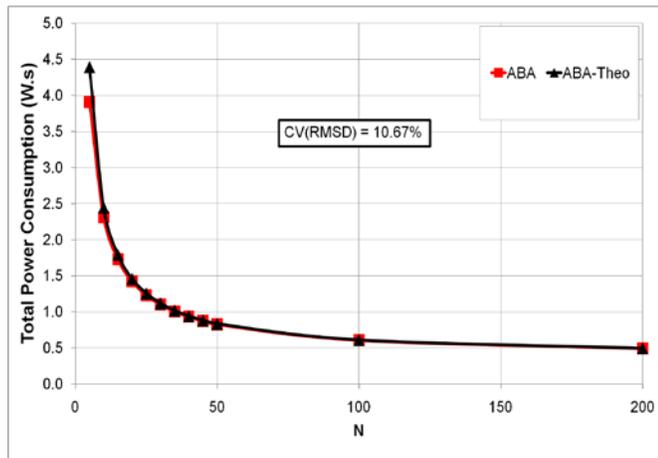


Fig. 8. Total Power Consumption (W.s) of ABA Under Unacknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

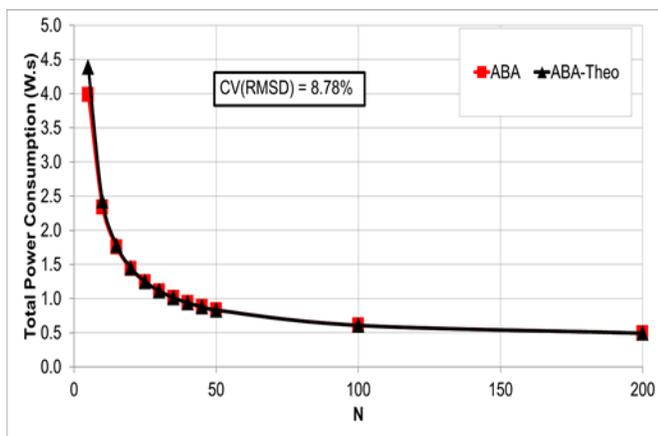


Fig. 9. Total Power Consumption (W.s) of ABA Under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

3) *Power wasted in collisions*: Fig. 10, for unacknowledged traffic, and Fig. 11, for acknowledged traffic, depict the theoretical and simulated performance in terms of the power wasted due to packet collisions. These figures illustrate an accurate matching between our Markov model and the simulations.

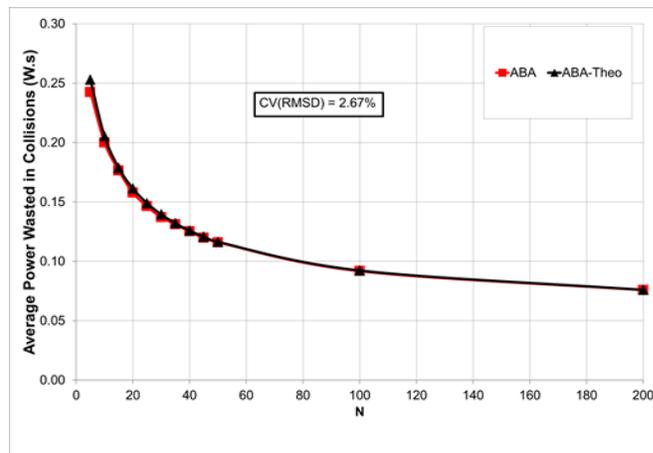


Fig. 10. Power Wasted In Collisions (W.s) Under Unacknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

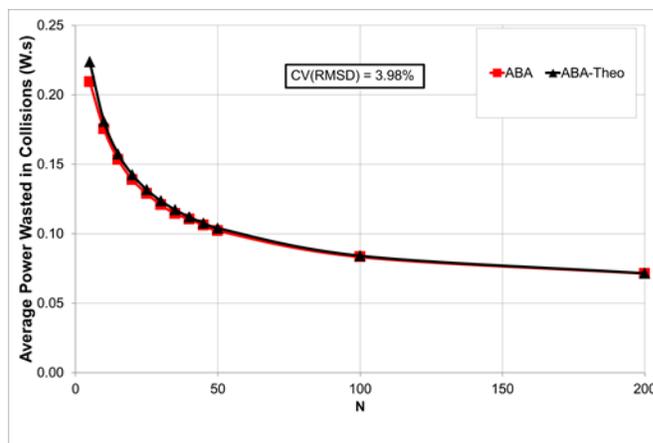


Fig. 11. Power Wasted In Collisions (W.s) Under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

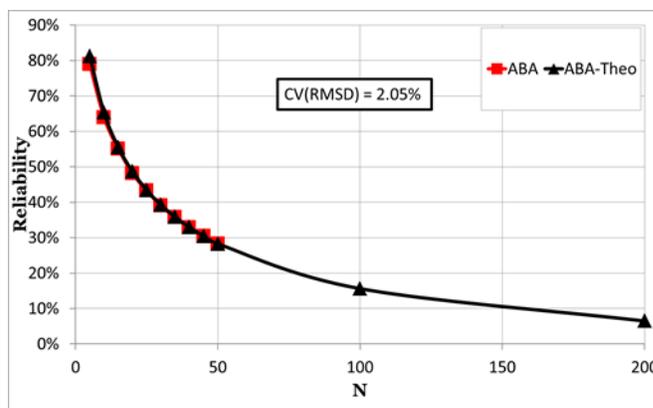


Fig. 12. Reliability of ABA Under Unacknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

4) *Reliability*: Fig. 12, for unacknowledged traffic, show a perfect match between our mathematical expression and the simulations for the reliability of ABA. The same observation is seen in Fig. 13 for the acknowledged traffic.

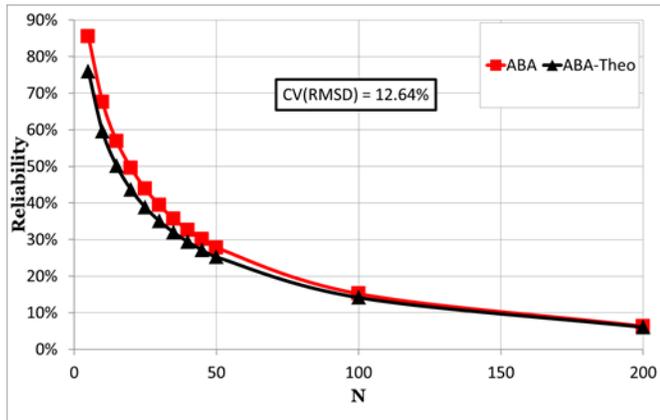


Fig. 13. Reliability of ABA Under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

5) *Channel collision TimeL*: ABA’s theoretical and simulated behavior in terms of the achieved channel collision time, under different traffic conditions, is depicted in Fig. 14 and 15. Although we observe a deviation between the theoretical curves and the simulation ones in all of these figures, the deviation is minor and does not undermine the accuracy of our model. We argue, however, that this deviation is occurring as a result of the term  $N_c$  in Equation (32).  $N_c$  is computed using Equation (33), which includes the term  $(1 - \tau)^{N-k}$ . We discussed in Section IV that this term, originally used in Equation (13), is formed based on the assumption that a node that is not at the CCA1 state can be at any other state in the Markov chain of Fig. 4. This assumption provides a reasonable approximation of the probability of collision in the network, and the deviations we see in Fig. 14 and 15 are resulting from it.

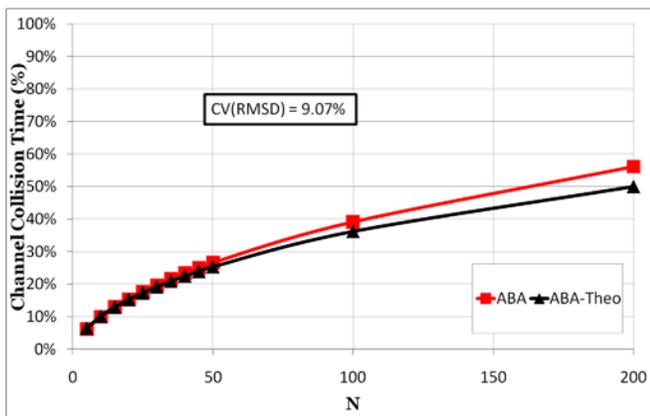


Fig. 14. Channel Collision Time with ABA, Under Unacknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

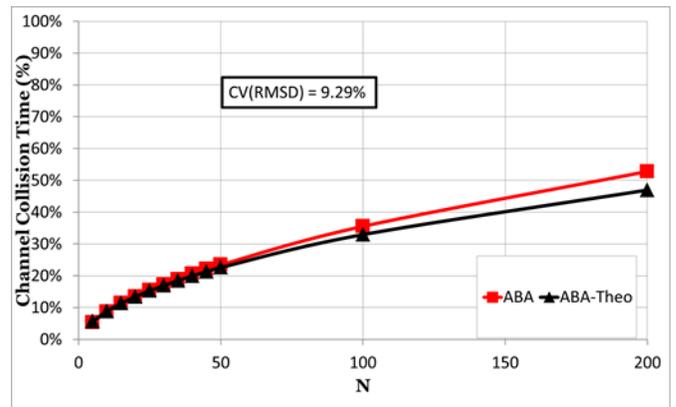


Fig. 15. Channel Collision Time with ABA, Under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

In general, by examining Fig. 6 to 15, and by noticing the values of that we achieved, we can conclude that our Markov-based theoretical model of ABA is accurate and successful in predicting the simulated performance.

### B. Comparing ABA with other Algorithms

In this subsection we study the performance of ABA compared to that of NO-BEB and the standard BEB.

1) *Channel utilization*: We show in Fig. 16 ABA’s performance in terms of channel utilization, under unacknowledged traffic conditions, compared to BEB and NO-BEB. The comparison under acknowledged traffic conditions is shown in Fig. 17. We can see in these figures that ABA achieves a superior performance compared to BEB and NO-BEB. The enhancements over these algorithms become significant as the network’s size increases (especially beyond a size of 20 nodes). For example, in Fig. 16, at 35 nodes, ABA achieves a  $U$  of 59.84%, while BEB and NO-BEB achieve 19.63% and 35.63%, respectively. This means that as ABA enables nodes to update the size of their contention windows in an adaptive manner, a better utilization of the communication channel is achieved.

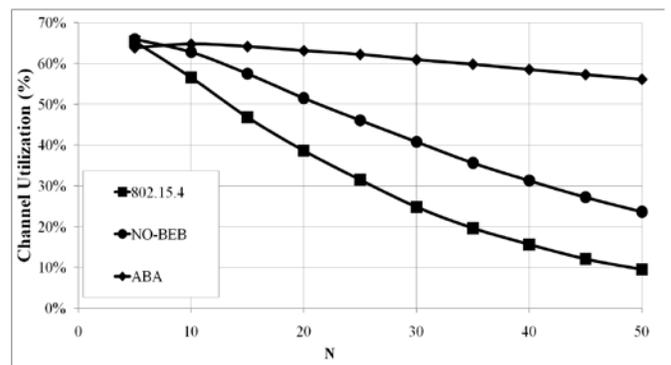


Fig. 16. Channel Utilization of ABA, BEB, and NO-BEB Under Unacknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

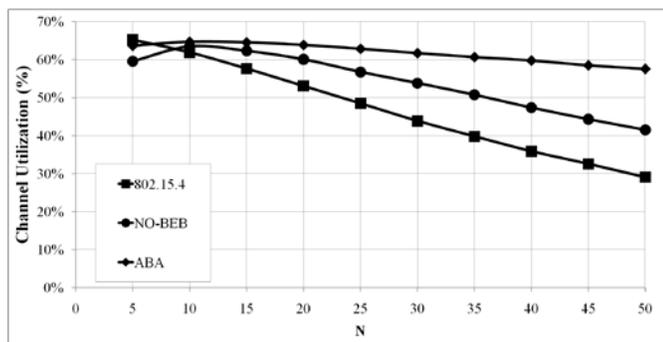


Fig. 17. Channel Utilization of ABA, BEB, and NO-BEB Under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

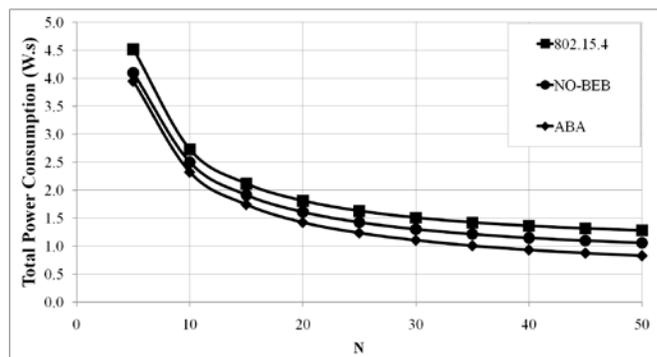


Fig. 19. Total Power Consumption (W.s) of ABA, BEB, and NO-BEB Under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

2) *Power consumption*: In Fig. 18 and 19 we show the performance of ABA in terms of power consumption. It is evident in all these figures that ABA is consuming the least amount of power among all the algorithms. Compared to BEB (Fig. 18), ABA is able to achieve another 10.3% (at  $N = 5$ ) to 36.7% (at  $N = 50$ ) of power savings. The savings compared to NO-BEB range from 3.5% to 21.8%. Comparable results can be drawn from Fig. 19. The power savings achieved with ABA do not reflect a strong performance boost, and therefore, we need to investigate the portion of the total power that is wasted in useless activities, that is, collisions. In Fig. 20 and 21 we show the amount of power lost due to collisions under each algorithm. It is quite evident that ABA is capable of lowering the percentage of collisions, and therefore, the power lost during these situations is the lowest compared to the other algorithms. In Fig. 20, compared to BEB, ABA manages to reduce the power wasted due to collisions significantly. At  $N = 5$ , ABA wastes 39% less in power than BEB. At  $N = 50$ , the power wasted is 69.3% less than BEB. That is, ABA is able to utilize the power resources of the sensor nodes in useful activities. Compared to NO-BEB, ABA loses less in power by 16.7% due to collisions (At  $N = 5$ ). The savings in power jump to 50.6% at  $N = 50$ . Comparable conclusions can be observed in Fig. 21. In conclusion, we can see that ABA is proving to be more conservative in depleting the power resources of the nodes.

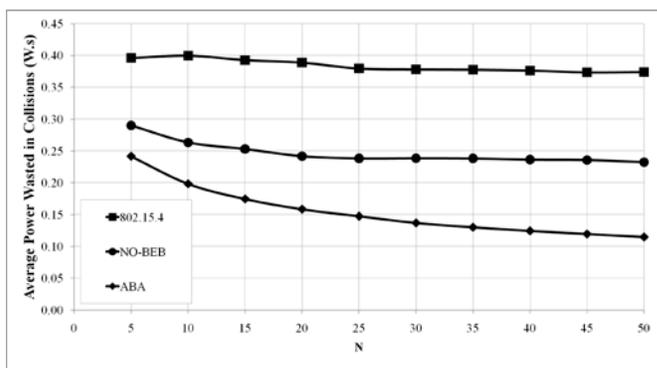


Fig. 20. Power Wasted in Collisions (W.s) Under Unacknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

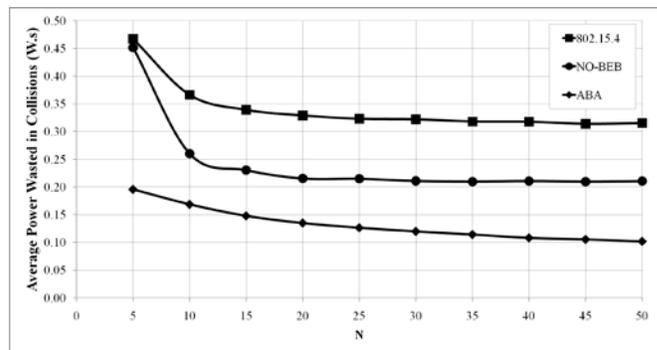


Fig. 21. Power Wasted in Collisions (W.s) Under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

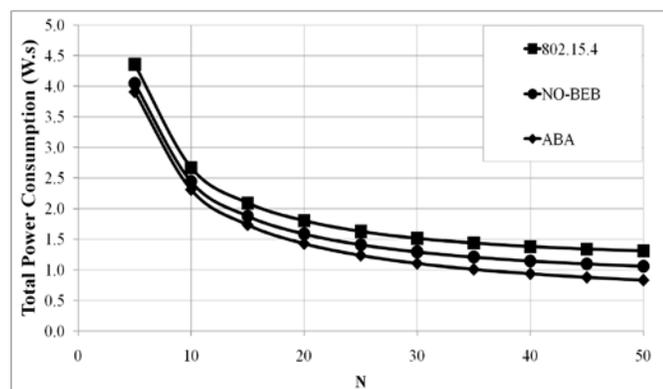


Fig. 18. Total Power Consumption (W.s) of ABA, BEB, and NO-BEB Under Unacknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

3) *Reliability*: In Fig. 22 and 23 we depict the performance of ABA in terms of the reliability. These figures demonstrate the superiority of ABA over all the other algorithms in terms of reliability. A significant improvement can be observed over BEB and NO-BEB. In particular, in Fig. 22, ABA manages to achieve a boost in reliability that starts from 39% (at  $N = 5$ ) and keeps increasing till 69.3% (at  $N = 50$ ) compared to BEB. Compared to NO-BEB, the increase in reliability goes from 8.32% (at  $N = 10$ ) and continues to 61.8% (at  $N = 50$ ). In Fig. 23, we can observe a similar performance.

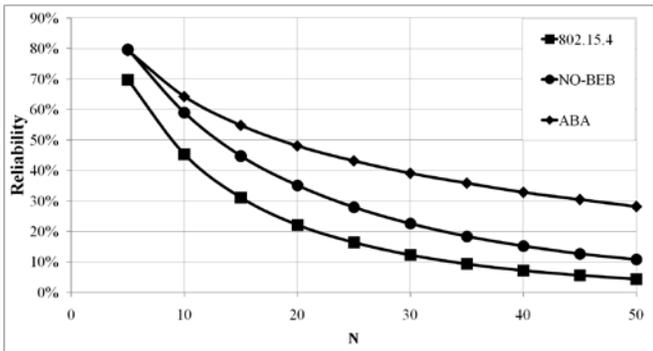


Fig. 22. Reliability of ABA Under Unacknowledged Traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

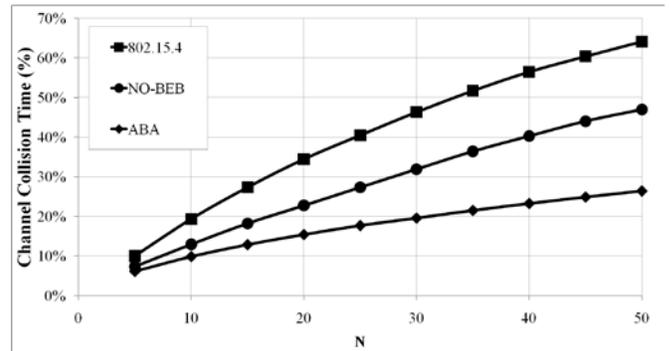


Fig. 24. Channel Collision Time with ABA, Under Unacknowledged Traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

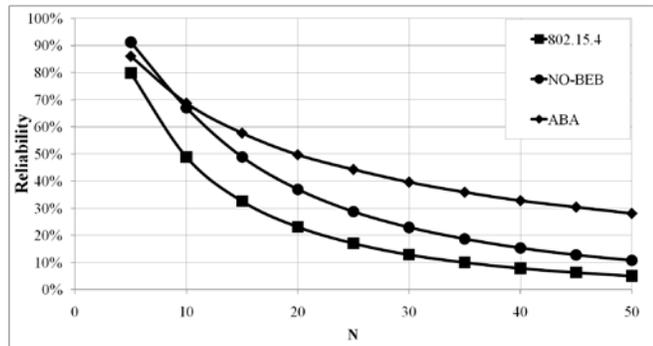


Fig. 23. Reliability of ABA Under Acknowledged Traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

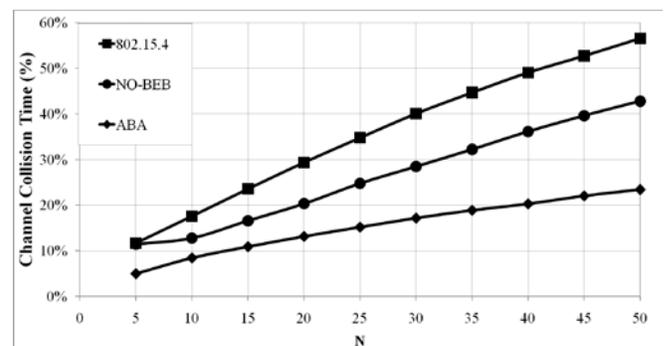


Fig. 25. Channel Collision Time with ABA, Under Acknowledged Traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

4) *Channel collision time*: We examine the performance in terms of the channel collision time in Fig. 24 and 25. Again, ABA is showing superiority in terms of its ability to keep the channel collision time at its lowest level compared to the other algorithms. In particular, in Fig. 24, ABA can achieve a channel collision time that is 38.5% less than BEB at N = 5. This percentage jumps to 58.8% at N = 50. Compared to NO-BEB, ABA's improvements in channel collision time range from 16.5% (at N = 5) and 43.74% (at N = 50). Again, comparable observations can be seen in Fig. 25. ABA's ability to adapt the contention window's size in accordance with the collisions level allows for an efficient utilization of the network's resources.

5) *Fairness*: Finally, we examine the fairness of ABA in order to see whether it allows nodes an equal opportunity to access the wireless medium or not. We adopt Jain's fairness index [40] to measure ABA's fairness:

$$fairness\ index = \frac{(\sum x_i)^2}{N \sum x_i^2} \quad (33)$$

where,  $x_i$  denotes the  $i$ th node's share of the medium. An algorithm is achieving better sharing of the medium among the nodes if its fairness index is closer to 1.

Fig. 26 shows the fairness of ABA, BEB, and NO-BEB under unacknowledged traffic conditions while Fig. 27 shows the fairness under acknowledged traffic conditions. We can clearly see that, for different packet lengths, ABA, BEB, and NO-BEB achieve a fair sharing of the medium among the nodes (the three curves are overlapping, and therefore, only one curve is apparent in the figures).

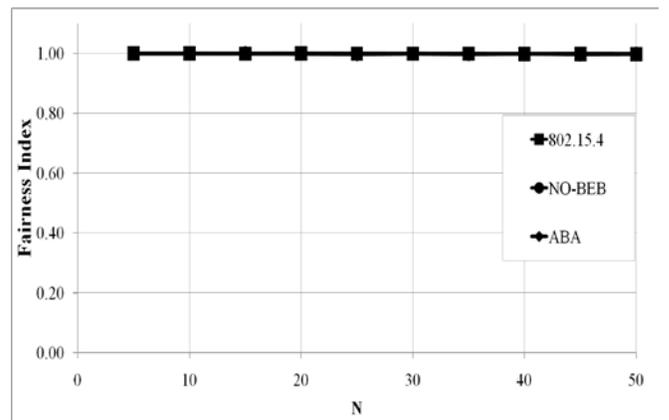


Fig. 26. Fairness of ABA Under Unacknowledged Traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

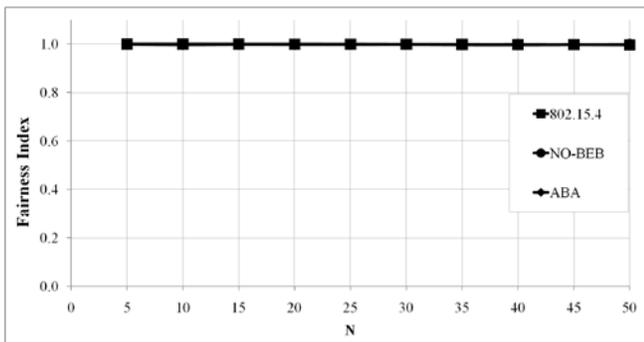


Fig. 27. Fairness of ABA Under Acknowledged Traffic.  $L=14$ ,  $macMaxCSMABackoff=4$ , and  $macMaxFrameRetries=3$ .

### C. Discussions

In the previous subsection we found that the ABA algorithm is achieving a promising performance in terms of enhancing channel utilization, conserving power resources, improving reliability, reducing the level of collisions, while preserving the fairness among the nodes in the network. The superiority of ABA over the other algorithms, especially BEB, comes from the fact that it indirectly relates the contention window ( $W$ ) to the number of nodes in the network. This can be understood by recalling Equation (13) in which we have a direct relation between the probability of collision ( $P_c$ ) and the number of nodes in the network ( $N$ ).  $P_c$  increases with the increase of  $N$ , and therefore, the value of the  $W$  should be changed taking into consideration the size of the network. Thus, the main strength of ABA is that it is controlling  $W$  probabilistically, in such a way it self-adapts to the network's size and the activity over the communication channel. Depending on a deterministic methodology, as in BEB, to change  $W$  without any consideration for the network's size gives a poor performance as we demonstrated. The same problem is found with NO-BEB which adopts from BEB the idea of resetting  $W$  to a predefined minimum. Although NO-BEB shows a considerable improvement over BEB's performance, resetting  $W$  to its minimum without taking into consideration the current status over the medium will degrade the performance.

### VI. CONCLUSION AND FUTURE DIRECTIONS

In this paper we studied IEEE 802.15.4's BEB algorithm and highlighted its major limitations that degrade the overall performance of the wireless sensor network. We pointed out that BEB's methodology of updating the size of the contention window is highly deterministic and cannot cope with the changing levels of activity over the communication channel. Based on these observations, we introduced a novel backoff algorithm, the Adaptive Backoff Algorithm (ABA), which introduces an adaptive, probabilistic methodology to control the size of the contention window. ABA depends on including the probability of collisions, as computed locally by each sensor node, in the computation of the size of the contention window. In this way, the number of nodes competing to access the medium is involved indirectly in the process of updating the contention window. Therefore, we end up with a backoff algorithm that self-adapts to the size of the network, and therefore, manages the medium access in a way

that improves the overall performance. We modeled ABA using Markov chain and validated our model using a C-based simulator. Our simulations prove the accuracy of our theoretical model of ABA. Also, they demonstrated a superior performance over BEB, as well as two other backoff algorithms, in terms of channel utilization, power consumption, reliability, and channel collision time. The simulations also proved that ABA is fair in terms of allowing the competing nodes an equal opportunity to access the medium.

As future research directions, we will work on elaborating the concept of probabilistic backoff algorithms such that more effective MAC protocols are designed for wireless sensor networks. In fact, the methodology of exploiting the probability of collision to gain information about the size of the network and the status over the communication medium can prove usefulness in prioritizing nodes' access to the access the medium. We plan to explore the latter topic in our future research.

### REFERENCES

- [1] K. J. Son, S. H. Hong, S. P. Moon, T. G. Chang and H. Cho, "Segmentized clear channel assessment for IEEE 802.15." 4 networks. *Sensors*, 16(6), 815, 2016.
- [2] T. M. Hoang, V. T. Nguyen, N. G. Nguyen and T. N. Lang, "Analysing the performance of unslotted sensor networks based on the IEEE 802.15. 4 employed EIED algorithm." In 2017 International Conference on Information Networking (ICOIN) (pp. 682-685). IEEE, 2017, January.
- [3] S. Xie, K. S. Low and E. Gunawan, "A distributed transmission rate adjustment algorithm in heterogeneous CSMA/CA networks." *Sensors*, 15(4), 7434-7453, 2015.
- [4] H. R. Hussien, C. R. Teja, T. Miao, K. Kim and K. H. Kim, "Traffic-aware cooperative binary exponential backoff algorithm for low power and lossy networks." *Wireless Personal Communications*, 86(4), 1913-1929, 2016.
- [5] H. P. Sultana and P. V. Krishna, "Priority focused medium access control in wireless sensor actuator networks for CPS." *International Journal of Communication Networks and Distributed Systems*, 16(2), 99-113, 2016.
- [6] Z. Yifan, S. Zhou, H. Ding, Z. Yang and Q. Liu, "IEEE 802.15. 4 CSMA/CA Scheme for Heterogeneous Sensor Networks Based Adaption and RTS/CTS Mechanism." *Sensor Letters*, 14(7), 719-726, 2016.
- [7] M. Elappila, S. Chinara and D. R. Parhi, "Survivability Aware Channel Allocation in WSN for IoT applications." *Pervasive and Mobile Computing*, 61, 101107, 2020.
- [8] Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, An Efficient Adaptive Backoff Algorithm for Wireless Sensor Networks, IEEE Global Communications Conference, GLOBECOM 2011, Houston, Texas, USA, 5-9 December 2011.
- [9] F. I. Engoti, "Réalisation d'une plate-forme pour l'optimisation de réseaux de capteurs sans fil appliqués au bâtiment intelligent" (Doctoral dissertation, Limoges), 2018.
- [10] M. G. Asuti and P. I. Basarkod, "An optimal clear channel assessment in IEEE 802.15. 4 medium access control protocol for recurrent data transmission and long acknowledgement wait period." *Transactions on Emerging Telecommunications Technologies*, e4167, 2020.
- [11] M. Li, J. Dong, Y. Zhang, H. Yang, L. V. Zwietaen, H. Lu, ... and X. Jiang, "A Critical Review of Methods for Analyzing Freshwater Eutrophication." *Water* 2021, 13, 225, 2021.
- [12] P. S. Habibullah and N. Nagendhiran, "Medium Access Control Methods in Sensor and Actuator Based Wireless Networks-A Review." *Walailak Journal of Science and Technology (WJST)*, 14(4), 267-274, 2017.
- [13] M. Khanafer, M. Guennoun and H. T. Mouftah, "Priority-Based CCA Periods for Efficient and Reliable Communications in Wireless Sensor

- Networks,” *Wireless Sensor Network (WSN)*, Scientific Research, Vol. 4, No. 2, February 2012.
- [14] B. Bala, M. Pandey and D. Prasad, “An Adaptive Timeslot Allocation Scheme for Wireless Body Area Networks.” *International Journal of Computer Applications*, 975, 8887, 2016.
- [15] B. Bala and M. Pandey, “Survey on Priority Based Schemes Used For Data Dissemination in Wireless Body Area Network.” *International Journal of Advanced Research in Computer Science*, 6(2), 2015.
- [16] M. Gamal, N. Sadek, M. Rizk and M. Ahmed, “Markov Model of Modified Unslotted CSMA/CA for Wireless Sensor Networks.” In 2019 31st International Conference on Microelectronics (ICM) (pp. 57-61). IEEE, 2019, December.
- [17] P. K. Sahoo, S. R. Pattanaik and S. L. Wu, “A reliable data transmission model for IEEE 802.15.4e enabled wireless sensor network under WiFi interference.” *Sensors*, 17(6), 1320, 2017.
- [18] Hussein T. Mouftah, Mounib Khanafer, Mouhcine Guennoun, *Wireless sensor network architectures for intelligent vehicular systems*, Symposium International for Telecommunication Techniques, 2010.
- [19] P. K. Sahoo, S. R. Pattanaik and S. L. Wu, “A novel IEEE 802.15.4e DSME MAC for wireless sensor networks.” *Sensors*, 17(1), 168, 2017.
- [20] M. Gamal, N. Sadek, M. R. Rizk and M. A. E. Ahmed, “Optimization and modeling of modified unslotted CSMA/CA for wireless sensor networks.” *Alexandria Engineering Journal*, 59(2), 681-691, 2020.
- [21] G. Bianchi, “Analysis of the IEEE 802.11 distributed coordination function,” In *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 3, pp. 535-547, Mar. 2000.
- [22] G. Bianchi, L. Fratta and M. Oliveri, “Performance Evaluation and Enhancement of the CSMA/CA MAC Protocol for 802.11 Wireless LANs,” in proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC’96), pp. 392-396, Taipei, Taiwan, Oct. 1996.
- [23] F. Cali, M. Conti and E. Gregori, “Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit,” *IEEE/ACM Transactions on Networking*, vol. 8, no. 6, Dec. 2000.
- [24] M. Albalt and N. Qasim, “Adaptive Backoff Algorithm for IEEE 802.11 MAC Protocol,” *International Journal of Communications, Network and System Sciences*, vol. 2, no. 4, pp. 249-324, Jul. 2009.
- [25] V. V. Kamath, “An Approach to Increase Channel Utilization in the IEEE 802.11 Networks by Improving Fairness at the Medium Access Control Sub-Layer,” Master’s thesis, George Mason University, Dec. 2008.
- [26] S. Xu and T. Saadawi, “Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?,” *IEEE Communications Magazine*, vol. 39, no. 6, pp. 130-137, Jun. 2001.
- [27] N. O. Song, B. J. Kwak, J. Song and L. E. Miller, “Enhancement of IEEE 802.11 Distributed Coordination Function with Exponential Increase Exponential Decrease Backoff Algorithm,” in proceedings of the 57<sup>th</sup> IEEE Semiannual Vehicular Technology Conference (VTC’03), vol. 4, pp. 2775-2778, Apr. 2003.
- [28] J. G. Ko, Y. H. Cho and H. Kim, “Performance Evaluation of IEEE 802.15.4 MAC with Different Backoff Ranges in Wireless Sensor Networks,” in proceedings of the 10<sup>th</sup> IEEE International Conference on Communications Systems (ICCS’06), pp. 1-5, Singapore, Oct. 2006.
- [29] S. Y. Lee, Y. S. Shin, J. S. Ahn and K. W. Lee, “Performance Analysis of a Non-Overlapping Binary Exponential Backoff Algorithm over IEEE 802.15.4,” in proceedings of the 4th International Conference on Ubiquitous Information Technologies & Applications (ICUT’09), Japan, Dec. 2009.
- [30] S. Woo, W. Park, S. Y. Ahn, S. An and D. Kim, “Knowledge-Based Exponential Backoff Scheme in IEEE 802.15.4 MAC,” *Lecture Notes in Computer Science (LNCS)*, vol. 5200, pp. 435-444, 2008.
- [31] B. M. Khan, F. H. Ali and E. Stipidis, “Improved Backoff Algorithm for IEEE 802.15.4 Wireless Sensor Networks,” in proceedings of the 3<sup>rd</sup> IFIP Wireless Days (WD’10), Italy, Oct. 2010.
- [32] IEEE Std 802.15.4-2006, September, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).
- [33] B. H. Lee and H. K. Wu, “Study on Backoff Algorithm for IEEE 802.15.4 LR-WPAN,” in proceedings of the 22<sup>nd</sup> International Conference on Advanced Information Networking and Applications (AINA’08), pp. 403 - 409, Okinawa, Japan, Mar. 2008.
- [34] H. Minooei and H. Nojumi, “Performance evaluation of a new backoff method for IEEE 802.11,” *Computer Communications*, vol. 30, no. 18, pp. 3698-3704, Dec. 2007.
- [35] Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, *Adaptive Sleeping Periods in Slotted IEEE 802.15.4 for Efficient Energy Savings: Markov-Based Theoretical Analysis*, IEEE International Conference on Communications, ICC 2011, Kyoto, Japan, 5-9 June 2011.
- [36] P. Park, P. D. Marco, C. Fischione and K. H. Johansson, “Adaptive IEEE 802.15.4 protocol for reliable and timely communications,” in proceedings of the 9<sup>th</sup> ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN’10), pp. 327-338, Stockholm, Sweden, Apr. 2010.
- [37] S. Pollin, M. Ergen, S. C. Ergen, B. Bougard, L. V. derPerre, I. Moerman, A. Bahai, P. Varaiya and F. Catthoor, “Performance Analysis of Slotted Carrier Sense IEEE802.15.4 Medium Access Layer,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 9, pp. 3359-3371, Sept. 2008.
- [38] J. Mišić and V. B. Mišić, “Access Delay for Nodes with Finite Buffers in IEEE 802.15.4 Beacon Enabled PAN with Uplink Transmissions,” *Computer Communications*, vol. 28, no. 10, pp. 1152-1166, Jun. 2005.
- [39] J. Zhu, Z. Tao and C. Lv, “Performance Evaluation of IEEE 802.15.4 CSMA/CA Scheme Adopting a Modified LIB Model,” *Wireless Personal Communications, Online First*: <http://www.springerlink.com/content/712431107jwx1h66/fulltext.pdf>, pp. 1-27, Jan. 2011.
- [40] R. Jain, D. Chiu and W. Hawe, “A Quantitative Measure of Fairness and Discrimination for Resource Allocation in Shared Computer Systems”, DEC-TR-301, Sept. 26<sup>th</sup>, 1984.
- [41] M. Martalò, G. Ferrari and S. Busanelli, “Markov Chain-Based Performance Analysis of Multihop IEEE 802.15.4 Wireless Networks,” *Performance Evaluation*, vol. 66, no. 12, pp. 722-741, Dec. 2009.
- [42] I. Ramachandran, A. K. Das and S. Roy, “Analysis of the Contention Access Period of IEEE 802.15.4 MAC,” *ACM Transactions on Sensor Networks*, vol. 3, no. 1, article 4, Mar. 2007.
- [43] Z. Xiao, C. He and L. Jiang, “Slot-Based Model for IEEE 802.15.4 MAC with Sleep Mechanism,” *IEEE Communications Letters*, vol. 14, no. 2, pp. 154-156, Feb. 2010.
- [44] C. Y. Jung, H. Y. Hwang, D. K. Sung and G. U. Hwang, “Enhanced Markov Chain Model and Throughput Analysis of the Slotted CSMA/CA for IEEE 802.15.4 Under Unsaturated Traffic Conditions,” *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, pp. 473-478, Jan 2009.
- [45] S. Fang, L. Rong, Q. Xu and Y. Du, “Analysis of Performance of Unsaturated Slotted IEEE 802.15.4 Medium Access Layer,” in proceedings of PIRS, pp. 348-352, Beijing, China, Mar. 23-27, 2009.
- [46] Z. Chen, C. Lin, H. Wen and H. Yin, “An Analytical Model for Evaluating IEEE 802.15.4 CSMA/CA Protocol in Low-Rate Wireless Application,” in proceedings of the 21<sup>st</sup> International Conference on Advanced Networking and Applications Workshops (AINAW’07), vol. 2, pp. 899-904, Niagara Falls, Ontario, Canada, May 2007.
- [47] I. Ramachandran, A. K. Das and S. Roy, “Analysis of the Contention Access Period of IEEE 802.15.4 MAC,” *ACM Transactions on Sensor Networks*, vol. 3, no. 1, article 4, Mar. 2007.
- [48] K. Ashrafuzzaman and K. S. Kwak, “On the Performance Analysis of the Contention Access Period of IEEE 802.15.4 MAC,” *IEEE Communications Letters*, vol. 15, no. 9, Sept. 2011.
- [49] J. Zhu, Z. Tao and C. Lv, “Delay Analysis for IEEE 802.15.4 CSMA/CA Schemewith Heterogeneous Buffered Traffic,” in proceedings of the 3<sup>rd</sup> International Conference on Measuring Technology and Mechatronics Automation (ICMTMA’11), vol. 1, pp. 835-845, Shanghai, China, Jan. 2011.
- [50] A. Faridi, M. R. Palattella, A. Lozano, M. Dohler, G. Boggia, L. A. Grieco and P. Camarda, “Comprehensive Evaluation of the IEEE 802.15.4 MAC Layer Performance With Retransmissions,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, Oct. 2010.

- [51] S. Wijetunge, U. Gunawardana and R. Liyanapathirana, "Performance Analysis of IEEE 802.15.4 MAC Protocol for WSNs with ACK Frame Transmission Under Unsaturated Traffic Conditions," in proceedings of the 6<sup>th</sup> International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP'10), pp. 55-60, Brisbane, Australia, Dec. 2010.
- [52] C. M. Wong, R. L. Lai and I. T. Lai, "An Enhanced Carrier Sensing Algorithm for IEEE 802.15.4 Low-Rate Wireless Sensor Networks," in proceedings of IEEE Symposium on Industrial Electronics and Applications (ISIEA'10), pp. 10-15, Penang, Malaysia, Oct. 2010.
- [53] J. Deng, P. K. Varshney and Z. J. Hass, "A New Backoff Algorithm for the IEEE 802.11 Distributed Coordination Function," in proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS '04), San Diego, California, USA, Jan. 2004.
- [54] K. C. Noh, S. Y. Lee, Y. S. Shin, K. W. Lee and J. S. Ahn, "Performance Evaluation of an Adaptive Congestion Avoidance Algorithm for IEEE 802.15.4," in proceedings of the IEEE 13<sup>th</sup> International Conference on Computational Science and Engineering (CSE'10), pp. 14-19, Hong Kong, China, Dec. 2010.
- [55] P. Serrano, A. Bachs, V. Targon and J. F. Kukielka, "Detecting Selfish Configurations in 802.11 WLANs," IEEE Communications Letters, vol. 14, no. 2, pp. 142-144, Feb. 2010.
- [56] L. Guang and C. Assi, "Mitigating Smart Selfish MAC Layer Misbehaviour in Ad Hoc Networks," in proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking, and Communications (WiMob '06), pp. 116-123, Montreal, Quebec, Canada, Jun. 2006.
- [57] L. Guang and C. Assi, "MAC Layer Misbehavior in Wireless Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 15, no. 4, pp. 6-14, Aug. 2008.
- [58] M. Raya, I. Aad, J. P. Hubaux and A. El Fawal, "DOMINO: Detecting MAC Layer Greedy Behaviour in IEEE 802.11 Hotspots," IEEE Transactions on Mobile Computing, vol. 5, no. 12, pp. 1691-1705, Dec. 2006.
- [59] K. Kredo and P. Mohapatra, "Medium access control in wireless sensor networks", Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 51, no. 4, pp. 961-994, 2007.
- [60] Zolertia Z1 datasheet, [http://zolertia.sourceforge.net/wiki/images/e/e8/Z1\\_RevC\\_Datasheet.pdf](http://zolertia.sourceforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf), Mar. 2010.
- [61] Lucent Technologies, WaveLAN/EC-S User's Guide, [http://wireless.ictp.it/school\\_2001/docs/specs/orinoco/station\\_adapter.pdf](http://wireless.ictp.it/school_2001/docs/specs/orinoco/station_adapter.pdf).
- [62] RFM ZPM3570 ZigBee Pro Module datasheet, <http://www.rfm.com/products/data/zpm3570-e.pdf>, May 2011.
- [63] M. O. Rahman, C. S. Hong, S. Lee and Y. C. Bang, "ATLAS: A Traffic Load Aware Sensor MAC Design for Collaborative Body Area Sensor Networks," Sensors, vol. 11, no. 12, pp. 11560-11580, Dec. 2011.
- [64] B. Otal, L. Alonso and C. Verikoukis, "Energy-Efficiency Analysis of a Distributed Queuing Medium Access Control Protocol for Biomedical Wireless Sensor Networks in Saturation Conditions," Sensors, vol. 11, no. 2, pp. 1277-1296, Jan. 2011.
- [65] X. Sun and L. Dai, "Backoff Design for IEEE 802.11 DCF Networks: Fundamental Tradeoff and Design Criterion," In Proceedings of the IEEE/ACM Transactions on Networking, Vol. 23, No. 1, pp. 300-316, 2015.
- [66] D. Sharma, R. Srivastava and R. K. Sharma, "Effect of Contention Windows Size in Binary Exponential Back of Algorithm," in Proceedings of the Second International Conference on Advances in Computing and Communication Engineering, pp. 655-660, 2015.
- [67] A. Ullah and J. S. Ahn, "Performance evaluation of X-MAC/BEB protocol for wireless sensor networks," In Journal of Communications and Networks, Vol. 18, No. 5, pp. 857-869, 2016.
- [68] Q. Liu and A. Czulwik, "A collision-aware backoff mechanism for IEEE 802.15.4 wireless sensor networks," in 2013 IFIP Wireless Days (WD), pp. 1-3, 2013.
- [69] M. Shurman, B. Al-Shua'b, M. Alsaadeen, M. F. Al-Mistarihi and K. A. Darabkh, "N-BEB: New backoff algorithm for IEEE 802.11 MAC protocol," In Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, pp. 540-544, 2014.
- [70] X. Liu, G. Ma, H. Kuang and F. Li, "An efficient backoff algorithm for QoS guaranteeing in wireless networks," In Proceedings of the Chinese Control and Decision Conference, pp. 5353-5358, 2016.
- [71] Y. He, J. Sun, X. Ma, A. V. Vasilakos, R. Yuan and W. Gong, "Semi-Random Backoff: Towards Resource Reservation for Channel Access in Wireless LANs," In IEEE/ACM Transactions on Networking, Vol. 21, No. 1, pp. 204-217, Feb. 2013.
- [72] M. A. Bender, J. T. Fineman, S. Gilbert and M. Young, "How to Scale Exponential Backoff: Constant Throughput, Polylog Access Attempts, and Robustness," In Proceedings of the Twenty-seventh Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 636-654, 2016.
- [73] T. N. V. L. Alekhya, B. Mounika, E. Jyothi and B. N. Bhandari, "A waiting-time based backoff algorithm in the IEEE 802.11 based wireless networks," In Proceedings of the 2012 National Conference on Communications, pp. 1-5, 2012.
- [74] J. Sarrthong and S. Sittichivapak, "Backoff algorithm optimization for IEEE802.11 wireless local area networks," In Proceedings of the 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, pp. 1-4, 2012.
- [75] J. Sarrthong, S. Sittichivapak, A. Kaewpukdee and I. Boonpikum, "Binary Exponential Increment Half Decrement backoff algorithm for IEEE802.11 wireless LANs," In Proceedings of the 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, pp. 1-6, 2013.
- [76] R. T. Chekka, T. Miao and K. H. Kim, "Implementation of adaptive binary exponential backoff (ABEB) algorithm with dynamical sizing buffer for load-balanced RPL," In Proceedings of the sixth International Conference on Ubiquitous and Future Networks, pp. 562-564, 2014.
- [77] Q. Liu and A. Czulwik, "Study on adaptive priority-based service-differentiation scheme for IEEE 802.15.4 Wireless Sensor Networks," In Proceedings of the 2014 IEEE Symposium on Computers and Communications, pp. 1-6, 2014.
- [78] E. D. N. Ndihi and S. Cherkaoui, "Adaptive 802.15.4 backoff procedure to survive coexistence with 802.11 in extreme conditions," In Proceedings of the 13th IEEE Annual Consumer Communications Networking Conference, pp. 556-561, 2016.
- [79] Y. Huang, Y. Wang, R. Zhu, X. Chen and Q. Meng, "Synchronized contention windows-based backoff algorithm in IEEE 802.11 wireless networks," In Proceedings of the International Conference on Computer, Information and Telecommunication Systems, pp. 1-5, 2016.
- [80] M. Guennoun, M. Khanafer and H. T. Mouftah, "Modeling of Variable Clear Channel Assessment MAC Protocol for Wireless Sensor Networks," Elsevier Computer Communications, Volume 59, March 2015.

#### APPENDIX A

In Section IV, Equations (27) and (28) are used to formulate the reliability ( $R$ ) for a WSN operating the Adaptive Backoff Algorithm (ABA). In this appendix we show the detailed derivations of the probabilities of having  $m+1$  backoffs and/or  $n+1$  transmission retries [60].

Based on Equation (27), we can write the following set of equations:

$$z(\pi_s + \pi_{B_1} + \dots + \pi_{B_{m+1}} + \pi_c) = \pi_s \quad (A.1)$$

$$y(\pi_s + \pi_{B_1} + \dots + \pi_{B_{m+1}} + \pi_c) = \pi_c \quad (A.2)$$

$$x\pi_s + x\pi_{B_{m+1}} + x\pi_c = \pi_{B_1} \quad (A.3)$$

$$x\pi_{B_1} = \pi_{B_2} \quad (A.4)$$

$$x\pi_{B_m} = \pi_{B_{m+1}} \quad (A.5)$$

The summation  $\pi_s + \pi_{B_1} + \dots + \pi_{B_{m+1}} + \pi_c$  is equal to 1 because it includes all the states that a node can encounter while attempting to send a packet. Therefore, Equations (A.1) and (A.2) reduce to:

$$z = \pi_s \quad (A.6)$$

$$y = \pi_C \quad (A.7)$$

Therefore, Equation (A.3) can now be re-written as follows:

$$xz + x\pi_{B_{m+1}} + xy = \pi_{B_1} \quad (A.8)$$

From Equations (A.4) and (A.5), and by clearly examining Equation (27), we can directly see that  $\pi_{B_{m+1}}$  can be expressed in terms of  $\pi_{B_1}$ , as follows:

$$\pi_{B_{m+1}} = x^m \pi_{B_1} \quad (A.9)$$

By solving both Equations (A.8) and (A.9) for  $\pi_{B_{m+1}}$ , we end up with the following expression:

$$\pi_{B_{m+1}} = \frac{x^{m+1}(z+y)}{(1-x)^{m+1}} \quad (A.10)$$

Based on Equation (28), we can write the following set of equations:

$$z(\pi_s + \pi_{C_1} + \dots + \pi_{C_{n+1}} + \pi_B) = \pi_s \quad (A.11)$$

$$x(\pi_s + \pi_{C_1} + \dots + \pi_{C_{n+1}} + \pi_B) = \pi_B \quad (A.12)$$

$$y\pi_s + y\pi_{C_{n+1}} + \pi_{C_1}\pi_B = \pi_{C_1} \quad (A.13)$$

$$y\pi_{C_1} + \pi_{C_2}\pi_B = \pi_{C_{n+1}} \quad (A.14)$$

$$y\pi_{C_n} + \pi_{C_{n+1}}\pi_B = \pi_{C_{n+1}} \quad (A.15)$$

The summation  $\pi_s + \pi_{C_1} + \dots + \pi_{C_{n+1}} + \pi_B$  is equal to 1 because it includes all the states that a node can encounter while attempting to send a packet. Therefore, Equation (A.11) reduces to (A.6) while Equation (A.12) reduces to:

$$x = \pi_B \quad (A.16)$$

Therefore, Equations (A.13)-(A.15) can now be re-written as follows:

$$yz + y\pi_{C_{n+1}} + x\pi_{C_1} = \pi_{C_1} \quad (A.17)$$

$$y\pi_{C_1} + x\pi_{C_2} = \pi_{C_{n+1}} \quad (A.18)$$

$$y\pi_{C_n} + x\pi_{C_{n+1}} = \pi_{C_{n+1}} \quad (A.19)$$

From Equations (A.18) and (A.19), and by clearly examining Equation (28), we can directly see that  $\pi_{C_{n+1}}$  can be expressed in terms of  $\pi_{C_1}$ , as follows:

$$\pi_{C_{n+1}} = \left(\frac{y}{1-x}\right)^n \pi_{C_1} \quad (A.20)$$

By solving both Equations (A.17) and (A.20) for  $\pi_{C_{n+1}}$ , we end up with the following expression:

$$\pi_{C_{n+1}} = \frac{z\left(\frac{y}{1-x}\right)^{n+1}}{1 - \left(\frac{y}{1-x}\right)^{n+1}} \quad (A.21)$$

Finally, by knowing Equations (A.10) and (A.21), Equation (26) from Section IV, and by noticing that  $z = 1 - x - y$ , we can formulate  $R$  as follows:

$$R = \frac{1}{1 + \frac{(1-x)x^{m+1}}{(1-x^{m+1})(1-x-y)} + \frac{y^{n+1}}{(1-x)^{n+1} - y^{n+1}}}$$

# Distinctive Context Sensitive and Hellinger Convolutional Learning for Privacy Preserving of Big Healthcare Data

Sujatha K<sup>1</sup>

Research Scholar  
School of computing and IT  
REVA University, Bangalore, India

Udayarani V<sup>2</sup>

Senior Associate Professor  
School of computing and IT  
REVA University, Bangalore, India

**Abstract**—The collection and effectiveness of sensitive Big Data have grown with Information Technology (IT) development. While using sensitive Big Data to acquire relevant information, it becomes indispensable that irrelevant sensitive data are reduced to safeguard personal information in healthcare sector. Many privacy-preserving strategies have been applied in the recent years using quasi-identifiers (QI) for applications like health services. However, privacy preservation over quasi-identifiers is still challenging in the context of Big Data because most datasets were of huge volume. Existing methods suffer from higher time consumption and lower data utility because of dynamically progressing datasets. In this paper, an efficient Distinctive Context Sensitive and Hellinger Convolutional Learning (DCS-HCL) is introduced to ensure privacy preservation and achieve high data utility for big healthcare datasets. First, Distinctive Impact Context Sensitive Hashing model is designed for the given input Big Dataset where both the distinctive and impact values are identified and applied to Context Sensitive Hashing. With this, similar QI-classes are mapped to evolve the computationally efficient anonymized data. Second, Hellinger Convolutional Neural Privacy Preservation model is presented to preserve the privacy of the sensitive unstructured data. This is performed by hashing QI-class values, weight updation and bias in CNN to increase the accuracy and to reduce the information loss. Evaluation results demonstrate that with proposed method with large-volume unstructured datasets improved performance of run time, data utility, information loss and accuracy significantly over existing methods.

**Keywords**—Big data; information technology; distinctive; impact; context sensitive hashing; quasi-identifier; Hellinger; convolutional neural

## I. INTRODUCTION

Privacy-preservation issues have made an appearance with the growing magnitudes of data being issued together with sensitive, private information pertaining to individual persons and also business establishments. To address such issues, several strategies of minimizing risk connected with data being published have been designed. One of the remedies is protecting sensitive data via quasi identifier. Equivalence Classes with Cuckoo Filter (ENCC) [1] utilized anatomy alternative for suppression to design more effective l-diversity algorithm with the objective of preserving the privacy of those datasets. Moreover, a Cuckoo filter was utilized to approximate set-membership tests for enhancing the efficiency

involved in data processing. With the application of l-diversity algorithm, the running time was found reduced than when compared to traditional re-anonymization techniques.

In addition, filter mechanism was used to maintain privacy of dynamically progressing datasets. Despite maintaining privacy and reducing the running time with the absence of strong data-anonymization models, data utility was not focused. To address this issue, in this work, Distinctive Impact Context Sensitive Hashing model is designed that evolves with computationally efficient quasi-identifiers with minimal time and higher data utility.

A novel privacy model utilizing integrated anonymization and reconstruction was proposed in [2] for making the strong assumption. The separation of quasi-identifiers (QIDs) was carried out from sensitive attributes. A sensitive QID using l-diversity and t-closeness was designed. It was in novel privacy model, anonymization and reconstruction was possible while maintaining the high quality of data within stipulated time period.

Though high data quality within stipulated time period was maintained, the accuracy and information loss was not concentrated. To address this issue in this work, Hellinger Convolutional Neural Privacy Preservation model is proposed to protect both the sensitive data by designing a significant privacy preservation model considering both the distance by means of Hellinger and improving the accuracy by updated weight and bias via convolutional neural learning.

## A. Contributions

The main contributions of this paper to the literature are summarized as follows:

- A, Distinctive Context Sensitive and Hellinger Convolutional Learning (DCS-HCL) method is designed with the purpose of preserving the privacy of big healthcare data along with high data utility and minimum information loss.
- Distinctive Impact Context Sensitive Hashing model is developed for performing sensitive hashing to surpass the defined limitations and focuses on the run time and therefore improving the data utility.

- Hellinger Convolutional Neural Privacy Preservation model is a new privacy preservation model used for identifying quasi-identifiers to improve accuracy and reduce information loss.
- Privacy preservation methods are compared with the conventional privacy preservation ones. Experimental results demonstrated that proposed method showed comparatively better performance in terms of run time, accuracy and loss error.

### B. Organization Structure

The organization of this paper is as follows. Section II reviews the development of privacy preservation techniques concerning big data. The details of the proposed method Distinctive Context Sensitive and Hellinger Convolutional Learning (DCS-HCL) is presented in Section III. The experimental analysis of the proposed method is discussed in Section IV. The result discussion with the other well-known privacy preservation methods is presented in Section V. Finally, the conclusion is given in Section VI.

## II. RELATED WORKS

In recent years, the escalating issue of Internet phishing has been menacing the secure proliferation of sensitive data over the web, including several domains like healthcare data, video surveillance, Internet trafficking and so on. Therefore, privacy preservation has become a major challenge resulting in imprecise distribution of data.

A global survey on privacy preservation for big data was investigated in [3]. But, the information loss was not minimized. With big healthcare data to enhance patient outcomes, to predict pandemic outbreaks in early stage, keep away from avertable diseases, the security and privacy concerns were discussed in [4]. But, the runtime consumption was not minimized. An encryption algorithm using honey encryption algorithm was proposed in [5] to address the issues related to data security. However, the dimensionality issues were not minimized. A comprehensive focus was made for identical data types using quasi-identifiers called identical generalization hierarchy (IGH). An optimal solution was designed based on globally optimized k-anonymity [6] for minimizing the overall convergence time to a greater extent. But, accuracy level was not taken into consideration.

The privacy preservation in big data utilizing solution towards data warehousing was proposed in [7] using nearest similarity based clustering (NSB) with Bottom-up generalization. The susceptibility with respect to sensitivity was addressed and ensured privacy for user data. But, the computational cost was not minimized. A survey of privacy preservation techniques was investigated in [8]. However, security level was not improved. A review of privacy preservation for resource constrained sensors was proposed in [9]. However, attribute disclosure prevention were not met.

Two privacy models called enhanced identity-reserved diversity and enhanced identity-reserved anonymity were presented in [10] to minimize the error. Though the error was reduced, multiple sensitive attributes preservation remained unaddressed. To provide solution to this issue, bucketization

principles were utilized in [11] for preserving the vulnerable records. But, the computational complexity was not minimized. A bidirectional personalized generalization model was designed in [12] for multi-record datasets. Through validating the quasi-identifier anonymity and ensuring diversity on equivalence groups, information loss was reduced to a large extent. However the privacy level gets varied for different users.

In [13], a privacy preservation model to prevent data loss using hash anomaly detection process was designed, therefore improving the data privacy along with the minimization of data portability cost. However, the time consumption was not minimized. In [14], local differential privacy was applied with the objective of providing significant accuracy. Though the accuracy level was improved, the computational cost was not minimized. In [15], a healthcare privacy preservation scheme called, Healthchain was designed on the basis of the blockchain technology. The healthcare data were initially encrypted for ensuring fine-grained access control. The users significantly had possibility of either revoking or including certain features for efficient key management. But, the runtime was not reduced for healthcare privacy preservation.

Tampering was avoided to keep away from contentions or alterations for ensuring both privacy and security. In [16], security and privacy issues concerning healthcare sector was surveyed and mechanisms were included in addressing the issues. The focus was specifically designed depending one anonymization and encryption. Moreover, the advantages and disadvantages of introducing the anonymization and encryption standards were also made. However, the accuracy level was not taken into consideration.

An in-depth concentration on privacy and security aspects in big data and differentiation between the privacy and security aspects in big data was presented in [17]. But, the information loss was not focused. A systematic approach was proposed in [18] for selecting the seed with the purpose of clustering the records by employing adaptive  $k$ -anonymity algorithm. But, privacy preservation performance was not improved considerably. Rough set approach was proposed in [19] to balance between quasi-identifier anonymity and sensitive attribute diversity. However, runtime performance was not at required level by designed approach.

### A. Research Gap

As a part of information sharing information via internet, each business establishments print data that are considered to be highly sensitive or personal. In this advancing IT-era towards big data, user's privacy protection is becoming a major issue to be addressed. In the recent years, as prototype of medical services has transformed from therapy to safeguard, there arises the heightening interest in healthcare sector. Despite the data being valuable asset, serious privacy issue is said to occur with the leakage of sensitive information. These data have to be preserved. After reviewing the existing methods, there are still difficulties in data utility management and information loss.

In addition, the high information loss, high runtime consumption, high computational cost, high computational

complexity, less accuracy, less security and privacy were issues faced by the user's during data communication in healthcare sector. Therefore, Distinctive Context Sensitive and Hellinger Convolutional Learning (DCS-HCL) is introduced for support fine-grained access control with big healthcare data to ensure data utility with high accuracy and minimum information loss as well as runtime consumption.

### III. METHODOLOGY

In this section, the quasi-identifier arrangement based x model and y model are formulated in detail. Section 'A' sketches out the system model. In Section 'B', Distinctive Impact Context Sensitive Hashing model is described for quasi-identifier detection from Big (unstructured) Data. Based on the established arrangements (i.e. detected quasi-identifier) via Quasi-Identifier Classes, Section 'C' elaborates the design and development of privacy preservation for unstructured data. Fig. 1 shows the block diagram of Distinctive Context Sensitive and Hellinger Convolutional Learning (DCS-HCL) method.

As shown in Fig. 1, large volume Big Data dataset of diabetic patients are provided as input. Attribute segregation is initially performed with the input Big Data dataset by means of Distinctive Impact Context Sensitive Hashing model. With this, unique QI-classes possessing unstructured data are mapped to detect the computationally efficient anonymous data (i.e., quasi attributes or quasi-identifiers) from Big Data.

#### A. System Model

Let us consider a big data dataset 'DS' extracted from Diabetes 130-US hospitals for years 1999-2008 Data Set [3] consisting of 50 different features or attributes 'Attr =  $a_1, a_2, \dots, a_n$ ' of 'n' patients. Each attribute classifies the data columns 'C' into four different classes 'Cl =  $\{cl_1, cl_2, cl_3, cl_4\}$ ' referred to as quasi attributes 'Q =  $\{q_1, q_2, \dots, q_n\}$ ', external attributes 'E =  $\{e_1, e_2, \dots, e_n\}$ ', sensitive attributes 'S =  $\{s_1, s_2, \dots, s_n\}$ ' and non-sensitive attributes 'NS =  $\{ns_1, ns_2, \dots, ns_n\}$ ' respectively.

#### B. Distinctive Impact Context Sensitive Hashing Model

First quasi attributes are identified from Big Data using Distinctive Impact Context Sensitive Hashing (DI-CSH) model. Quasi attributes are attributes that reveal data of precise identifiers employing background knowledge. Several strategies have been presented by various research analysts to identify the quasi identifiers where resources are considered for executing privacy. However, these techniques are not free from limitations like higher time consumption and lower data utility. The proposed DI-CSH model controls the limitation by extracting base essential quasi attributes with minimum time complexity and higher data utility. In ENCC [1] method, anonymization has been applied on quasi identifiers to convert it into more diversified form, the privacy expanded to certain extent. But, the issue remains in identifying the optimal quasi attributes in big data dataset.

Many quasi attributes on one side decreases the data utility. On other hand, less quasi attributes results in privacy breach. The objective of Distinctive Impact Context Sensitive Hashing model is to identify the optimal quasi attributes in Big Data dataset in optimal time and complexity resulting in the improvement of performance in preserving the privacy with the optimal number of quasi attributes. Fig. 2 given above shows the sample format of Distinctive Impact Context Sensitive Hashing model.

As shown in the above Fig. 2, with the input diabetic dataset provided as input, the objective of designing Distinctive Impact Context Sensitive Hashing model remains in extracting the quasi-attributes with minimum time complexity and high data utility. The distinctive value 'DV' is evaluated based on the number of distinct values 'DV' in column 'C<sub>i</sub>' and the total number of different values in column 'TV' respectively. The distinctive value is expressed as given below.

$$DV = \frac{\sum_{i=1}^n DV[C_i]}{TV} \quad (1)$$

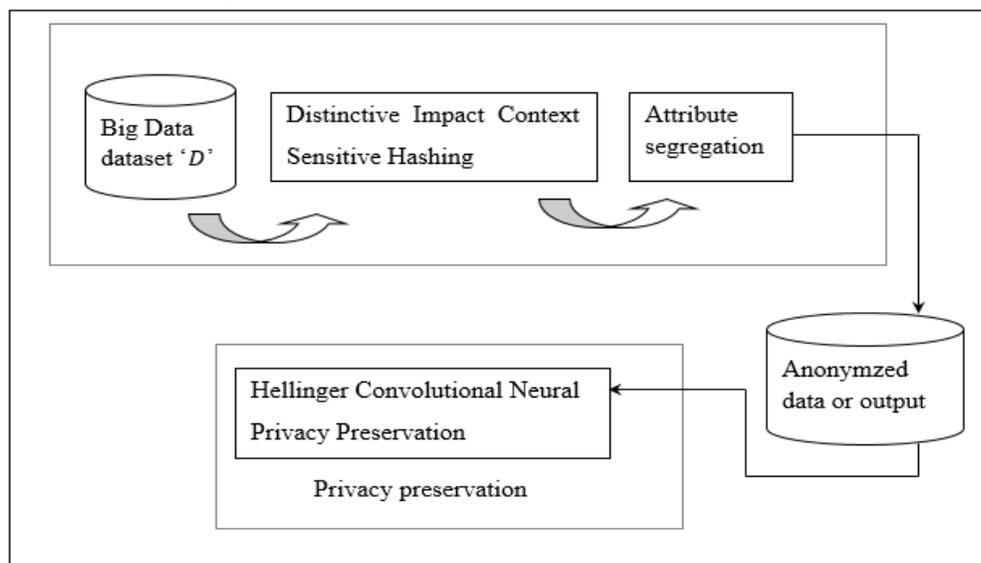


Fig. 1. Block Diagram of Distinctive Context Sensitive and Hellinger Convolutional Learning Method.

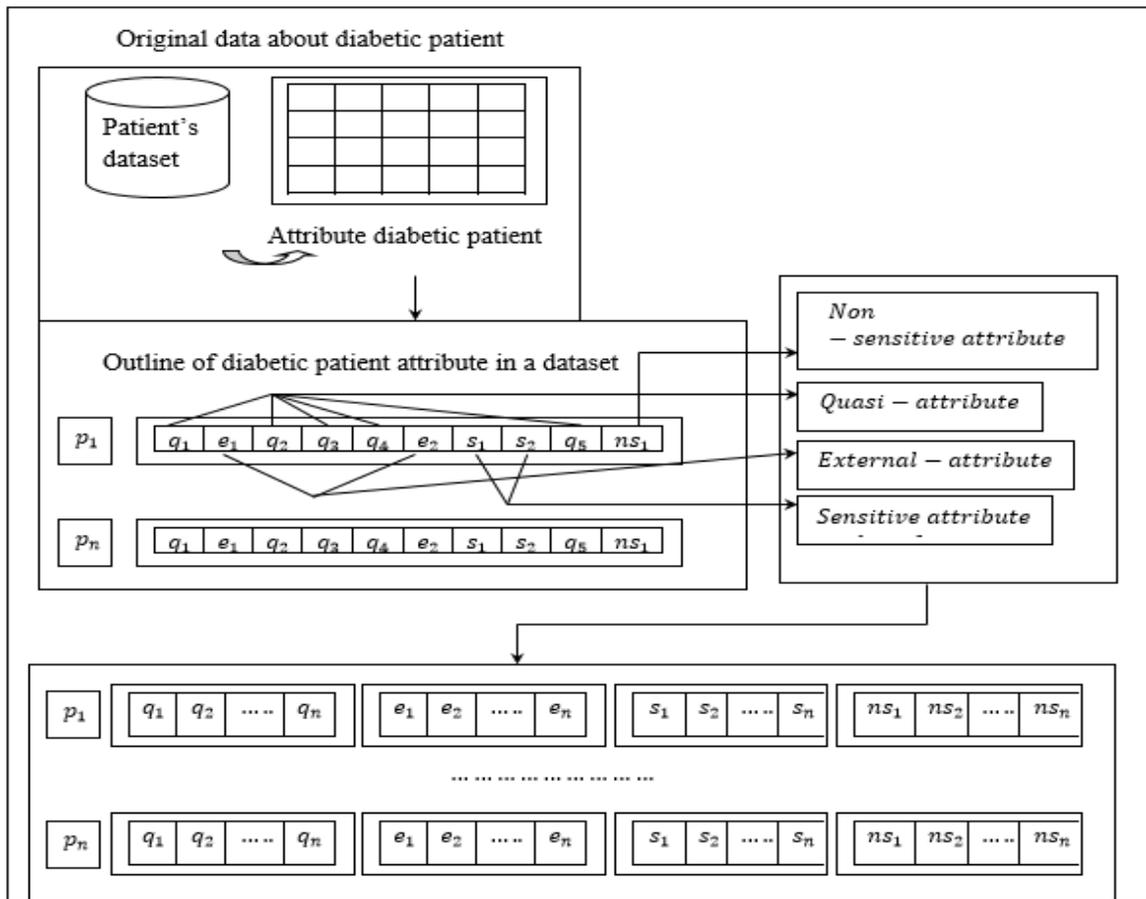


Fig. 2. Sample Distinctive Impact Context Sensitive Hashing.

Next, the impact value ‘IV’ is evaluated based on the equivalent class ‘EC’, total number of different values in column ‘TV’ and the ‘ith’ column in consideration ‘Ci’ respectively.

$$IV = 1 - \frac{EC(TV - C_i)}{EC(TV)} \quad (2)$$

To improve the performance of arrangements of Quasi Identifier Classes (QI-classes), heterogeneous and unstructured data were used in terms of missing values or inconsistent record, the hash function ‘H(qeid)’ map similar QI-classes in place of arbitrarily map QI-classes. When QI-classes are nearer in terms of their quasi-identifiers, segregating QI-classes while preserving privacy become more ease when compared with dynamically evolving datasets [1] dispersed in a dynamic manner.

For instance, Context Hashing and hash QI-classes are integrated for every distinctive and impact values generated for total number of different values in column. The distance designates proximity between two quasi-identifiers (i.e. quasi encounter identifiers) ‘ $qeid^x$ ’ and ‘ $qeid^y$ ’. It is described in order to incorporate Context Hashing. Let distance between two quasi-identifiers denoted as ‘ $Dis(qeid^x, qeid^y)$ ’ and moreover ‘ $qeid^x = (q_1^x, q_2^x, \dots, q_n^x)$ ’ and ‘ $qeid^y = (q_1^y, q_2^y, \dots, q_n^y)$ ’ respectively. Then, the distance is mathematically expressed as given below.

$$Res = Dis(qeid^x, qeid^y) = \sqrt{\sum D^2(q_i^x, q_i^y)} \quad (3)$$

Equation (3), ‘ $D(q_i^x, q_i^y)$ ’, represent the distance between ‘ $q_i^x$ ’ and ‘ $q_i^y$ ’. With the resultant distance obtained from the above equation (3), a Context Hash function is associated to map homogeneous QI-classes. Let us assume that ‘ $d_i$ ’ and ‘ $d_j$ ’ are two distances, then the hash function is evolved using ‘ $(d_i, d_j)$ ’ for any two quasi-identifiers ‘ $qeid^x, qeid^y$ ’ via duality principle and probability function as stated in the pseudo code. The pseudo code representation of Distinctive Impact Context Hash is given below.

As given in the above Distinctive Impact Context Hash Quasi-Identifier algorithm, three steps are incorporated. First, with the big data dataset (i.e., diabetic dataset) provided as input, distinctive and impact value for total number of different values in columns are identified. Then, similar QI-classes are mapped by means of a Context Hashing distance function. Finally, with the aid of the duality principle by mapping similar QI-classes, computationally efficient similar quasi-identifiers are obtained. With application of this algorithm, optimal and computationally efficient quasi-identifiers are identified. Therefore, maximum of attributes are not selected as quasi-identifiers and only optimal attributes are selected as quasi-identifiers to improve data utility performance.

Algorithm 1: Distinctive Impact Context Hash Quasi-Identifier

<b>Input:</b> Patients ‘ $P = P_1, P_2, \dots, P_n$ ’, big data dataset ‘ $DS$ ’, attributes ‘ $Attr = a_1, a_2, \dots, a_n$ ’
<b>Output:</b> Computationally efficient and optimized quasi-identifiers
<p>Step 1: <b>Initialize</b> ‘<math>qeid^x</math>’ and ‘<math>qeid^y</math>’</p> <p>Step 2: <b>Initialize</b> classes ‘<math>Cl = \{cl_1, cl_2, cl_3, cl_4\}</math>’, column ‘<math>C_i</math>’</p> <p>Step 3: <b>Begin</b></p> <p>Step 4: <b>For</b> each big data dataset ‘<math>DS</math>’ with ‘<math>n</math>’ attributes ‘<math>Attr = a_1, a_2, \dots, a_n</math>’ and Patients ‘<math>P</math>’</p> <p>Step 5: <b>For</b> two quasi-identifiers (i.e., quasi encounter identifiers) ‘<math>qeid^x</math>’ and ‘<math>qeid^y</math>’</p> <p>Step 6: Evaluate distinctive value using equation (1)</p> <p>Step 7: Evaluate impact value using equation (2)</p> <p>Step 8: Evaluate distance between two quasi-identifiers using equation (3)</p> <p>Step 9: <b>If</b> ‘<math>Res(qeid^x, qeid^y) \leq d_j</math>’</p> <p>Step 10: <b>Then</b> ‘<math>Prob[H(qeid^x) = H(qeid^y)]</math>’</p> <p>Step 11: <b>End if</b></p> <p>Step 12: <b>If</b> ‘<math>Res(qeid^x, qeid^y) \geq d_j</math>’</p> <p>Step 13: <b>Then</b> ‘<math>Prob[H(qeid^x) = H(qeid^y)]</math>’</p> <p>Step 14: <b>End if</b></p> <p>Step 15: <b>End for</b></p> <p>Step 16: <b>End for</b></p> <p>Step 17: <b>Return</b> quasi attributes ‘<math>p = Q = \{q_1, q_2, \dots, q_n\}</math>’</p> <p>Step 18: <b>End</b></p>

C. Hellinger Convolutional Neural Privacy Preservation Model

With the computationally efficient quasi-identifiers retrieved, Distinctive Impact Context Hash Quasi-Identifier algorithm is used to learn features from unstructured data and initialize the CNN arrangement. Hellinger Convolutional

Neural Privacy Preservation model is used to reduce significant amount of information loss while identifying quasi-identifiers and preserving it for ensuring privacy.

In this work, Hellinger Distance values are determined in each equivalence class (i.e. class other than QI-classes) to quantify the distance. After that, the cautious scrutiny is paid to QI-classes with minimum distance values. By quantifying the distance, information loss is said to be minimized and accuracy level gets increased. Then, the learned Distinctive Impact Context Hash Quasi-Identifier is utilized to train a CNN for privacy preservation. The proposed privacy-preserving data analysis architecture is illustrated in Fig. 3.

As illustrated in the above Fig. 3, with the separation between QI-classes and non QI-classes, let us assume that ‘ $X = \{x_1, x_2, \dots, x_n\}, x_i \in R^m$ ’, where ‘ $X = Q = \{q_1, q_2, \dots, q_n\}$ ’, where ‘ $n$ ’ represents the number of samples (i.e. other than quasi identifiers obtained in QI-classes) and ‘ $m$ ’ represents the length of non-quasi identifiers, ‘ $Y = SIGMOID(Wa + b)$ ’. ‘ $W$ ’ represents the weight and ‘ $b$ ’ represents the bias respectively. With these two, activation function is mathematically expressed as given below.

$$H_{w,b} = H(x_i, W, b) = SIGMOID(Wx_i + b) \tag{4}$$

In equation (4), the sigmoid of the weight along with the bias is utilized at the average activation. The origination hypothesis is then mathematically formulated as given below.

$$P_{init} = \sum_{j=1}^l HD(\alpha || \alpha_j) \tag{5}$$

From the above equation (5), ‘ $l$ ’ refers to the number of samples remained in Big Data dataset after the application of quasi-identifier detection and ‘ $HD(.)$ ’ refers to the Hellinger distance, quantifying the similarity between two probability distributions. This is mathematically formulated as given below.

$$H^2(P, Q) = \int (\sqrt{dP} - \sqrt{dQ})^2 \tag{6}$$

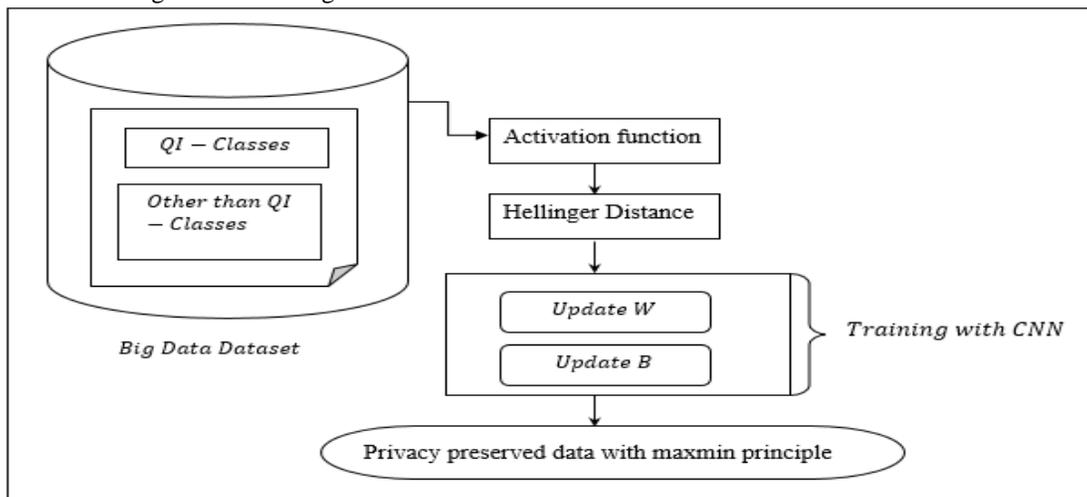


Fig. 3. Architecture of Proposed Privacy-Preserving Data Analysis.

From the above equation (6), ‘P’ and ‘Q’ refers to the two probability measures (i.e., quasi encounter identifiers and the non-quasi encounter identifiers) are continuous with respect to the third measure with a different probability measure with respect to which both ‘P’ and ‘Q’ are continuous. Next, the learned Distinctive Impact cost function is mathematically expressed as given below.

$$C_{Cl}(W, b) = \left[ \frac{1}{n} \sum_{i=1}^n \left( \frac{1}{2} (H_{W,b}(x_i) - (y_i))^2 \right) + H^2(P, Q) \right] \quad (7)$$

From the above equation (7), the cost function ‘ $C_{Cl}$ ’ is arrived at based on resultant activation function ‘ $H_{W,b}$ ’, its Hellinger distance ‘ $H^2(P, Q)$ ’ and the input vector ‘ $x_i$ ’. The parameters ‘ $W_{ij}$ ’ and ‘ $b_i$ ’ are updated and formulated as,

$$W_{ij} = W_{ij}(l) - LR \frac{\partial}{\partial W_{ij}(l)} \quad (8)$$

$$b_i = b_i(l) - LR \frac{\partial}{\partial b_i(l)} \quad (9)$$

Finally, the mean square error of the Distinctive Impact cost function is evaluated as given below.

$$C(W, b) = \left[ \frac{1}{n} \sum_{i=1}^n \left( \frac{1}{2} (H_{w,b}(x_i) - (y_i)^2) \right) + \frac{y}{2} \sum_{i=1}^n \sum_{j=2}^n \sum_{l=1}^n W_{ij}(l) \right] \quad (10)$$

Finally, the efficiency of the proposed Distinctive Impact cost function is verified by original and transformed data from the Big Data dataset to train CNN for classification and to ensure privacy of the data. The pseudocode representation of Hellinger Convolutional Neural Privacy Preservation is given below.

Algorithm 2: Hellinger Convolutional Neural Privacy Preservation

<b>Input:</b> Input Vector ‘ $X = \{x_1, x_2, \dots, x_n\}, x_i \in R^m$ ’
<b>Output:</b> Accurate and minimum loss privacy preserved identifiers
<p>Step 1: <b>Initialize</b> Weight ‘<math>W</math>’, Bias ‘<math>B</math>’</p> <p>Step 2: <b>Begin</b></p> <p>Step 3: <b>For</b> each Input Vector ‘<math>X</math>’</p> <p>Step 4: Mathematically formulate activation function using equation (4)</p> <p>Step 5: Obtain origination hypothesis using equation (5)</p> <p>Step 6: Evaluate similarity between two probability distribution using equation (6)</p> <p>Step 7: Mathematically formulate learned Distinctive Impact cost function using equation (7)</p> <p>Step 8: Update parameters weight and bias using equation (8) and (9)</p> <p>Step 9: Evaluate mean square error of the Distinctive Impact cost function using equation (10)</p> <p>Step 10: <b>Return</b> (privacy preserved identifiers)</p> <p>Step 11: <b>End for</b></p> <p>Step 12: <b>End</b></p>

As given in the above Hellinger Convolutional Neural Privacy Preservation algorithm, three steps are followed. At first, non QI-classes are provided as input. After that, the process remains in generating maxmin principle (i.e., maximizing accuracy and minimizing information loss) to ensure privacy preservation for unstructured data for protecting the sensitive data. An activation function is derived by hashing QI-classes and then using Hellinger distance to minimize the information loss with minimum distance values. After that, it is provided as input for learning with updated CNN, i.e., updating weight and bias by Distinctive Impact cost function. In this manner, the accuracy level and the information loss is improved. Therefore, privacy preservation of sensitive unstructured data is carried out in efficient manner.

#### IV. EXPERIMENTAL ANALYSIS

In this section, a detailed analysis of experimental results has been presented to evaluate the performance of Distinctive Context Sensitive and Hellinger Convolutional Learning (DCS-HCL) method for privacy preserving of sensitive unstructured big healthcare data through quasi-identifier. Based on recent state-of-the-art methods in the literature, an evaluation of privacy preservation of big healthcare data using quasi identifiers is performed in terms of run time, accuracy and information loss with respect to number of patients. The proposed DCS-HCL method is compared with two existing privacy preservation methods, Equivalence Classes with Cuckoo Filter (ENCC) [1] and integrated anonymization and reconstruction [2]. The result analysis shows that DCS-HCL method ensures data utility with higher accuracy and minimum information loss as well as runtime consumption for support fine-grained access control with big healthcare data when compared to state-of-the-art works.

##### A. Dataset Description

The Diabetes 130-US hospitals for years 1999-2008 Data Set [20] is used for conducting the experiments. The dataset comprises 10 years of clinical care obtained from 130 US hospitals and integrated delivery networks and covers 50 features denoting patient and hospital outcomes. Certain attributes present in dataset are patient number, race, gender, age, admission type, time in hospital, medical specialty of admitting physician, number of lab test performed, HbA1c test result, diagnosis, number of medication, diabetic medications, numbers of outpatient, inpatient, and emergency visits in year before hospitalization, etc. With the aid of this dataset experiments for privacy preserving is conducted using Python. In this section, performance metrics, namely run time, accuracy and information loss with respect to number of patients are considered for privacy preservation.

1) *Run time evaluation:* With the big healthcare data being shared between the patients and in public domain, the run time involved should be minimum otherwise the data is said to be loss or privacy is said to be compromised. However, a significant amount of time is said to be consumed while preserving privacy of big healthcare data. The run time involved is mathematically expressed as given below.

$$RT = \sum_{i=1}^n P_i * Time [PP] \quad (11)$$

From the above equation (11), the run time ‘RT’ involved in preserving the privacy of big healthcare data using quasi identifiers is evaluated based on the number of patients considered during simulation ‘ $P_i$ ’ and the time involved in preserving the privacy ‘ $Time [PP]$ ’. It is measured in terms of milliseconds (ms).

2) *Accuracy evaluation*: The accuracy maintenance for quasi identifiers is an important issue in preserving privacy of big healthcare data. The accuracy refers to the amount of sensitive data being preserved during the process involved in privacy preservation using quasi identifiers. The accuracy measure is mathematically expressed as given below.

$$A = \sum_{i=1}^n \frac{P_{AP}}{P_i} * 100 \quad (12)$$

From the above equation (12), the accuracy ‘ $A$ ’ is measured on the basis of the number of patients ‘ $P_i$ ’ considered for simulation and the patients data accurate preserved ‘ $P_{AP}$ ’. It is measured in terms of percentage (%).

3) *Information loss evaluation*: During the privacy preservation of big healthcare data, certain amount of information gets lost. However, the information loss should be lesser so that higher amount of information is said to be preserved. The information loss is mathematically evaluated as given below.

$$IL = \sum_{i=1}^n \frac{P_{dc}}{P_i} * 100 \quad (13)$$

From the above equation (13), the information loss ‘ $IL$ ’ is obtained on the basis of the number of patients considered for conducting simulation ‘ $P_i$ ’ and the number of patient data compromised ‘ $P_{dc}$ ’ during privacy preservation. It is expressed in terms of percentage (%).

## V. RESULT AND DISCUSSIONS

In this section, a series of experiments are conducted to verify the significance of the proposed method Distinctive Context Sensitive and Hellinger Convolutional Learning (DCS-HCL) using Diabetes 130-US hospitals dataset. Then, three commonly used evaluation metrics, run time, accuracy and information loss are used to compare the performance of the privacy preservation with two existing methods, Equivalence Classes with Cuckoo Filter (ENCC) [1] and integrated anonymization and reconstruction [2].

### A. Performance Measure of Run Time

First, the performance analysis of run time is carried out. Table I shows the run time comparison of the proposed DCS-HCL with the existing methods, ENCC [1] and integrated anonymization and reconstruction [2] using 10 different values of ‘ $P_i$ ’. The rise in ‘ $P_i$ ’ value causes an increase in the run time for all the three methods due to the increase in the records and their corresponding similar quasi-identifiers. The proposed method run time values are lesser than existing methods [1] and [2] in most cases because the proposed method selects only the optimized identifiers as the quasi-identifiers.

TABLE I. ANALYSIS RESULTS OF RUNTIME USING DCS-HCL, ENCC [1] AND INTEGRATED ANONYMIZATION AND RECONSTRUCTION [2]

Number of patients	Run time (ms)		
	DCS-HCL	ENCC	Integrated anonymization and reconstruction
500	42.5	57.5	72.5
1000	75.35	105.35	125.35
1500	90.25	125.45	140.55
2000	105.35	140.55	175.55
2500	125.45	195.35	225.35
3000	140.55	215.25	255.85
3500	175.35	225.35	315.55
4000	190.15	240.55	335.25
4500	200.35	280.15	350.55
5000	225.55	315.55	385.55

Fig. 4 given shows the run time values of the proposed DCS-HCL method and its comparison with the existing two methods [1] and [2] on Diabetes 130-US hospitals dataset. From the figure, it is inferred that the run time linearly increases with the increase in number of patients during privacy preservation. With the simulation conducted for ‘500’ numbers of patients for preserving the privacy of big healthcare data using quasi identifiers, the run time involved for preserving single patient is ‘0.085ms’ by DI-CSH model. The overall run time for ‘500’ patients was found to be ‘42.5ms’, ‘57.5ms’ and ‘72.5ms’ using DCS-HCL, [1] and [2] respectively. From the results, the run time using DCS-HCL is comparatively lesser than [1] and [2]. The reason behind the improvement is the application of Distinctive Impact Context Sensitive Hashing (DI-CSH) model. By applying this model, the base essential quasi attributes are identified by mapping the similar QI-classes hash function when compared to the arbitrarily mapped QI-classes. With this, the run time involved in preserving the privacy of big healthcare data using DCS-HCL is comparatively lesser than 28% compared to [1] and 42% compared to the [2], respectively.

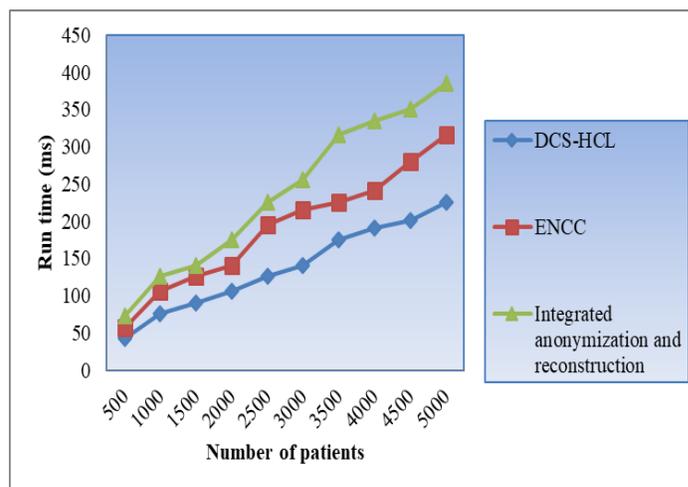


Fig. 4. Graphical Representation of Run Time.

**B. Performance Measure of Accuracy**

Secondly, the performance analysis of accuracy is investigated. Furthermore, the results were performed to compare the accuracy of the proposed DCS-HCL with two existing methods, ENCC [1] and integrated anonymization and reconstruction [2] using 10 different values of ‘ $P_i$ ’. Accuracy results are shown in Table II. From the results, it is clear that as ‘ $P_i$ ’ value is increased, the accuracy values of all the three methods decreased. The proposed method yields higher accuracy when compared to the existing privacy preservation methods in most cases by controlling the information loss via distance quantification. In contrast, the existing privacy preservation methods not apply the concept of distance quantification to control the information loss and attain relatively lesser accuracy.

TABLE II. ANALYSIS RESULTS OF ACCURACY USING DCS-HCL, ENCC [1] AND INTEGRATED ANONYMIZATION AND RECONSTRUCTION [2]

Number of patients	Accuracy (%)		
	DCS-HCL	ENCC	Integrated anonymization and reconstruction
500	97	95	92
1000	96.35	92.15	90.25
1500	96.15	90.55	88.35
2000	96	88.35	86.15
2500	95	86.25	84.35
3000	94.35	85.15	82.15
3500	94.15	84.35	80
4000	94	82.15	78.85
4500	93.25	81.55	75.35
5000	92	80	75

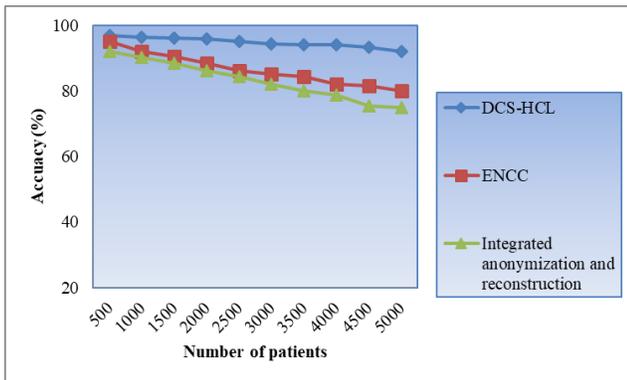


Fig. 5. Graphical Representation of Accuracy.

Fig. 5 illustrated above shows the average accuracy values obtained using three different methods, DCS-HCL, [1] and [2]. It is observed that, rise in the number of patient causes decrease in the accuracy due to less modification in the QI original values. The rationale regarding better accuracy of the proposed method compared to the existing methods [1] and [2] is derived from the fact that minimum distance consistency is maintained in the quasi-identification process. With ‘500’ number of patients considered for simulation to evaluate the privacy preservation of big healthcare data and ‘485’ number

of patients data accurately preserved, the overall accuracy using DCS-HCL was found to be ‘97%’, ‘95%’ using [1] and ‘92%’ using [2]. This is because of applying Hellinger Convolutional Neural Privacy Preservation algorithm in proposed model. A maxmin principle is applied for unstructured data. With this objective, an activation function is derived by hashing QI-classes. Hellinger distance maximizes the accuracy involved in preserving the privacy. In this manner, the accuracy of privacy being preserved for big healthcare data is said to be improved using DCS-HCL by 10% compared to [1] and 14% compared to [2], respectively.

**C. Performance Measure of Information Loss**

Finally, the information loss involved is presented in this section. To further demonstrate the effectiveness of the proposed method, information loss values have been measured and compared with the result of the two existing privacy preservation methods [1] and [2]. Results are shown in Table III. The proposed DCS-HCL method has produced lesser information loss value than other privacy preservation methods, [1] and [2]. The proposed method applies the concept of Hellinger Distance in privacy preservation process and maintains the QI’s values consistency resulting in higher data utility to reduce information loss.

TABLE III. ANALYSIS RESULTS OF INFORMATION LOSS USING DCS-HCL, ENCC [1] AND INTEGRATED ANONYMIZATION AND RECONSTRUCTION [2]

Number of patients	Information loss (%)		
	DCS-HCL	ENCC	Integrated anonymization and reconstruction
500	3	5	8
1000	3.5	6.25	9.35
1500	4	6.55	10
2000	4.25	6.85	10.55
2500	4.45	7	10.85
3000	4.85	7.25	11.35
3500	5	7.45	11.85
4000	6.35	7.85	12.45
4500	8	9	14
5000	8.15	10.15	15.35

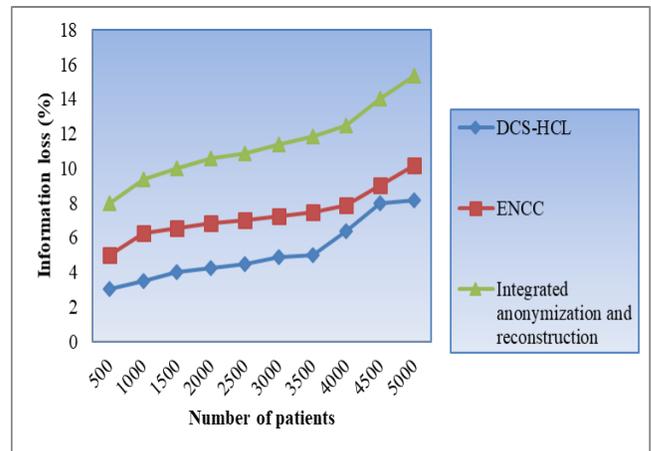


Fig. 6. Graphical Representation of Information Loss.

Fig. 6 shown above provides the graphical representation of information loss using three different methods. From the figure it is inferred that the information loss is linearly increased with the increase in the number of patients. This is owing to the fact that with the increase in the number of patients, the attributes involved in preserving the privacy also increases and obviously compromising the sensitive unstructured data. However with the simulations conducted for preserving the privacy with '500' number of patients '15' number of patients data compromised during the process and the overall information loss using DCS-HCL was observed to be '3', '5' using [1] and '8' using [2], respectively. From the results, it is inferred that the information loss using DCS-HCL is found to be comparatively lesser when compared to [1] and [2]. The improvement is due to the application of Hellinger Convolutional Neural Privacy Preservation model. Distinctive Impact cost function is used to update weight and loss for contributing to higher data utility. With this function, data utility is said to be improved and results in the minimization of information loss. The information loss using DCS-HCL is said to be reduced by 31% compared to [1] and 56% compared to the [2], respectively.

## VI. CONCLUSION

In this paper, the quasi-identifiers is used in big healthcare datasets to ensure the privacy requirements and to achieve high data utility simultaneously with minimum run time and information loss. Distinctive Impact Context Sensitive Hashing (DI-CSH) model is used for privacy preservation by extracting base essential quasi attributes. The designed model access only a part of attributes in data asset rather than access all data records as required by existing methods. To further enhance the performance of privacy preserving mechanism, Hellinger Convolutional Neural Privacy Preservation model is used to preserve the data via maxmin principle. Thus, the number of data nodes across QI-group gets reduced considerably with minimum information loss. Evaluation results with Diabetes 130-US hospitals dataset have demonstrated in DI-CSH model in terms of run time, accuracy and information loss over existing methods for privacy preservation on big healthcare data set. In future, the accuracy level can be further enhanced by using deep learning algorithms. In addition, cryptosystem can be included in order to enhance the security level during data communication in healthcare and other applications.

## REFERENCES

- [1] O. Temuujin, J. Ahn and D. Im, "Efficient L-Diversity Algorithm for Preserving Privacy of Dynamically Published Datasets," IEEE Access, vol. 7, pp. 122878-122888, September 2019.
- [2] Y. Sei, H. Okumura, T. Takenouchi and A. Ohsuga, "Anonymization of Sensitive Quasi-Identifiers for l-Diversity and t-Closeness," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 4, pp. 580- 593, August 2019.
- [3] M. Binjubeir, A. A. Ahmed, M. A. B. Ismail, A. S. Sadiq and M. K. Khan, "Comprehensive Survey on Big Data Privacy Protection," IEEE Access, vol. 8, pp. 20067- 20079, January 2020.
- [4] K. Abouelmehdi, A. B. Hessane and H. Khaloufi, "Big healthcare data: preserving security and privacy," J Big Data, Springer, vol. 5, no. 1, pp. 1-18, July 2018.
- [5] G. Kapil, A. Agrawal, A. Attaallah, A. Algarni, R. Kumar and R. A. Khan, "Attribute based honey encryption algorithm for securing big data: Hadoop distributed file system perspective," Peer J Computer Science, vol. 6, pp. 1-27, February 2020.
- [6] W. Mahanan, W. A. Chaovaitwongse and J. Natwichai, "Data anonymization: a novel optimal k-anonymity algorithm for identical generalization hierarchy data in IoT," Service Oriented Computing and Applications, Springer, vol. 14, pp. 89-100, February 2020.
- [7] P. S. Rao and S. Satyanarayana, "Privacy preserving data publishing based on sensitivity in context of Big Data using Hive," J Big Data, Springer, vol. 5, no. 20, pp. 1-20, August 2018.
- [8] P. R. M. Rao, S. M. Krishna and A. P. S. Kumar, "Privacy preservation techniques in big data analytics: a survey," J Big Data, Springer, vol. 5, no. 33, pp. 1-12, July 2018.
- [9] I. Ali, E. Khan and S. Sabir, "Privacy-preserving data aggregation in resource-constrained sensor nodes in Internet of Things: A review," Future Computing and Informatics Journal, Elsevier, vol. 3, no. 1, pp. 41-50, June 2018.
- [10] J. Wang, K. Du, X. Luo and X. Li, "Two privacy-preserving approaches for data publishing with identity reservation," Knowledge and Information Systems, Springer, vol. 60, pp.1039-1080, June 2018.
- [11] R. Khan, X. Tao, A. Anjum, H. Sajjad, S. R. Malik, A. Khan and F. Amiri, "Privacy Preserving for Multiple Sensitive Attributes against Fingerprint Correlation Attack Satisfying c-Diversity," Wireless Communications and Mobile Computing, Hindawi Publishing Cooperation, vol. 2020, pp. 1-18, January 2020.
- [12] X. Li and Z. Zhou, "A generalization model for multi-record privacy preservation," J Ambient Intell Human Comput, Springer, vol. 11, pp. 2899-2912, 2020.
- [13] C. Dhasarathan, V. Thirumal and D. Ponnuram, "A secure data privacy preservation for on-demand cloud service," Journal of King Saud University – Engineering Sciences, Elsevier, vol. 29, no. 2, pp. 144-150, April 2017.
- [14] J. W. Kim, B. Jang and H. Yoo, "Privacy-preserving aggregation of personal health data streams," PLoS ONE, vol. 13, no.11, pp. 1-15, November 2018.
- [15] J. Xu, K. Xue, S. Li, H. Tian, Ji. Hong, P. Hong and N. Yu, "Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8770 - 8781, October 2019.
- [16] K. Abouelmehdi, A. B. Hessane and H. Khaloufi, "Big healthcare data: preserving security and privacy," J Big Data, Springer, vol. 5, no. 1, pp. 1-18, February 2018.
- [17] P. Jain, M. Gyanchandani and N. Khare, "Big data privacy: a technological perspective and review," J Big Data, vol. 3, no. 25, pp.1-25, September 2016.
- [18] K. Arava, S. Lingamgunta, "Adaptive k-Anonymity Approach for Privacy Preserving in Cloud," Arab J Sci Eng, Springer, vol. 45, pp. 2425-2432, July 2019.
- [19] C. W. Soh, L. L. Njilla, K. K. Kwiat and C. A. Kamhoua, "Learning quasi-identifiers for privacy-preserving exchanges: a rough set theory approach," Granular Computing, Springer, vol. 5, pp. 71-84, August 2018.
- [20] B. Strack, J. P. D. Shazo, C. Gennings, J. L. Olmo, S. Ventura, K. J. Cios and J. N. Clore, "Impact of HbA1c Measurement on Hospital Readmission Rates: Analysis of 70,000 Clinical Database Patient Records," BioMed Research International, Hindawi Publishing Corporation, vol. 2014, pp. 1-11, April 2014.

# Big Data Analytics Framework for Childhood Infectious Disease Surveillance and Response System using Modified MapReduce Algorithm

## A Case Study of Tanzania

Mr. Mdoe Mwamnyange<sup>1</sup>, Dr. Edith Luhanga<sup>2</sup>, Mr. Sanket R. Thodge<sup>3</sup>

School of Computation and Communication Science and Engineering (CoCSE)<sup>1, 2</sup>

The Nelson Mandela African Institution of Science and Technology (NM-AIST) Arusha, Tanzania<sup>1, 2</sup>

Pi R Square Digital Solutions Pvt Ltd, S B Road, Gokhale Nagar, Pune, India<sup>3</sup>

**Abstract**—Tanzania, like most East African countries, faces a great burden from the spread of preventable infectious childhood diseases. Diarrhea, acute respiratory infections (ARI), pneumonia, malnutrition, hepatitis, and measles are responsible for the majority of deaths amongst children aged 0-5 years. Infectious disease surveillance and response is the foundation of public healthcare practices, and it is increasingly being undertaken using information technology. Tanzania however, due to challenges in information technology infrastructure and public health resources, still relies on paper-based disease surveillance. Thus, only traditional clinical patient data is used. Nontraditional and pre-diagnostic infectious disease report case data are excluded. In this paper, the development of the Big Data Analytics Framework for Childhood Infectious Disease Surveillance and Response System is presented. The framework was designed to guide healthcare professionals to track, monitor, and analyze infectious disease report cases from sources such as social media for prevention and control of infectious diseases affecting children. The proposed framework was validated through use-cases scenario and performance-based comparison.

**Keywords**—Big data analytics; childhood infectious diseases; infectious disease surveillance system; infectious disease report cases; framework; Hadoop; healthcare big data; map reduce

### I. INTRODUCTION

In 2018, there were 5.3 million deaths of children under the age of 5 years around the world (World Health Organization report, 2020, Oct. 15) with most of the deaths taking place in the African region. Data from UNICEF, WHO, World Bank, and UN-DESA Population Division (2019, Oct. 18), show that almost half of these deaths (18 of every 1,000 births globally) occurs within the first 28 days of life. The probability of death lowers to 11 per 1,000 births between the ages of 1 month to 1 year and 10 per 1,000 births between the ages of 1 and 5. The main causes of mortality are malnutrition and preventable, childhood diseases including diarrhea, pneumonia, and malaria. Malaria, pneumonia, and diarrhea are the main causes of the majority of child deaths in Tanzania [1].

The United Nations Sustainable Development Goal no. 3 has set a childhood mortality rate of 25 deaths per 1,000 births as the target. A wide range of solutions to achieve this goal

have been implemented across Sub-Saharan Africa (SSA). The solutions include: providing affordable maternal health care services and improved access to drinking water and sanitation services [2], providing broad-spectrum antibiotics, such as azithromycin to children [3], and effective coverage of available cost-effective interventions and technologies [4]. A strong functional infectious disease surveillance system has also been highlighted as a significant tool to provide healthcare information to support public health decision-making worldwide (WHO 2000). According to WHO, a disease surveillance system “is the continuous, systematic collection, analysis and interpretation of healthcare-related data needed for the planning, implementation, and evaluation of public health practices”. It serves as an early warning and alert system for unforeseen public health emergencies, supports medical practitioners to prepare infectious disease spread report cases for intervention, track disease spread advancement, and provides crucial information to the epidemiologist, policy, and decision-makers.

In 1998, the United Republic of Tanzania adopted an Integrated Disease Surveillance and Response Program (IDSR) for all disease surveillance activities in the country [5]. Thirty-four (34) notifiable diseases were included in the guidelines, as well as procedures for disease case detail, reporting, and actions to be taken for public health service levels to achieve timely infectious disease detection, investigation, and response to disease outbreaks. The IDSR has been facilitated with the nationwide implementation and functioning of the Health Management Information System (HMIS) and District Health Information System (DHIS2) systems. However, there was still weakness in data coverage and completeness, as not all infectious diseases were accommodated for surveillance, healthcare data from the laboratory were not linked with the IDSR system, and data on cases shared via the internet, web-based system, and short text message system (SMS) were not accommodated, even though no-care or home-care was sometimes practiced [6].

Due to the challenges of emerging and reemerging infectious diseases in the world [7], it has become very difficult for the existing IDSR system to detect and analyze small to medium size outbreaks of infectious diseases. As a result, these outbreaks remained hidden and distributed

unnoticed over a wide local geographic area because of the growing local food processing technologies in the country. The emergence of the novel coronavirus (Covid-19) in 2020 in the world and the continued reemergence of cholera, dengue, and other infectious diseases in Tanzania necessitate that such measures of engaging additional sources of healthcare data in surveillance, and the use of big data analytics processes to identify patterns, trends, and other valuable new directions on infectious disease surveillance systems are implemented. Though mining the web-based healthcare data through websites, social networks, short text messages and other online news archives using big data analytics technology provide a valuable new direction on infectious disease surveillance system [8][9], but the new technology is still unknown what are the requirements and best frameworks to be adopted for Tanzanian context. Despite the efforts to include non-clinical data in surveillance, there is no framework available to guide public health officials on which sources of data should be included, what analytics processes should be used and how the generated insights can be validated and used for decision making.

Using big data analytics technology in healthcare such as text analytics [10], data streams analytics [11], social network analytics [12] [13], machine learning techniques [14], natural language processing, data mining, and predictive analytics in healthcare [15] can effectively help to analyze diverse-mix of healthcare data from laboratory, diagnoses and medications, drug-resistance patterns, drug interactions and dosing patterns, fraud detection [16] and early warning of disease outbreaks which can boost healthcare system in Tanzania.

The purpose of this study was to identify how healthcare big data can be collected, integrated, and transformed into useful information for preoccupation healthcare planning and implementation in Tanzania, particularly for childhood infectious diseases. The requirements gathering for the big data analytics framework for childhood infectious disease surveillance and response system and validation were conducted via surveys and use-case scenarios respectively, with health facilities' IT personnel, pediatricians, and nurses from four referral hospitals in the country. We modified and existing big data for infectious disease surveillance framework to fit the identified needs and during validation, we found that the framework supported wide coverage of healthcare data collection from online data sets. It allowed transmission and processing of large-scale structured and unstructured healthcare data sets with minimal processing time, provided flexibility to write user-defined programs or run queries on top of the native program to produce the expected results and was overall well accepted by the users.

The rest of this paper is organized into the following sections: Section 2 background, Section 3 related work, Section 4 research methodology, Section 5 results, Section 6 proposed framework, Section 7 use-case diagram, Section 8 proposed system design architecture, Section 9 data flow diagram, Section 10 framework validation experiment, Section 11 validation results, Section 12 discussion and finally Section 13 conclusion.

## II. BACKGROUND

### A. Health Information and Healthcare-seeking behavior

Despite advancements in medical and increased vaccine availability to the children, emerging and re-emerging of infectious diseases continues to pose threats to parents, children, and the community at large, based on reported cases of pneumonia, malnutrition, hepatitis, malaria, and other infectious diseases. In 2019 an estimated 5.2 million children under 5 years died mostly from preventable and treatable causes in the world. Children aged 1 to 11 months accounted for 1.5 million of these deaths while children aged 1 to 4 years accounted for 1.3 million deaths of which the leading causes include pneumonia, diarrhea, and malaria. Sub-Saharan Africa remains the region with the highest under-5 mortality rate in the world with more than 80% of the 5.2 million under-five deaths in 2019 (WHO, 2019). This is the average of 1 child in 13 dying before his or her fifth birthday. In Tanzania, according to Tanzania Demographic and Health Survey (TDHS, 2010) reported that 1 out of 20 children die before their first birthday, and 1 out of 12 die before their fifth birthday. These challenges have led to the need for new approaches and technologies for infectious disease alerts, detection, and immediate response.

Also, the use of computer and internet access has been growing at a very high speed in Tanzanian with estimates of 25.7 million internet users in a population of more than 58 million till 2019 (TCRA quarterly communications statistics report, December 2019). 62% have access to mobile phones, and they use them to share information (CIA world Factbook 2019). The 2010 Tanzania Communications Regulatory Authority (TCRA) report [17] has also proved that the number of internet users has been growing at an average rate of 24% per annum from 2005 to 2010. This means that there is also an increased frequency of using internet-based technologies to acquire health and disease information among parents and members of the community. Members of the community have experienced plenty of useful healthcare information available from the mass media. The sources of information involve radio, television, mobile phones, social media, and health websites in which health free-text data and audio of disease causes, diagnosis, prevention, and control are needed.

Socio-demographic characters, possession of health insurance, exposure to mass media (internet, radio, television) have changed the traditional healthcare-seeking behavior characters of relying on health facilities in Tanzania [18]. Exposure to mass media was found to be statistically and significantly associated with appropriate healthcare-seeking behavior change. The influence of seeking appropriate healthcare information such as disease causes, diagnosis, treatment, prevention, and control has changed the healthcare-seeking behavior among parents and members of the community to seek appropriate health information anywhere from the mass media. Some research studies have shown that using mass media (including radio, television, mobile phones, social media, and health websites) has a positive impact on health facility deliveries [19].

### B. Big Data Analytics in Healthcare

Big data in the healthcare system is the collection and processing of a multi-diverse mix of healthcare data sets such as structured, semi-structured, and unstructured data which make complicated data mining processes in the traditional system [20]. In big data analytics phenomena in healthcare, data comes from various data sources such as local information news, structured and unstructured data, laboratory test information, radiology images, healthcare website reports, click streaming, Twitter feeds, e-mails, call detail reports, video camera, social network data, weblog files, smartphones mobile apps, audio, healthcare equipment sensors, and others. The data if properly analyzed can greatly aid in evidence-based decision-making on childhood infectious disease management and decision-making. These types of data cannot be processed and stored in a traditional database as they belong to different formats of data sets. The data typically cannot be analyzed with traditional Structured Query Language (SQL) tools such as HIMS. Instead, new non-relational database technology such as Hadoop, MapReduce algorithm, and NoSQL database tools are needed [21]. The high-speed performance, multiprocessing, concurrency, per server throughput, and parallelism processing clusters technologies are the essential requirements on highly scalable healthcare big data analytics [22].

The advantage of using big data analytics technology on infectious disease detection and control is to use e-mail and online free-text health data from the internet to disseminate information of infectious disease outbreaks by e-mailing and posting infectious disease case reports. It can help to conduct disease mapping surveillance by continuously gather and display public health data about new infectious disease outbreak using internet-based data sources such as online news, websites, RSS feeds, expert opinion, and official alerts based on geographical location, time, and disease agent which cannot be supported with the traditional system.

### III. RELATED WORK

Many research studies to supplement existing traditional systems and design new models to detect infectious diseases using big data analytics such as social network and internet search queries to gather and process data at a speed that is close to real-time have been conducted in many countries. The following are some related works extracted from the literature review studied on this research:

#### A. Big Data Analytics using Online Information Aggregates Search Engines

Google Flu Trends Healthcare Big Data Analytics; this service was conducted by Google to predict and locates flu infectious disease outbreaks by making use of online information aggregates search queries.

The San Francisco-Based Global Viral Forecasting Initiative (GVFI) has been used advanced big data analytics on information mined from the internet to identify locations, sources, and drivers of local infectious disease outbreaks before they become global epidemic [23].

Ginsburg et al. [24], also developed a method to collect and analyze healthcare big data through search queries from Google (<http://www.google.com/>) to track Influenza-Like Illness (ILI) within a given population. They conducted their research on Google search queries taken from historical logs during 5 years (2003 up to 2008) using 50million of the most popular searches.

#### B. Big Data Analytics using Social Networks

A. Signorini, A. M. Segre, and P. M. Polgreen [25] employed big data analytics technology on social media using Twitter post data across the United States by searching through particular areas and analyzing the data to predicate weekly Influenza-Like Illness (ILI) levels. The focus of their efforts was on the period when the H1N1 epidemic was happening in the United States. The overall aim was to examine the use of information about news and geopolitical events embedded in Twitter to track rapidly-evolving public sentiment concerning H1N1 and measure actual disease activity to monitor the seasonal influenza-related traffic within the United States.

They gathered data set consisted of 4,199,166 tweets selected from the roughly 8 million influenza-related tweets (i.e., keywords h1n1, swine, flu, or influenza) observed between October 1, 2009, up to May 20, 2010, using Twitter's streaming application programmer's interface (API). The tweets were sifted through looking for posts containing a preset of keywords correlated to H1N1 (h1n1, flu, swine, influenza). They trained 32 times on each 31-week subset of the training data. The estimates of the prediction model for national ILI values produced by the system were fairly accurate, with an average error of 0.28% and a standard deviation of 0.23%.

H. Achrekar, A. Gandhe, R. Lazarus, S. Yu, and B. Liu [26]. Used big data analytics technology by developed a system deemed Social Network Enabled Flu Trends (SNEFT) which continuously monitored tweets to detect and track the spread of ILI epidemics. The study used a data set of tweets and profile details of the Twitter users who commented on flu keywords started on October 18, 2009. They used an OSN crawler that searched online social networks they developed to retrieve tweets from the internet using keywords flu, H1N1, and swine flu.

Yuan et al. [27] also developed a system to collect and analyze the big data of healthcare using search query data. The study used search queries gathered from Baidu ([baidu.com](http://index.baidu.com/)) to track ILI epidemics across China. The author gathered their data from Baidu's database (<http://index.baidu.com/>) which stored the online search query since June 2006. For this study, they only gathered data from March 2009 to August 2012, which was during the Influenza virus (H1N1) epidemic, and compare their results to that of China's Ministry of Health (MOH). Yuan et al.'s system was split into four main parts: (a) choosing keywords, (b) filtering these keywords, (c) defining weights and composite search index, and (d) fitting the regression model with the keyword index to that of the influenza case data.

Ashish Naveen, B. Antarip, D. Sumit, N. Saurav, and P. Rajiv[28], created an online big data analytics platform called Abzooba Smart Health Informatics Program (SHIP). Their purpose was to help patients connect to the medical experiences of other patients posted throughout the internet via online discussion message boards. They used a pool of 50,000 discussion messages including posts extracted from websites such as inspire.com, medhelp.com, and others to extract and execute big data text processing to extract information of each entry including posts and replies which have medical significance related to health such as treatments, side effects, medicines, etc.

### C. Big Data Analytics for Healthcare in Africa

Although the application of big data analytics in healthcare is still in its infancy stages in Africa compared to the developed nations, some evidence proved that big data analytics is emerging in Africa particularly in Sub-Saharan Africa, and has shown the potential to improve the public health system. The emergency use of the internet, web-based systems, social networks (Baidu, Instagram, WhatsApp, Twitter, and Facebook, etc.), and other mobile devices in Africa is making a foundation source of big data which can help to improve infectious disease surveillance. Through the preliminary evidence of an emerging technology few research studies have been made by researchers to practically demonstrate the usefulness of using big data analytics in public health for the African continent using mobile phones and social networks.

The first example of the use of big data analytics for infectious disease management in Africa was the use of mobile phones in connection with the HealthMap online system in 2014 for detecting the Ebola virus epidemic in Guinea, Liberia, Nigeria, and Sierra Leone in western Africa. The system used emails, RSS feeds, text, and online free-text data on its surveillance.

Wesolowski et al., 2012 [29] used mobile phones to monitor the movement of malaria parasites by analyzing call and text data of mobile phone subscribers of about 15 million people of Kenya. They estimated 14,816,521 Kenyan mobile phone subscribers between June 2008 and June 2009, through mapping every call and text made by each individual to one of 11,920 cell towers located within the boundaries of 692 settlements. The aim was to identify the dynamics of human carriers that drive parasite importation between regions and mapping the routes of parasite dispersal by human carriers in Kenya. The result of this analysis was compared with the hospital records to detect malaria transmission in the local geographical areas in Kenya. This research study assisted the Kenyan government to develop an effective malaria control program. The strength of this study was the ability of the system to pool huge amounts of data from the mobile phone subscribers to track the movement of people. However, the limitation of this system was also the inability to combine structured and unstructured data for sophisticated healthcare data analysis.

The use of internet-based and mobile phone technology systems for disease surveillance in the world has quickly become controlling sources of information on emerging

infectious disease surveillance, however, their impacts on public health dynamics remain undetermined. Lack of authenticity, false reports, and information overload restrict the cognizance of their potential for public health practices. In Tanzania, the appropriate usage of big data analytics technologies for infectious disease surveillance is still unknown. The issues on how nontraditional healthcare data can be incorporated with the traditional health data, what are the sources and limitations of the available unstructured infectious disease report cases data, how the online healthcare data can be extracted and transformed into useful information, unaffordable high-performance computing infrastructures for big data analytics are still the challenges. This work aims to address this gap, with a focus on the development of a childhood infectious disease surveillance system.

## IV. RESEARCH METHODOLOGY

### A. Study Area

This study was conducted in four regions in Tanzania, Dar es Salaam, Arusha, Kilimanjaro and Mbeya. Six regional referral hospitals were included, namely Amana, Temeke, and Mwananyamala referral hospitals in Dar es Salaam, Mount Meru hospital in Arusha, Mawenzi hospital in Kilimanjaro, and Mbeya referral hospital in Mbeya. The hospitals were purposively selected since they are responsible for coordinating surveillance activities and mobilizing resources and providing technical support for the surveillance activities conducted at lower levels.

### B. Participants

A total of 110 participants took part. Forty-nine (49.09%) were pediatricians, thirty-two (32.73 %) were medical records officers and eighteen (18.18%) were IT healthcare professionals in the hospitals. The heads of departments from the hospitals were asked to propose people who met the following criteria: (i) able to read and write in English (since the questionnaire was in English) (ii) have 3+ years' experience particularly in infectious disease data collection and analysis. The heads were also asked to ensure gender balancing in their list of proposed participants.

### C. Data Collection

Data collection was conducted between February and May 2019. Surveys, interviews, and observation were used to:

- 1) Identify challenges facing healthcare professionals from infectious diseases prevention and control perspective.
- 2) Identify healthcare information gaining mechanisms and decision-making information gaps and.
- 3) Identify healthcare system opportunities for future infectious disease prevention and detection.

The questionnaires developed asked questions on: major challenges on infectious diseases prevention and control; Infectious disease data collection and analysis; Involvement of citizens/ public to collect and analyze infectious diseases; Organization experience in healthcare big data and data-driven innovation; and the use of healthcare big data technology in the healthcare system, among others. There were a total of 31 questions, with 28 requiring responses on a 5-point Agreement

Likert scale (1 = strongly disagree, 2 = disagree, 3 = neither agree nor disagree, 4 = agree and 5 = strongly agree).

The interview was used to gain further insights into the infectious disease surveillance process and its successes, challenges, and the solutions they used to overcome the challenges particularly on collecting and analyzing unstructured data. The data were also recorded and analyzed using the descriptive statistics method.

#### D. Data Analysis

A total of 108 questionnaire sheets that qualified for data analysis were returned and analyzed. Descriptive statistics were used to analyze the survey responses. Free-text responses were inductively coded and the frequencies of each theme were calculated.

The analysis of the questionnaire was performed based on the indicated themes. The major challenges that the healthcare professionals experience in their day to day performance were measured by seven questions (inadequate of the infrastructure /facilities; access and quality of the healthcare centers' services; difficulties to reach remote areas; inability to collect infectious disease data from the patient's environments; poor quality of food, water, and housing services; people's culture; and shortage of the number of healthcare staff).

The theme of data collection and involvement of citizens was also measured to assess if the traditional system can integrate healthcare data from other healthcare-related systems such as healthcare websites, social media, mobile phones, and public pharmacies to improve cross-functional communication and collaboration among healthcare systems.

### V. RESULTS

The results in this study show that in the traditional system, three of the six hospitals (Mwananyamala, Mawenzi, and Mbeya) only clinical data were used for surveillance. The other three hospitals (Ilala, Temeke, and Mount Meru) relied on clinical data and other healthcare data sources including community case findings as well.

The results of the questions v/s responses in histogram chart:

However, the following results were obtained based on the analysis of the individual cases:

#### A. Sources of Non-clinical Data for Surveillance

The results in questions 1-7 confirmed that the healthcare professionals have greater challenges collecting data of infectious disease report cases from the patients' environments as indicated in question 5. Over 70% (n=78) of the responses strongly agreed that inability to collect data from the patient's environment and involvement of citizens hampered surveillance and response as indicated on the histogram chart in Fig. 1. Data collection from other sources including free-text from mobile phones, social networks like WhatsApp, Facebook, Twitter, and email system would improve infectious disease surveillance systems.

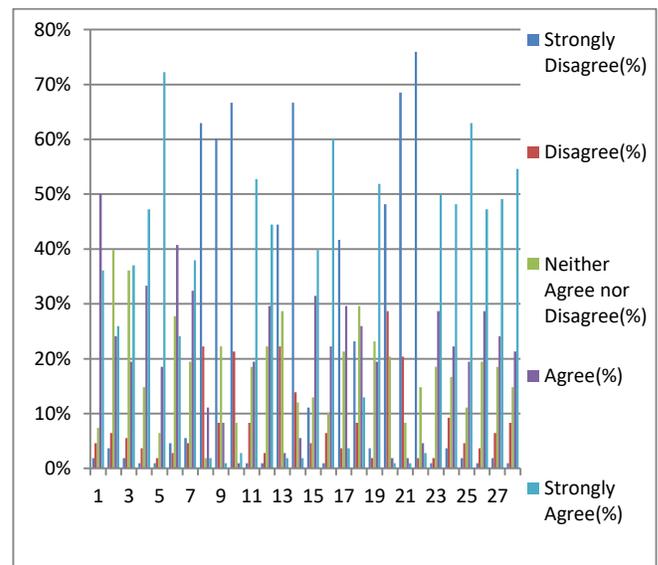


Fig. 1. Histogram Chart of the Questions v/s Response Percentages from the Respondents.

#### B. Experience in Healthcare Big Data and Data-driven Innovation

The results confirmed that 70(65%), out of 108 respondents strongly agreed that they do not have experience in healthcare big data and data-driven innovation. Also, they agreed that they do not have a healthcare big data framework for collecting, analyzing, and transforming very large infectious disease report cases data sets as indicated in questions 17-21 in Fig. 1. In this group of respondents 33(30%) were pediatricians, 21(20%) medical records and 16(15%) were IT professionals.

#### C. Current and Proposed Health Data Sources

Over 75% (n=81) of the 108 respondents strongly agreed that the collection and analysis of infectious disease report cases from other sources using multiple channels such as mobile phones, websites, e-mails, social media, and content management systems would improve the traditional surveillance system as indicated in question 22 in Fig. 1. 86(80%) of 108 respondents chosen mobile phone short-text messages as a good source of information. 54(50%) of 108 respondents selected web-based free-text information as the source of health data and 97(90%) of 108 respondents opted for social media free-text application as the good source of health data.

### VI. PROPOSED BIG DATA ANALYTICS FRAMEWORK

The big data analytics framework for the healthcare system developed by [30] was considered as a reference for the development of this framework. This dynamic framework has been considered as a healthcare big data framework base for the general healthcare system which can support tracking and monitoring infectious disease. It has incorporated the general known healthcare big data analytics approach based on the fundamental variables. This is inefficient to be adopted for the process of collection and analyzing the healthcare big data in Tanzania environment.

In this study, the author developed a framework that serves as a reference model to make healthcare professionals in Tanzania ready to explore and implement big data analytics technology in the healthcare system. The data collected for this study could only relate to the short time validation of this framework. The findings are limited based on the local scale of the use-cases scenarios phenomenon. Further research and update are needed throughout the framework studies. The resulting big data analytics framework which was proposed to be suitable for the Tanzania context was shown in Fig. 2.

The proposed framework was divided into the following layers: (a) data capture layer (b) data acquisition layer (c) data analytics layer and (d) information exploration.

#### A. Data Capture Layer

The data capture layer involves all traditional and non-traditional data sources necessary to provide insights on early infectious disease prevention and control. It involves structured data from HIMS/DHIS-2, Health Insurance, medical healthcare sensors system, online structured healthcare information archives, home patient monitoring sensors, and public pharmacy. These clinical data can be collected from various sources through tables, csv files, json data files, and text file format and stored in the relational databases depending on the content format such as MySQL, Oracle, PostgreSQL, and others. Since unstructured data cannot be processed using structured databases [31], then data will be stored in the nontraditional databases which can handle unstructured data such as MongoDB Databases.

#### B. Data Acquisition Layer

The data acquisition layer is responsible for handling data that comes from various healthcare data sources. In this layer, healthcare data stored in the various structured databases such as tables and csv files and unstructured databases such as free-text, json data, video, and audio format can be transformed into Hadoop Distributed File System (HDFS) format ready to be processed in big data analytics tools. Since the incoming data comes from various data sources, their characteristics are varying in terms of a communication channel, frequency, size, volume, and file format. Therefore, the transformation engine must be able to extract, merge and transform data into key-value pairs.

In this layer, the transformation engine must be able to support functions such as data transfer, cleaning, splitting, sorting, merging, and validating data. For instance, structured healthcare data sets records such as (patient name, age, address, location, and disease descriptions or medical history) can be extracted and transformed into key-value pairs of the HDFS format. This process can also be done in unstructured data whereby data in the format of e-mail, weblogs, or text can be extracted and transformed into key-value pairs as well.

#### C. Data Analytics Layer

In this layer, data can be processed and analyzed in three ways: Hadoop MapReduce data processing, data streaming, and in-database analytics.

MapReduce data processing works by breaking data processing into two phases: Map phase and Reduce phase. Each phase contains key-value pairs as input and output. The input to our Map phase is the raw or unstructured data, which is processed by split up into key-value pairs. And the output from the *Map function* is processed by the MapReduce framework before being sent to the *Reduce function*. MapReduce processing in big data analytics provides the ability to process a large volume of structured and unstructured healthcare data in batch processing and massively parallel processing [32].

Data streaming processing can help to process and analyze real-time and near real-time stream data processing. In real-time stream data processing, healthcare professionals can track healthcare data-in-motion such as rates of infectious disease spread, prediction of infectious disease outbreaks, respond to unexpected infectious disease outbreak and quickly make an evidence-based decision for early infectious disease notification, prevention, and control.

In this layer, the healthcare data analytics such as healthcare revenue cycle, healthcare supply chain, disease management, disease case-specific management, healthcare cost and quality management, and operational efficiency can be analyzed. The proposed framework can help to conduct these analyses using various big data analytics techniques. For example: in the healthcare revenue cycle, we can use the framework to conduct analytics through collect, compile and analyze health data from various healthcare centers reported on a monthly, quarterly and annual basis to enable healthcare professionals and the community to gain insight into the national average and top quartile of the revenue cycle. This can be done in a framework through developing a modified MapReduce algorithm that can be able to map and reduce health data accordingly based on the modified principles of the MapReduce algorithm.

#### D. Information Exploration Layer

The information exploration layer provides output results based on visualization reports, real-time information monitoring, and other useful healthcare business insights reports. Some information and visualization reports which were felt important were healthcare revenue cycle, healthcare supply chain, healthcare information technology, healthcare cost, and quality and operational efficiency. Because it will help to provide healthcare executives and leadership teams with objective, actionable best practice research and implementation resources. It will help healthcare professionals to make early evidence decisions such as infectious disease alerts, warnings, and notifications to the citizens before an infectious disease outbreak.

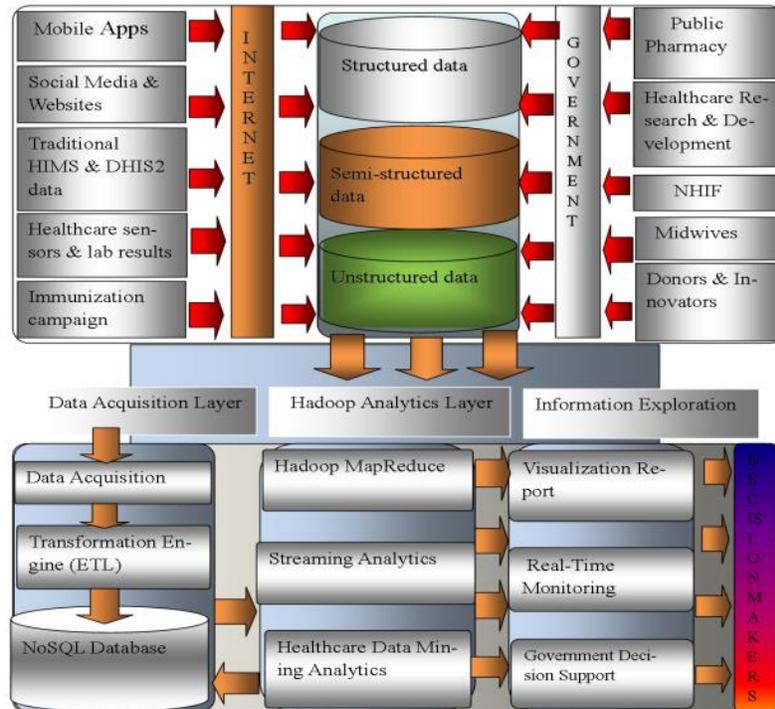


Fig. 2. Proposed Big Data Analytics Framework.

## VII. FRAMEWORK MODEL USE CASE DIAGRAM

The framework model use case diagram in Fig. 3 is a simple representation of user interaction which provides a simplified real picture to the stakeholders of how the framework can be implemented in the real world as presented in the proposed system design architecture in Fig. 4. Based on the use case diagram, we can divide the diagram into four areas: (a) Healthcare big data sources (b) Data ingestion zone (c) Big data analytics zone, and (d) Big Data Application zone.

### A. Healthcare Big Data Sources

Healthcare big data sources involve roles of data collection from the various healthcare data sources. It involves the collection of infectious disease data from patients using various tools including mobile-apps, web-based systems, social media, content management systems, clickstreams, weblogs, and online archives. The traditional system already has dynamic categories of healthcare provider users who collect infectious disease data using HIMS/DHIS-2, Infectious Disease Week Ending System (IDWE), and the community healthcare activists who collect and submit data to the hospitals. These categories of users will be improved by assigned activities of collecting infectious disease data using digitized data through mobile applications and web-based systems instead of the existing manual paper-based system. Initially, doctors, IT personnel, laboratory scientists and medical records personnel can help to collect other data of infectious disease from pharmacies, social media, clickstreams, weblogs, and online archives through healthcare

websites, mobile applications, and online healthcare systems as indicated on the data flow diagram in Fig. 5.

### B. Data Ingestion Zone

Data ingestion zone involves data integration and streaming processes. IT personnel, doctors, medical records personnel, and laboratory scientists can help to conduct this process. It involves running queries and commands to extract, transform and load infectious disease data from the data sources into the Hadoop platform. Structured databases such as tables, csv files, and json data from local pharmacies, healthcare insurances, and others can be collected and integrated at this stage. The unstructured data will also be extracted and transformed before transmitted into the Hadoop Big Data analytics engine as indicated in Fig. 5.

### C. Big Data Analytics Zone

The big data analytics zone involves running healthcare data analytics. It involves executing healthcare data jobs using Hadoop MapReduce data processing, Data streaming, and In-Database Analytics. These activities can be done by the doctors, healthcare executive officers, medical officers, and medical records personnel in collaboration with the IT personnel. Structured and unstructured health data will be executed as healthcare data jobs in Hadoop Cluster using the MapReduce algorithm as indicated in Fig. 4. The real-time monitoring streaming will be monitored by the Healthcare specialist and the healthcare big data analytics visualized reports will be submitted to the decision-makers as indicated in Fig. 5.

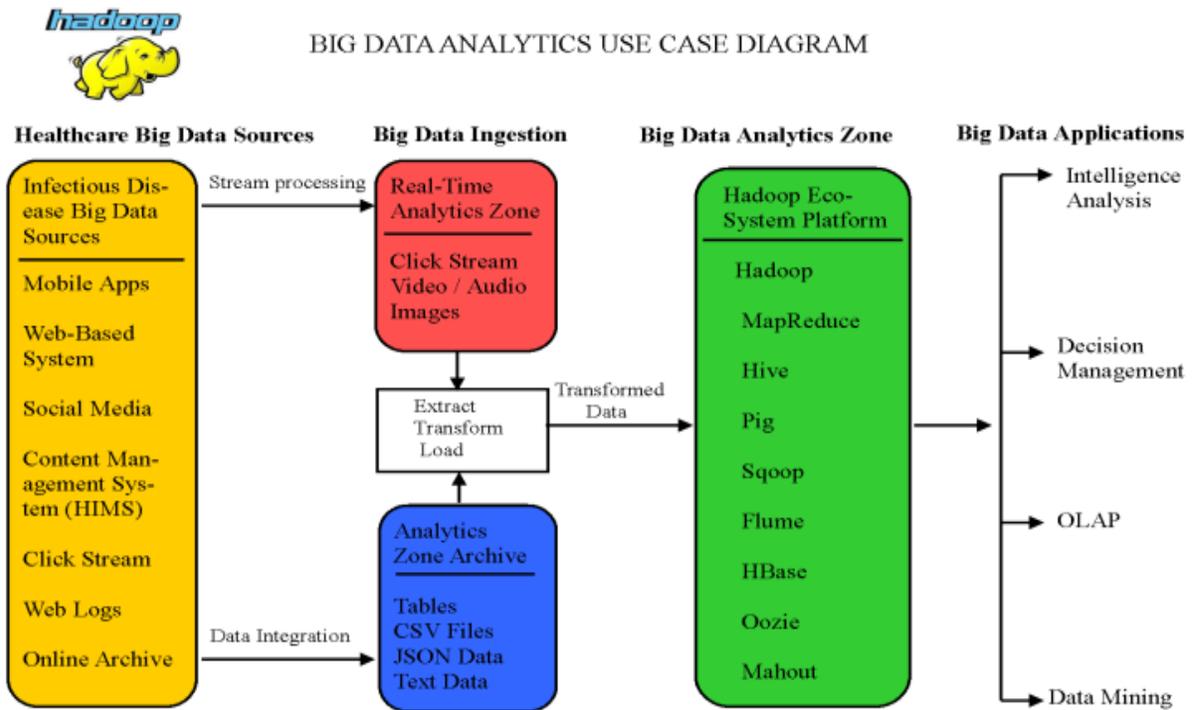


Fig. 3. Use Case Diagram for the Implementation of the Proposed Framework.

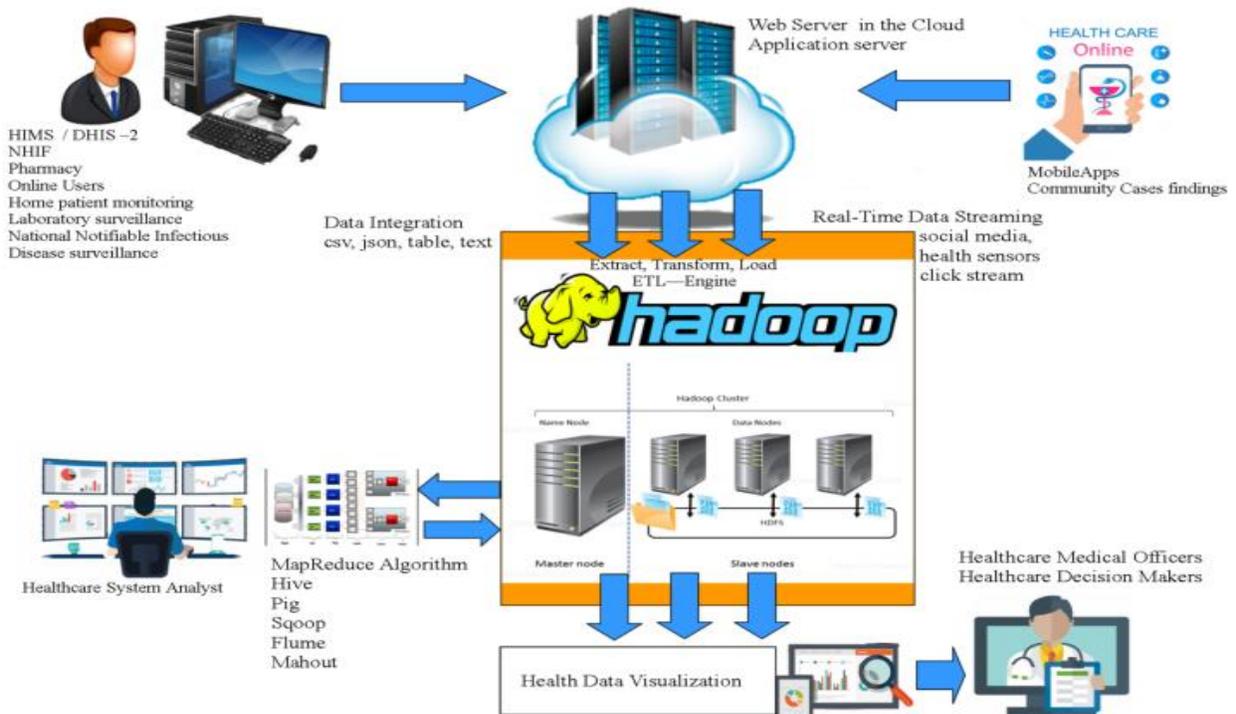


Fig. 4. Proposed Big Data Analytics Framework System Design Architecture.

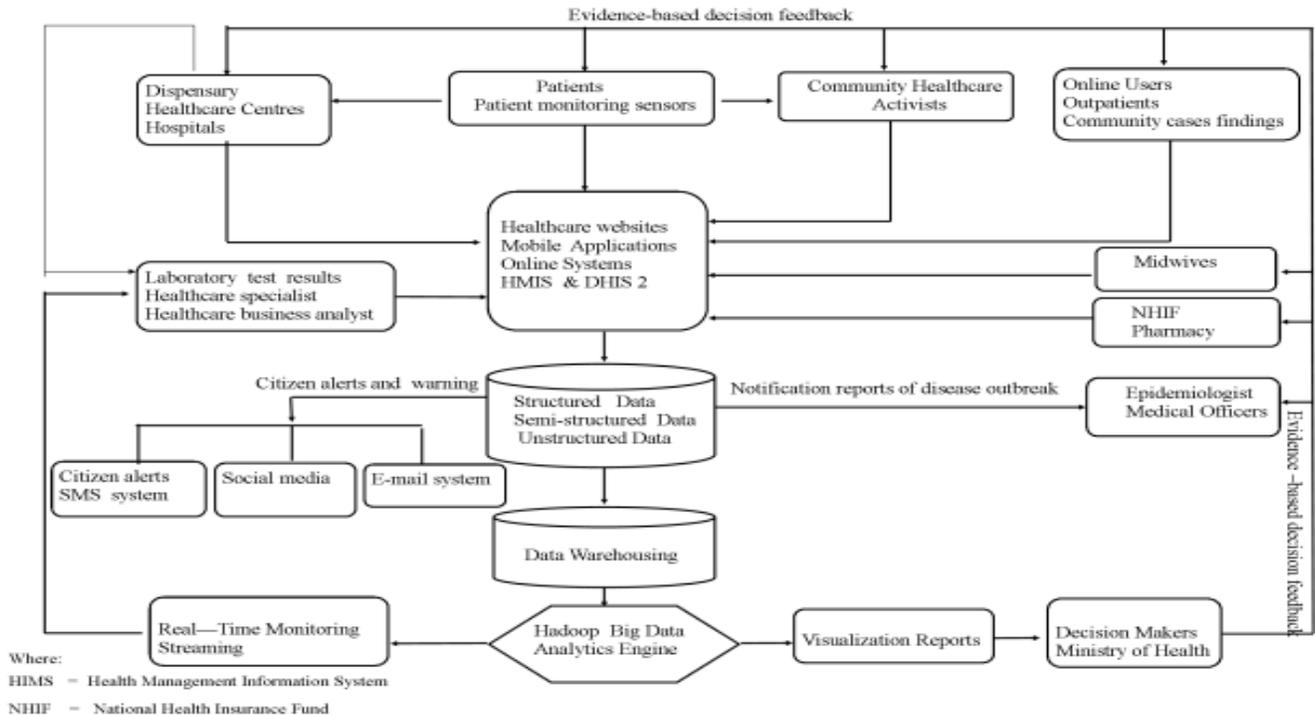


Fig. 5. Data Flow Diagram of the Proposed Big Data Analytics Framework.

#### D. Big Data Application Zone

The big data application zone involves decision-making processes based on the processed healthcare big data analytics reports. It involves healthcare master data management security and privacy, data standardization, policies, and data incorporation to create immediate, completeness, accurate evidence-based decision-making. It involves executing and managing complex analytics algorithms on data mining and intelligence analysis to manage healthcare business information. These activities can be performed by the higher authority and decision-makers in the healthcare organization

### VIII. FRAMEWORK VALIDATION EXPERIMENT

To validate the proposed big data analytics framework for usability and applicability, we conducted the following experiment using the following use-cases scenario:

#### A. Use Case-Scenario 1

Integrate healthcare data sets from various healthcare-related data sources.

During the research study, one of the great challenges facing traditional systems identified was integrating healthcare data sets from other healthcare-related data sources and analyzing them all together for evidence-based decision-making.

Currently, in the traditional system, each organization has its independent system of tracking infectious disease report cases. The hospital conducts disease surveillance using a

paper-based system, National Health Insurance Fund (NHIF) also has its way of tracking costs, local pharmacies also have their way of tracking medicines provided to the patients suffering from infectious disease symptoms. These systems cannot communicate with each other even though they dealt with the same common function of prevention and control of infectious diseases.

In this use-case scenario, we modified the MapReduce algorithm programming design model (API) to enable healthcare professionals to integrate healthcare data sets from various healthcare-related data sources. The aim was to use the framework to track patients against the repetition of drug use for the same infectious disease which in turn develop drug resistance adverse effects. This simulation can help healthcare professionals improve drug risk management and cost implication management for evidence-based decision-making.

Because of the confidentiality and integrity of health data sets, we generated healthcare data sets dummy data in json format using the online tool at [www.mockaroo.com](http://www.mockaroo.com) for the experiment:

NHIF data sets: patient\_id, patient\_name, drug\_description, amount, disease\_case\_description, and

Hospital data sets: patient\_id, first\_name, last\_name, address, gender, age, and disease\_case\_diagnosed.

The following modified MapReduce algorithm design model was developed:

## I. Modified MapReduce Algorithm Design Model:

### Reduce-side joins MapReduce algorithm design model:

**Procedure:** Reduce-Side Joins Multiple Datasets from different files

**Input:** Hospital and NHIF datasets

**Output:** Combination of Hospital and NHIF datasets

**Begin:**

**// Mapper:**

**// Task I:** Read two input files one tuple at a time

: Tokenize each word in a tuple and fetch Patient\_ID, Name, Infectious\_disease, and Amount

**//Task II:** Add tags “hosp” to indicate Hospital tuple and “nhif” for NHIF input data to produce Key-Value pairs for Mapper as:

Key-Value pair [Patient\_ID, hosp name]

Key-Value pair [Patient\_ID, nhif name]

**//Sorting and Shuffle:**

**//Task:** Aggregate the value to each Key to produce key list as {Patient\_ID1 – [(hosp name1), (nhif amount1), (nhif amount2), (nhif amount3)....]}

**//Reducer:**

**//Task I:** Process sorting output to have Patient\_ID key and list of Amount from NHIF and Hospital details.

**// Task II:** Loop the values to check if they belong to Hospital or NHIF details

**//If the value belongs to NHIF;**

1. Show infectious disease trend
2. Increase counter by 1
3. Accumulate amount spent, then
4. Get Total Amount.

**// Else,**

Store variable for future assignment;

**End Task:**

### B. Use Case Scenario II

Identify the number of notifiable infectious disease report cases at the local geographic areas from 2010 to 2019:

Another great challenge of the traditional system was to identify some historical infectious disease report cases at the local geographical areas (disease report cases counts in weekly, monthly, or yearly for many previous years) to identify trends of the disease before they developed into large massive disease outbreaks for early warning, alerts, quick response, and government intervention.

Currently, this function is done in the traditional system using a paper-based system through counting the number of infectious disease report cases from old documents (mtuha) which is very difficult when it comes to the issue of counting the number of historical infectious disease report cases involves many previous years example cases from 2010 to 2019.

In this validation, we tested the applicability of the framework using a modified MapReduce algorithm to count the number of infectious disease report cases based on local geographical areas for many previous. In this experiment, infectious disease report cases data files (2010-2019) were

generated and the following modified MapReduce algorithm design model was developed:

## II. Modified MapReduce Algorithm Design Model;

### InfectiousDiseaseReportCases WordCount algorithm design model:

**Procedure:** Count Number Of InfectiousDiseaseReportCases WordCount

**Input:** InfectiousDiseaseReportCases 2010 – 2019 datasets

**Output:** Number Of Counts of InfectiousDiseaseReportCases for Each Local Geographical Area

**Begin:**

**// Mapper:**

**// Task I:** Read ten input files one tuple at a time

: Tokenize each word in a tuple and fetch Area\_Name and Disease\_Name words that matching

**//Task II:** Splits the line into tokens separated by whitespaces and emits Key-Value pair as

Key – Value pair [Area\_ID, Area\_name

Key – Value pair [Disease\_name, DiseaseReportCase]

**//Sorting and Shuffle:**

**//Task:** Aggregate the value to each Key to produce key list as {Area\_ID1 – [(Area\_name1, Disease\_name1),DiseaseReportCase 1), (Area\_name2, Disease\_name2), DiseaseReportCase 2), (Area\_name3, Disease\_name3), DiseaseReportCase 3),.....]}]

**//Reducer:**

**//Task I:** Process sorting output to have Area\_ID, Area\_Name, Disease\_name key, and list of DiseaseReportCases from each Area\_Name

**//Task II:** Loop the values to check the Frequency for each Area\_ID, Area\_Name, Disease\_Name, key to sum up the DiseaseReportCases count

**//If there is more value of DiseaseCasesReport in one Area;**

1. Count number of DiseaseReportCases
2. Increase counter 1
3. Accumulate the number of DiseaseReportCases, then
4. Display Area\_Name, Disease\_Name, and Number of DiseaseReportCases.

**// Else,**

Store variable for future assignment;

**End Task:**

### C. Use Case Scenario III

Collecting and analyzing Infectious disease data from the online news archives.

Another great challenge of the traditional system was to collect and analyze online infectious disease data sets from online websites, social media, and online healthcare news archives. This function is currently not done in the traditional system which hinders data coverage and completeness on the evidence-based decision-making.

In this validation experiment, we tested the applicability of the framework to collect and analyze online healthcare news archives data sets. 12 text-free document files from the healthcare news archives from the internet were collected from Google scholar and Tanzania Online Daily News using WebCrawler spider developed using Python and Java

programming languages. Our goal was to use the framework to conduct healthcare information mined from the internet to identify news articles that contain medical-significance-related information on the key infectious diseases. Our keywords for distributed cache were pneumonia, hepatitis, measles, malnutrition, diarrhea, and acute respiratory infection. In our experimental studies the following modified MapReduce algorithm was set:

### III. Modified MapReduce Algorithm Design Model:

#### Distributed Cache MapReduce Algorithm:

**Procedure:** Distributed Cache MapReduce Algorithm Design

**Input:** 12 – Input files of Text documents with 1 – Keyword file datasets

**Output:** Number of Keywords matching in each text document

**Begin:**

// Mapper:

// Task I: Check the existence of both input and output parameters

: Read and write twelve input files one line at a time

: Tokenize each word in a tuple and fetch words that matching with keywords in the Cache file

//Task II: Set String Keywords in a Hash set

: Call Distributed Cache static helper and pass URI-reference in HDFS Cache file

: Set the output Key as LongWritable for the line numbers and Value as Text

: Tokenize each line by spaces, and a wordlist set used to store each distinct word we are interested in searching.

: Check if the line contains in our Keyword list

: If a match is found;

: Emit the line number it was found on as the key and the token itself as the value as Key-Value pair: [Key: Line number, token]

//Sorting and Shuffle:

//Task: Pull the complete list of cache file URIs in the distributed cache and check the URI array returned

//Task I: Loop the values to check if the URI Array passes the test.

//If the value belongs to URI Array;

1. Grab the keywords file located in HDFS
2. Write the keywords in a temporary working directory
3. Save the contents in a local file named ./keywords.txt

// Else,

Store variable for future assignment;

**End Task:**

## IX. FRAMEWORK VALIDATION RESULTS

### A. Use-Case Scenario I

In this experiment, the healthcare professionals observed that the proposed big data analytics framework system can integrate structured and unstructured data for multi-processing

in large-scale data operations to produce expected results. As indicated in this experiment, the system can integrate structured data format from multiple sources and process them to interpret the results as they wished to solve the problem of integrating and analyzing all together hospital data, health insurance, and pharmacy data as indicated in Fig. 6.

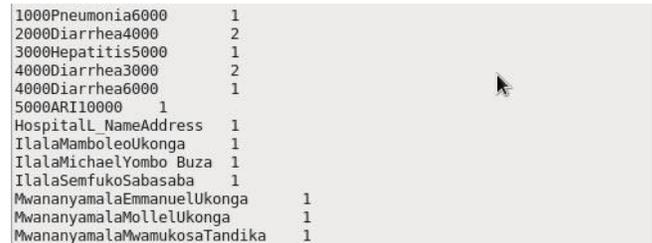
### B. Use-Case Scenario II

In this experiment, the healthcare professionals observed that the proposed big data analytics framework system can count the number of infectious disease report cases based on local geographical areas from 2010 to 2019 as indicated in Fig. 7.

This experiment proved that the proposed big data analytics framework system can count the number of infectious disease report cases in a very efficient and fastest method than the traditional system. This has been recommended by a good number of healthcare professional participants from Temeke, Ilala, Mwananyamala, and Mount Meru Referral Hospitals.

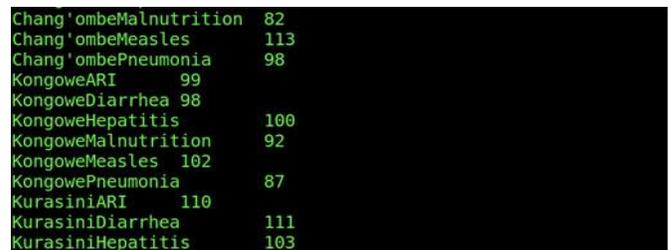
### C. Use-Case Scenario III

In this result, out of 12 collected online healthcare news archives, 8 news articles found contain significance related information on various diseases including diarrhea, malnutrition, pneumonia, measles, and hepatitis as indicated in Fig. 8.



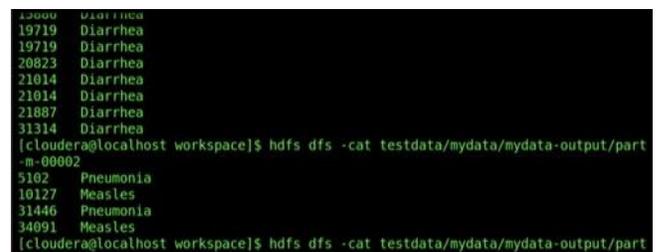
1000Pneumonia	6000	1
2000Diarrhea	4000	2
3000Hepatitis	5000	1
4000Diarrhea	3000	2
4000Diarrhea	6000	1
5000ARI	10000	1
HospitalL_NameAddress		1
IlalaMamboleoUkongu		1
IlalaMichaelYombo Buza		1
IlalaSemfukoSabasaba		1
MwananyamalaEmmanuelUkongu		1
MwananyamalaMolleUkongu		1
MwananyamalaMwamukosaTandika		1

Fig. 6. Output Results from Part-00000 file in Hadoop Cloudera Express.



Chang'ombeMalnutrition	82
Chang'ombeMeasles	113
Chang'ombePneumonia	98
KongoweARI	99
KongoweDiarrhea	98
KongoweHepatitis	100
KongoweMalnutrition	92
KongoweMeasles	102
KongowePneumonia	87
KurasiniARI	110
KurasiniDiarrhea	111
KurasiniHepatitis	103

Fig. 7. Analytic Results of the Processed MapReduce Algorithm Program.



```
13000 Diarrhea
19719 Diarrhea
19719 Diarrhea
20823 Diarrhea
21014 Diarrhea
21014 Diarrhea
21887 Diarrhea
31314 Diarrhea
[cloudera@localhost workspace]$ hdfs dfs -cat testdata/mydata/mydata-output/part-m-00002
5102 Pneumonia
10127 Measles
31446 Pneumonia
34091 Measles
[cloudera@localhost workspace]$ hdfs dfs -cat testdata/mydata/mydata-output/part
```

Fig. 8. Number of the Appearance of Keywords of the Online News Archive Files.

This experiment proved that the proposed big data analytics framework system offers more support for healthcare data processing. It offers an opportunity to collect and analyze web-based and internet healthcare data through writing user-defined programs or run queries using other languages such as Python programming language to produce the expected results from the online unstructured healthcare data sets.

## X. DISCUSSION

The big data analytics framework model for childhood infectious disease surveillance and response system has been designed for patients, community, healthcare professionals, and decision-makers to meet their specific needs to prevent and control infectious diseases affecting children 0-5 years of age in Tanzania. The framework model has been developed to overcome the following healthcare issues that prevail in the traditional system:

### A. Data Collection

The framework model has been developed to accommodate the data collection and analysis process from various healthcare stakeholders including patients through mobile apps and healthcare sensors, community through social media and websites, public pharmacies, laboratory test results, healthcare insurances, and others. The collection of web-based free-text data and mobile phone data will improve the traditional infectious disease surveillance system in Tanzania.

In data collection, the framework model can be widely implemented using a mobile application, short-text messages (sms), online healthcare system, social network, blogging, Internet protocol address, weblogs, and healthcare websites which can be integrated into the same database. This will improve the healthcare data collection process from the citizens including traditional, nontraditional, and pre-diagnostic data from community-level case findings and healthcare centers.

### B. Early Detection

Infectious diseases control measures are always done using monitoring tools that help to monitor and limiting infectious disease spread to prevent disease outbreaks by identifying and managing infectious disease report cases through early detection, notification, and warning. Through the proposed framework model, the infectious disease notification alerts including warnings, notification messages, and disease outbreaks notifications can easily be sent to the citizens and healthcare professionals through text messages, e-mail systems, and social network pop-ups for quick action as presented on the data flow diagram in Fig. 5.

### C. Healthcare Information Analysis

Having an integrated commodity computers cluster with big data analysis technology makes it easier to perform various types of data analysis in the public health sector. The use of the proposed framework in disease surveillance will help to solve technical and computational challenges that face traditional systems on the ongoing digital data revolution which requires high-performance computation system access to a high volume of stream data and the availability of high-performance computer clusters machine.

### D. Evidence-based Decision-making

Infectious disease surveillance and response system conducted in most developing countries are conducted in the condition of resource-limited settings in which often suffers from low reporting coverage, poor data quality, and completeness which in turn provide insufficient data accuracy, poor timely disease outbreak detection and lack of evidence-based decision support. Using the proposed framework model, the evidence-based decision-making process will be more accurate and relevant due to the high quality of healthcare data contents, coverage, and completeness. This will improve collaboration and coordination among healthcare professionals and other stakeholders.

## XI. CONCLUSION

The Big Data Analytics Framework for Childhood Infectious Disease Surveillance and Response System has focused mainly on the performance of the traditional system in Tanzania. Our framework is a simple data-parallel programming model enhanced with sorting, grouping, and reduction capabilities and with the ability to scale to very large volumes of healthcare data. It also works with existing SQL databases and analytics using hive tools. Its distributed implementation requires an underlying distributed file system to access input data, giving preference to local file system access and storing the output. It can be expressed as a data function from input to output framework model.

This approach can be used in similar environments worldwide, but particularly in developing countries, where many of the countries have similar conditions of not paid attention to the infectious disease data quality, coverage and representatives. Whether the infectious disease surveillance endpoint is situational awareness, disease outbreak detection, identifies estimation trends or disease-cost estimation analysis, infectious disease data quality, coverage, and completeness is the key factor during each stage. This approach can play a unique role in developing countries where dispensaries, healthcare centers, hospitals, and primary care settings are performed under limited resource settings while today's healthcare big data generation and advancement of technology realities demand integrated, relatively low-cost approaches to improve decision-making to comply with the standard of the World Health Organization and International Healthcare regulations.

This study has made the following contributions. First, we managed to propose the big data analytics framework for guidance to build a systematic infectious disease surveillance system that monitoring community case finding, online web-based and mobile phone data for infectious disease surveillance in Tanzanian. With such a framework, we can systematically collect infectious disease data from the Internet and mobile phones through web-based mapping, search engines, social networks, and local infectious disease cases, thus providing accurate and timely information to decision-makers. We believe that such a framework is very important to patients, researchers, epidemiologists, decision-makers, and other public healthcare providers.

Second, the techniques and methods used are based on big data analytics using the MapReduce algorithm which has been reported as the best performing algorithm in big data analytics. It allows distributed and parallel processing of large-scale data sets across commodity computers cluster which can easily be applied in resource-limited setting counties like Tanzania to improve high-performance computation.

The study has the following limitations which can be explored by the researchers for further studies: It is easy to imagine the potential benefits of extracting healthcare information from big data, access to such information is limited, costly, security and legal concerned and even impossible for many research societies. The online healthcare data needs to be evaluated and filtered to increase the signal-to-noise ratio for suitable healthcare data analysis. Another limitation is that most people in rural areas in Tanzania tend to lack or have limited Internet access. Online healthcare data needs web queries and search engines based surveillance. This depends on the availability of sufficient web-internet access to generate signals for data response.

#### REFERENCES

- [1] P. Sjoquist, "Tanzania," *Institutional Adjust. Econ. Growth Small Scale Ind. Econ. Transit. Asia Africa*, pp. 163–199, 2019, doi: 10.4324/9780429441561-7.
- [2] M. Acheampong, C. Ejiofor, A. Salinas-Miranda, F. M. Jaward, M. Eduful, and Q. Yu, "Bridging the under-five mortality gap for Africa in the era of sustainable development goals: An ordinary least squares (OLS) analysis," *Ann. Glob. Heal.*, vol. 84, no. 1, pp. 110–120, 2018, doi: 10.29024/aogh.9.
- [3] J. D. Keenan et al., "Azithromycin to reduce childhood mortality in sub-Saharan Africa," *N. Engl. J. Med.*, vol. 378, no. 17, pp. 1583–1592, 2018, doi: 10.1056/NEJMoa1715474.
- [4] M. C. Masanja H, De Savingy D, Smithson P, Schellenberg J, John T, "Child survival gains in Tanzania: analysis of data from demographic and health surveys," *Lancet*, vol. 371, no. table 1, pp. 1276–1283, 2008, doi: [http://dx.doi.org/10.1016/S0140-6736\(08\)60562-0](http://dx.doi.org/10.1016/S0140-6736(08)60562-0).
- [5] B. M. Nkwane, "Streamlining and strengthening the Disease Surveillance System in Tanzania: Disease Surveillance System review, asset mapping, gap analysis, and proposal of strategies for streamlining and strengthening disease surveillance," 2019.
- [6] A. M. Kanté et al., "Childhood Illness Prevalence and Health Seeking Behavior Patterns in Rural Tanzania," *BMC Public Health*, vol. 15, no. 1, pp. 1–12, 2015, doi: 10.1186/s12889-015-2264-6.
- [7] D. M. Morens and A. S. Fauci, "Emerging Infectious Diseases: Threats to Human Health and Global Stability," *PLoS Pathog.*, vol. 9, no. 7, pp. 7–9, 2013, doi: 10.1371/journal.ppat.1003467.
- [8] J. L. Hurtado, A. Agarwal, and X. Zhu, "Topic discovery and future trend forecasting for texts," *J. Big Data*, 2016, doi: 10.1186/s40537-016-0039-2.
- [9] K. Priyanka and N. Kulennavar, "A survey on big data analytics in health care," *IJCSIT, Int. J. ....*, vol. 5, no. 4, pp. 5865–5868, 2014, doi: 5: 5865-5868.
- [10] N. K. Nagwani, "Summarizing large text collection using topic modeling and clustering based on MapReduce framework," *J. Big Data*, pp. 1–18, 2015, doi: 10.1186/s40537-015-0020-5.
- [11] M. B. Chandak, "Role of big - data in classification and novel class detection in data streams," *J. Big Data*, 2016, doi: 10.1186/s40537-016-0040-9.
- [12] I. El Alaoui, Y. Gahi, R. Messoussi, Y. Chaabi, A. Todoskoff, and A. Kobi, "A novel adaptable approach for sentiment analysis on big social data," *J. Big Data*, 2018, doi: 10.1186/s40537-018-0120-0.
- [13] A. Mavragani and G. Ochoa, "Forecasting AIDS prevalence in the United States using online search traffic data," *J. Big Data*, 2018, doi: 10.1186/s40537-018-0126-7.
- [14] A. Ed and K. Maalmi, "A new Internet of Things architecture for real - time prediction of various diseases using machine learning on big data environment," *J. Big Data*, 2019, doi: 10.1186/s40537-019-0271-7.
- [15] C. Baechele and A. Agarwal, "A framework for the estimation and reduction of hospital readmission penalties using predictive analytics," *J. Big Data*, pp. 1–15, 2017, doi: 10.1186/s40537-017-0098-z.
- [16] M. Herland, T. M. Khoshgoftaar, and R. A. Bauder, "Big Data fraud detection using multiple medicare data sources," *J. Big Data*, pp. 1–21, 2018, doi: 10.1186/s40537-018-0138-3.
- [17] R. Authority, "For the year ended 30th June, 2010," 2010.
- [18] A. Nillson, "Using mass media as channel for healthcare information," pp. 1-, 2014.
- [19] J. Adinan, D. J. Damian, N. R. Mosha, I. B. Mboya, R. Mamseri, and S. E. Msuya, "Individual and contextual factors associated with appropriate healthcare seeking behavior among febrile children in Tanzania," *PLoS One*, vol. 12, no. 4, pp. 1–15, 2017, doi: 10.1371/journal.pone.0175446.
- [20] W. Raghupathi and V. Raghupathi, "Big data analytics in healthcare: promise and potential," *Heal. Inf. Sci. Syst.*, vol. 2, no. 1, p. 3, 2014, doi: 10.1186/2047-2501-2-3.
- [21] H. A. N. Hu, Y. Wen, S. Member, and T. Chua, "Toward Scalable Systems for Big Data Analytics : A Technology Tutorial," *IEEE Access*, vol. 2, pp. 652–687, 2014, doi: 10.1109/ACCESS.2014.2332453.
- [22] M. Torabzadehkashi, S. Rezaei, A. Heydarigorji, H. Bobarshad, and V. Alves, "Computational storage: an efficient and scalable platform for big data and HPC applications," *J. Big Data*, 2019, doi: 10.1186/s40537-019-0265-5.
- [23] A. K. Roy, "Impact of Big Data Analytics on Healthcare and Society *Journal of Biometrics & Biostatistics Impact of Big Data Analytics on Healthcare and Society*," no. January, 2016, doi: 10.4172/2155-6180.1000300
- [24] J. Ginsberg, M. H. Mohebbi, R. S. Patel, L. Brammer, M. S. Smolinski, and L. Brilliant, "query data," *Nature*, vol. 457, no. 7232, pp. 1012–1014, 2009, doi: 10.1038/nature07634.
- [25] A. Signorini, A. M. Segre, and P. M. Polgreen, "The use of Twitter to track levels of disease activity and public concern in the U.S. during the influenza A H1N1 pandemic," *PLoS One*, vol. 6, no. 5, 2011, doi: 10.1371/journal.pone.0019467
- [26] H. Achrekar, A. Gandhe, R. Lazarus, S. Yu, and B. Liu, "Twitter improves seasonal influenza prediction," 2003.
- [27] Q. Yuan, E. O. Nsoesie, B. Lv, G. Peng, R. Chunara, and J. S. Brownstein, "Monitoring Influenza Epidemics in China with Search Query from Baidu," vol. 8, no. 5, 2013, doi: 10.1371/journal.pone.0064323.
- [28] A. Naveen, B. Antarip, D. Sumit, N. Saurav, and P. Rajiv, "The Abzooba Smart Health Informatics Platform (SHIP) – From Patient Experiences to Big Data to Insights," *arXiv Prepr. arXiv1203.3764*, p. 3, 2012.
- [29] A. Wesolowski et al., "Quantifying the impact of human mobility on malaria," *Science (80-. )*, vol. 338, no. 6104, pp. 267–270, 2012, doi: 10.1126/science.1223467.
- [30] Y. Wang, L. A. Kung, and T. A. Byrd, "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations," *Technol. Forecast. Soc. Change*, vol. 126, pp. 3–13, 2018, doi: 10.1016/j.techfore.2015.12.019.
- [31] H. M. Al-barhamtoshi and F. Eassa, "A Data Analytic Framework for Unstructured Text A Data Analytic Framework for Unstructured Text," no. June, 2014, doi: 10.13140/2.1.4330.0485.
- [32] M. Barkhordari and M. Niamanesh, "Chabok : a Map - Reduce based method to solve data warehouse problems," *J. Big Data*, 2018, doi: 10.1186/s40537-018-0144-5.

# Recognizing Human Emotions from Eyes and Surrounding Features: A Deep Learning Approach

Md. Nymur Rahman Shuvo<sup>1\*</sup>, Shamima Akter<sup>2\*</sup>, Md. Ashiqul Islam<sup>3#</sup>  
Shazid Hasan<sup>4</sup>, Muhammad Shamsojjaman<sup>5</sup>, Tania Khatun<sup>6</sup>

Dept. of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh<sup>1,3,4,5,6</sup>  
Dept. of Bioinformatics and Computational Biology, George Mason University, Fairfax, VA-20110, USA<sup>2</sup>

**Abstract**—The need for an efficient intelligent system to detect human emotions is imperative. In this study, we proposed an automated convolutional neural network-based approach to recognize the human mental state from eyes and their surrounding features. We have applied deep convolutional neural network based Keras applications with the help of transfer learning and fine-tuning. We have worked with six universal emotions (i.e., happiness, disgust, sadness, fear, anger, and surprise) with a dataset containing 588 unique double eye images. In this study, we considered the eyes and their surrounding areas (Upper and lower eyelid, glabella, and brow) to detect the emotional state. The state and movement of the iris and pupil can vary with the various mental states. The common features found within the entire eyes during different mental states can help to capture human expression. The dataset was trained with pre-trained weights and used a confusion matrix to analyze the prediction to achieve better accuracy. The highest accuracy was achieved by DenseNet-201 is 91.78%, whereas VGG-16 and Inception-ResNet-v2 show 90.43% and 89.67%, respectively. This study will provide an insight into the current state of research to obtain better facial recognition.

**Keywords**—Human emotion recognition; convolutional neural network (CNN); transfer learning; fine-tuning; VGG-16; Inception-ResNet-V2; DenseNet-201

## I. INTRODUCTION

Facial expressions are an important nonverbal communication mediums used by humans to express their emotions [1]. In our everyday communication, the facial expression is just positioned next to the tone of the human voice. Different facial expressions are indicators of feelings and it allows a human being to express his/her current emotional state [2]. In Human Computer Interaction, it is crucial to recognize the emotional signs to recognize affective behavior [3], [4]. With the certain forms of thought and affective conducts, physical processes in the human brain changes, subsequently reflects to our eyes and surrounding areas [5], [6]. Therefore, researchers have used signals taken from human brains to understand the emotions, which correspond to the changes through upper and lower eyelid, glabella, and brow of eyes. Therefore, the eyes and surrounding areas can play a vital role in estimating the psychological state of a person. In this article, we work on diagnosing the mental state based on the visible changes in the eyes and its accessory regions to recognize human emotion.

Emotion recognition from facial expressions has incredible importance and wide applications, particularly its functions in human-machine connection frameworks [7]. Numerous studies have been performed to develop and create many facial emotion recognition systems and yet, several common problems still exist in the emotion recognition process. Two major concerns are observed; first, the features are quite sensitive to the changes in noise, illumination, and occlusion. This indicates that a slight change in noise, illumination, and occlusion may reduce the accuracy rate of the recognition process, and second, the large data dimension influences the performance of such systems [8].

The unprecedented development of deep neural networks and convolutional neural networks and the availability of required data have taken the task of classifying and recognition onto another level. Many complex tasks of recognition were thought to be challenging and show less accuracy. With the help of Convolutional Neural Networks (CNN), it becomes possible to achieve higher accuracy [9].

The eye expression could be identified by observing facial tissue signals. However, a few emotions contrast from one another in a couple of discrete facial highlights. This factor additionally relies upon a person's disparities of the subject, for example, degree, frequency, or rate of expression. Based on these, we can say that it is important to develop a facial expressions recognition system which recognizes facial expression in real-time with appropriate accuracy. The purpose of this study is to develop and study the prosperous algorithm of facial expressions recognition and emotion detection on specifically eye images of faces based on deep convolutional neural networks.

## II. RELATED WORK

Various methods for the recognition of human emotions from different facial expressions have been developed and analyzed by many researchers. In order to recognize face expressions, researchers applied methods such as Convolutional Neural Network (Deep learning-based algorithm), Viola-Jones algorithm, Haar Cascade Classifier, LBPH, K-Nearest Neighbor. Applying these algorithms, researchers showed various accuracy to predict the outcome and established the improved model which fits for respective dataset(s).

\*Both Authors Contributed Equally  
#Corresponding Author

Numerous studies have used CNN in their studies to select and optimize active face regions instead of using the whole face area. Researchers [10] have used CNN to extract features from three optimized active face regions i.e. Left eye, right eye, and mouth. Recently, researchers [11] developed a model which was able to predict both primary and secondary emotions by using CNN analysis. Authors utilized fiducial points and a feature selection method to select the relevant features from extracted dynamic features of Neural Network classifier and observed 99% accuracy. Also, researchers [12] presented a system of emotion recognition on video data using both CNN and Recurrent Neural Network (RNN). Study [13] examined emotions and grouped them in six categories by using deep neural network. Authors in [14] showed interest introduce the concept of visual was also based on a CNN structure. Viola-Jones algorithm [15] are using for face detection and deep learning convolutional neural networks for facial expression and emotion recognition. This system has reached a great accuracy rate 92.81%. Overall, the use of CNN seems prominent among researchers to establish great accuracy in the recognition of facial expressions. Beside these studies, some researchers [16],[17] applied deep learning and transfer learning approach to recognize minor visible leaf disease. They proposed a concept of assisted learning where a deep learning model category the emotions from an image into eight categories.

Researchers [18] worked with recognition of seven emotions using dual-feature fusion. They have worked using both texture and geometric features to detect facial expression by using Viola-Jones algorithm [19] in an unconstrained environment and gain average accuracy of 98%. They have used the images from the CMU-MultiPIE database. Researcher [20] used Viola-Jones Haar cascade, Active Shape Model, AdaBoost. They claimed that the systems can provide more accuracy 98% for still images. They worked to achieve better accuracy 97.3% with limited training samples of emotions under varying illumination. For global and local feature extraction researcher [21] used Haar Wavelet Transform (HWT) and Gabor wavelets, respectively. Some researchers have used Local Binary Pattern (LBP) and calculated LBP considering 4-neighbors and diagonal neighbors separately. Their study has shown improvement in the recognition rate on JAFFE, CK, FERF, and FEI face databases in both noisy and noise-free conditions. To analyze seven emotions and calculate the features for a three-dimensional face model, researchers [22] applied k-NN classifier and MLP neural network for feature classification. They gained the highest accuracy from k-NN 95.5%. Their classification accuracy can be affected by real conditions.

Researcher in [23] proposed a multimodal human emotion recognition framework as known as EmotionMeter. In real-life application to improve the chance and durability, they design

six electrode placements above the ears to collect EEG signals. Mainly worked on four (happy, sad fear, neutral) emotion using multimodal deep neural networks and achieved best accuracy that is 85.11%. Another study [24] mainly focused on Human Activity Recognition (HAR) and it is a review paper where represents a comprehensive analysis of both handcrafted and learning-based action representations, analysis and discussion on HAR.

Study [25] utilized real-time emotion detection for four basic emotions like happy, sad, anger, fear using five different approaches: AlexNet CNN, Affdex CNN, FER-CNN, SVM, and Multilayer Perception (MLP) and best accuracy achieved from Affdex CNN is 85.05%. Study [26] mainly focused on a novel emotion recognition by using shallowest reliable CNN architecture. They collected data from internet.

Besides, another study [27] mainly focused on multimodal human emotion recognition from eye images and eye movement using two fusion methods: feature level fusion (FLF), BDAE and one classification methods: SVM. For completing this study, they used SEED V datasets and achieved best accuracy from BDAE is 79.63%.

We can categorize the existing methods of emotion recognition from images as dimensional or categorical methods from multilayer hybrid framework [28]. Large scale visual sentiment ontology detections are used to identify adjective-noun pairing [29]. Some researchers recognize emotion based on art feature extraction with art theory [30], [31]. They investigated the shape of features in natural images that influence emotions with visual arts and psychology [32].

### III. PROPOSED SYSTEM

This is a quantitative applied research based on deep learning approach. After image acquisition, image preprocessing takes part with different parameters for two different dataset splits. Training data goes through various preprocessing techniques (zoom, rotation, flip, and shuffle) to improve data quality by enhancing image features important for the further training part of the system. Resizing (224x224) and rescaling (0-1) techniques are applied to testing data and only the common techniques are applied between training and testing splits. The pre-trained model with customized fully connected layer is trained by training split. The feature extraction part of the model at this time goes frozen and only fully connected layers are trained by the dataset. In fine-tuning, selected convolutional layers that are responsible for extracting features are trained alongside fully connected layers. This training process brings changes in pre-trained weights of the models. Trained models are evaluated by testing data split for comparative analysis. Fig. 1 visualizes the whole process of the system.

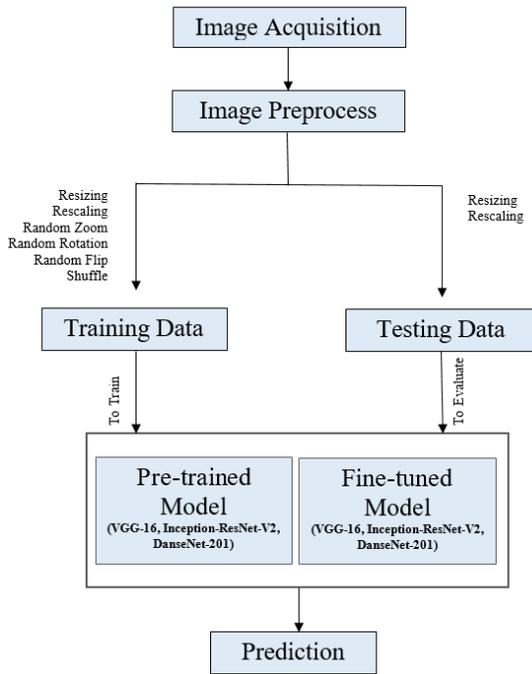


Fig. 1. Proposed Scheme of Emotion Recognition from Eyes and their Surrounding Features.

#### IV. SYSTEM OPERATION

CNN are based on specialized linear operations [2]. It uses convolution instead of matrix multiplication in at least one of their layers. Convolutional layers are used for processing data with a grid-like topology. In computer vision, it is a popular selection for extracting features from visual objects [12].

The convolutional layer takes patches from images known as filters or kernels shown in Fig. 2. These patches are a priority part of an important feature of the entire image. It helps better to understand the features of images than taking the whole image. The filter sizes vary for different layers of network but fix for any individual layer. The dimensionality of the 1<sup>st</sup> layer filter represented as Eq. 1.

$$K(n) = \dim(\text{filter}) = (f_l, f_l, nC_l - 1) \text{ here, } f = \text{filter size} \quad (1)$$

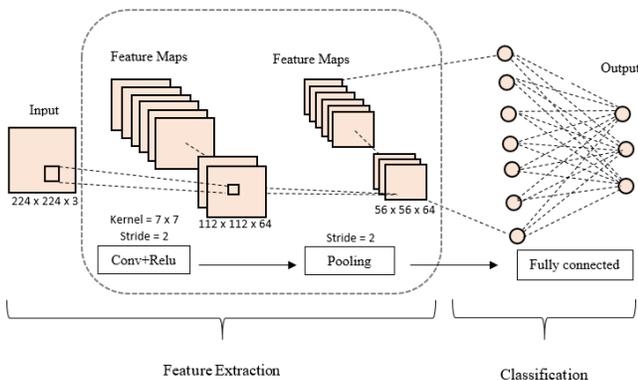


Fig. 2. Feature Extraction and Classification using Neural Network.

The filter shifted over the images with a stride value and computed the feature maps following the mathematical Eq. 2 and Eq. 3.

$$\forall n \in [1, 2, 3, \dots, nC[l]]: \text{conv}(a[l-1], K(n))_{x,y} = \varphi[l](I = 1nW[l-1]j = 1nH[l-1]k = 1nC[l-1]Ki, j, k(n)ax + i - 1, y + j - 1, k[l-1] + bn[l]) \quad (2)$$

$$a[l] = [\varphi[l](\text{conv}(a[l-1], K(1))), \varphi[l](\text{conv}(a[l-1], K(2))), \dots, \varphi[l](\text{conv}(a[l-1], K(nC[l]))) \quad (3)$$

In Eq. 2 and Eq. 3 a [l-1] denotes input data and the beginning image is a0.nC[l] is the number of filters in the image.  $\Phi$  and b denotes activation function and bias. a [l] is the output of convolution layer with size of nW[l], nH[l], nC[l]

Rectified linear units (ReLU) activation function is taken part over the feature map that is calculated by convolutional layer. Only the positive values from the feature map remain the same but the negative values are turned to zero in the ReLU function shown in Eq. 4.

$$f(x) = \max(0, x) \quad (4)$$

The pooling layer aims to pull down sample feature maps generated by following Eq. 3. The feature map value with less impact is neglected and the height value from the feature map is taken for the next sequential layer using the max-pooling function. And calculating the average value from the pooling filter and return is called average pooling. The pooling layer has no parameters to learn.

Eq. 5 is mathematical form of pooling layer,

$$ax, y, z[l] = \text{pool}(a[l-1])_{x,y,z} = \phi[l]((ax + I - 1, y + j - 1, k[l-1])_{i,j \in [1, 2, \dots, f[l]]} 2) \quad (5)$$

Here  $\phi[l]$  is the pooling function.

The fully connected layer is situated on top of the model and is used for classification tasks (Fig. 2). Feature vector obtains from the flatten layer and calculates the value to return to the next layer. Eq. 6 shows the node at faithfully connected layer.

$$Z_j[i] = l = 1ni - 1wj, l[i] al[i-1] + bj[i] \quad (6)$$

Here is the weight of the node.

Convolutional blocks:

The convolutional block is a combination of multiple convolutional layers with necessary activation functions and different types of layers. This combination of layers and activation functions works together to extract features from input data. VGG-16 network architecture contains 16 convolutional layers with the same 3x3 kernel size shown in Fig. 3 [33]. The convolutional layers are separated into five blocks. The model increases the number of feature maps as the depth of the network increases. The final layer of each block takes a pooling layer which reduces the size of feature maps.

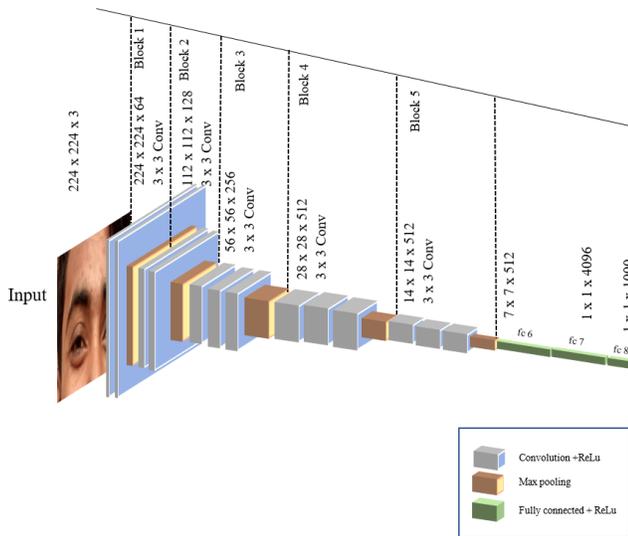


Fig. 3. VGG-16 Network Built-in Blocks.

Inception network breaks the concept of the same filter size in a block [34]. It focuses on different convolutional layers with different filter shape in a single built-in block. Multiple layers subsist in a block with parallel sequences and finally concatenate the output of each sequence of layers. In Fig. 4, the 1x1 convolution layer beginning of a parallel path of a sequence reduces the dimensionality of the input data. Concatenate the output from different filter size sequences facilitated with multi-level feature extraction.

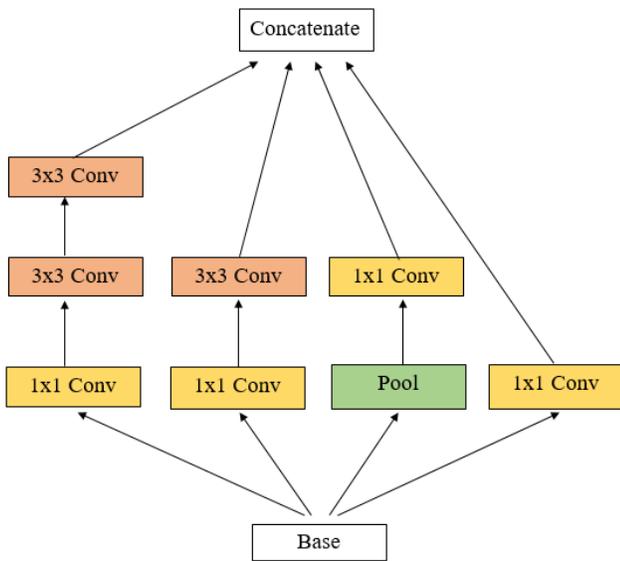


Fig. 4. Schema of INCEPTION BLOCK. Parallel LAYER Sequence with Different Filter Sizes.

Res-Net network fed the output of a convolutional layer to not only the next layer but also ahead of the layer. Then performed element-wise addition. This approach improves the vanishing gradient problem of the network [35]. The Inception-Res-Net network combines the concept of Inception and Res-Net [36]. Fig. 5 shows Inception-Res-Net blocks. This combination can extract multi-level features from images

with less vanishing gradient problems. Inception-Res-Net blocks followed by a 1x1 convolutional layer (without activation) scaling up the dimensionality of feature maps before concatenation.

In the Dense block [9], every convolutional layer obtains direct input from every previous layer shown in Fig. 6. Input feature maps from the previous block, at first go through the batch normalization layer which standardizes the input data. After each convolution, the number of channels remains the same and the number of channels indicates the growth rate of a block. After convolution, mapped output feature is sent not only to next convolutional layer but to the rest of the layers of the block.

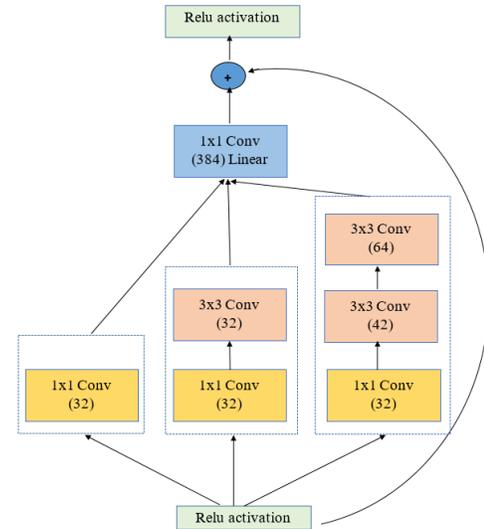


Fig. 5. Schema of Inception-ResNet-V2 Built-in Blocks.

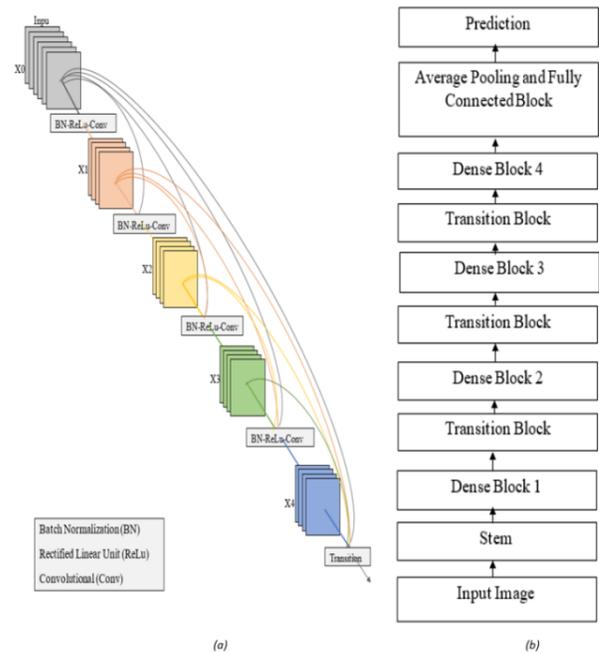


Fig. 6. 5-layer Dense Block Consists of a Growth Rate of 4(a) [6]. Schema of DenseNet-201 Network (b).

### A. Transfer Learning

Transfer learning is a machine learning approach that overcomes the isolated learning paradigm of one model. It opens the door of sharing knowledge to solve related problems. Keras applications (VGG-16, Inception-ResNet-V2, DenseNet-201, etc.) are trained with ImageNet dataset of millions of images of thousands of different classes [5]. The trained Keras model weights are transferable to make it easier to solve the related problem. The ImageNet dataset contains ‘person’, ‘individual’, ‘someone’, ‘somebody’, and more humanistic classes of photos. Transferring this knowledge gained from the ImageNet dataset can boost up the learning performance of selected models with the eye dataset.

### B. Fine Tuning

A pre-trained model contains weights in its node for solving any particular problem. The Keras model is pre-trained model trained with thousands of categorical images of the ImageNet dataset. Fine-tuning, a pre-trained model creates opportunities to solve correlated problems by changes in the weight values of the model. Different blocks of convolutional layers of deep neural networks contain different feature pattern recognition abilities. The last layers and blocks contain the most specific feature pattern of objects. The starting convolutional layers and blocks contain general features of objects like edges and shapes. Updating the weights of the upper blocks with the unique dataset can utilize the model more efficiently.

## V. FACIAL EXPRESSION TYPES AND DATASET DESCRIPTIONS

Human countenances are ostensibly the foremost things we see. We rush to differentiate them in any scene, which they command our consideration. Countenance plays a very important role in our daily lives and we express our emotions through this. Plenty of times we do not say anything but just our facial expressions can explain our situation. Although there are 21 or 30 kinds of facial expressions overall, 7 or 8 kinds of facial expressions are considered universal expressions like anger, disgust, fear, happiness, sadness, and surprise, contempt [37]. Once we convey any quiet expression on our face, all the part of the face like nose, eyes, lips, etc. carry a kind of change. It varies in several expressions. We will read human emotions by watching the expression of a specific organ of the whole face.

In this paper, we have focused on 6 universal facial expressions such as anger, disgust, fear, happiness, sadness, and surprise of human emotions by watching eye expressions shown in Fig. 7. The source of the dataset is attached in Kaggle (link: <https://www.kaggle.com/mdnymurrahmanshuvo/eye-emotion-dataset-diu>) the image mathematically generally represented and showed in Eq. 7.

$$dim(image) = (nW, nH, nC) \tag{7}$$

Here, nW, nH, nC respectively represent the size of the width, size of height, and several channels of an image.

The dataset quantitative properties are described in Table I(a), (b). The dataset is separated into training and

testing parts. In the training dataset, each data class shares an equal amount of data.

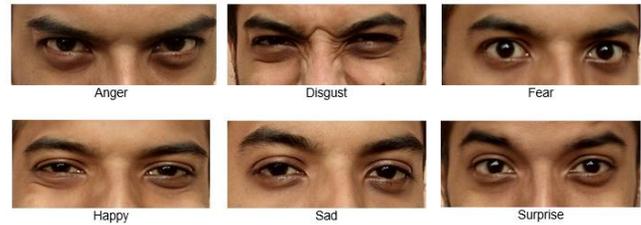


Fig. 7. Eye and its Surroundings Feature Condition in Different Emotional States.

TABLE I. (A) EYE-EMOTION DATASET DISCUSSION

Dataset features	Parameters
Total instance	588
Total training data	450
Total testing data	138
Number of classes	6

(B) EYE-EMOTION DATASET DISCUSSION

Name of classes	Number of test data in class	Number of test data in class
Angry	75	27
Disgust	75	15
Fear	75	23
Happy	75	34
Sad	75	21
Surprise	75	18

## VI. MODEL DESCRIPTIONS

Keras deep learning models are used for prediction, feature extraction and fine-tuning. The models are available with pre-trained weights. Table II contains notable information on some Keras applications used in this study for feature extraction. Depth of deep learning model defines the number of layers exist in the network. The weights of an artificial neural network refer as parameters of it. VGG-16 is a convolutional neural network architecture and was visualized (Fig. 3) with a schematic representation of the VGG-16 network architecture [33]. It improves the performance of Alex-Net by reducing the filter size and increasing the number of channels as the depth of the network. Inception-ResNet-V2 network architecture combines the concept of multi-feature extraction with the reduction of vanishing gradient issues [12]. Fig. 5 concerting the built-in blocks of the network where multiple filter size layers take part (1x1, 3x3) for feature extraction and concatenate the results obtained from parallel layer sequences and the input data from the previous layer (conceptualize from Res-Net architecture). Three Inception-ResNet blocks with a different number and layer combinations take place in the sequential model. The denseness-201 deep convolutional network contains four dense built-in blocks. Three transition blocks followed by the first three dense blocks. A fully connected layer block situated at top of the network shown in Fig. 6.

TABLE II. SELECTED PRE-TRAINED MODEL DESCRIPTION

Model Name	Depth	Number of Built-in Blocks	Parameters	Top-5 Accuracy
VGG-16	23	5	143,667,240	0.901
Inception-ResNet-V2	572	3	55,873,736	0.953
DenseNet-201	201	4	20,242,984	0.923

VII. EXPERIMENTAL ANALYSIS

A. Method and Result Analysis

This study has performed with three different deep convolutional neural network architectures with a dataset of 588 instances. To accelerate the learning process, this study used pre-trained weights to the network. Use of Adam's optimization function with a learning rate of 0.0009 and another parameter like beta\_1-2, epsilon remains the default. 450 epochs get better performance than the nearest numbers of it, where stepper epoch is taken as 10. For training and testing performance measurement, a confusion matrix is used to generate the accuracy ratio. Eq. (8) formula used to calculate the accuracy.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

After the execution of the models with the same dataset, this study found different training and testing accuracy with different methods shown in Tables III and IV. Training accuracy refers the accuracy of the model with training data and testing accuracy refers the accuracy obtain from the model while applying testing data. By freezing the trainable layers, the DenseNet-201 network achieves the height accuracy of 91.78% and 89.13% training and testing terms, respectively.

The noise of a dataset is also trained by a model which creates a performance gap between training and testing accuracy. This term is called overfitting in the field of machine learning. The DenseNet-201 model contains less overfitting of 0.0265 compared to other models.

Fig. 8 contains a training and testing accuracy graph of three different models where the DenseNet-201 graph is smoother than other network architecture. From Fig. 10(b) we observed the Inception-ResNet-V2 loss curve and indicate more overfitting than other two models.

After evaluating the model with test data, the model predicts the class name based on its learning. The predicted result could be True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FS).

TABLE III. RESULT OBTAINED FROM THE PRE-TRAINED

Models	Training Accuracy	Testing Accuracy	Overfitting
VGG-16	0.9043	0.8768	0.0275
Inception-ResNet-V2	0.8967	0.8551	0.0417
DenseNet-201	0.9178	0.8913	0.0265

TABLE IV. RESULT OBTAINED FROM FINE-TUNED MODELS

Model Name	Training Accuracy	Testing Accuracy	Overfitting
VGG-16	0.8432	0.8106	0.0326
Inception-ResNet-V2	0.8401	0.7806	0.0595
DenseNet-201	0.8621	0.8170	0.0451

Precision refers to the ratio of total correctly predicted positive values (TP) to total predicted positive values (TP+FP).

$$Precision = \frac{TP}{TP + FP} \quad (9)$$

Recall refers the proportion of total correctly predicted positive values (TP) to total actual positive values in dataset (TP+FN).

$$Recall = \frac{TP}{TP + FN} \quad (10)$$

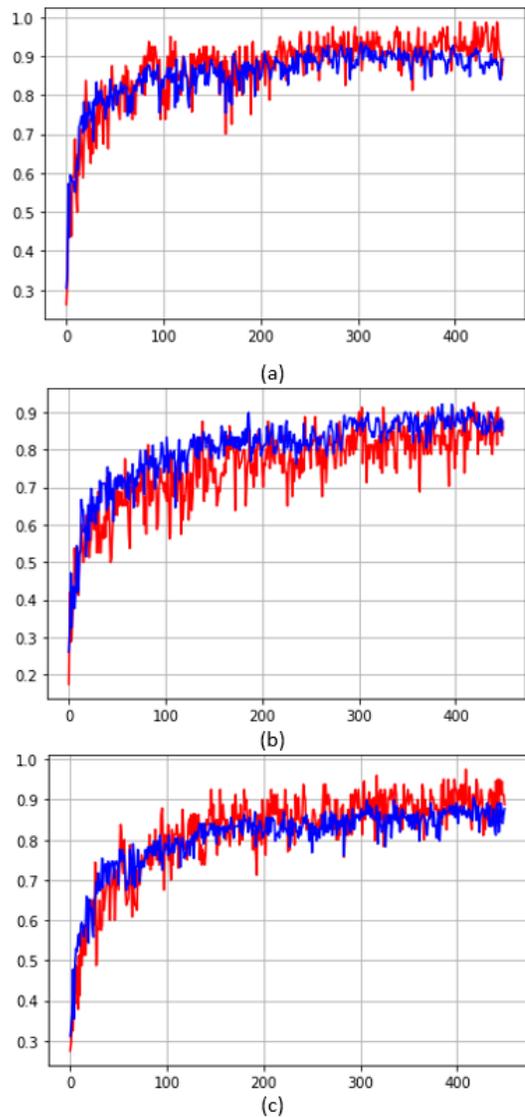


Fig. 8. Accuracy Graph of DenseNet-201 (a), InceptionResNet-V2 (b) and VGG-16(c).

TABLE V. PREDICTION RESULT ANALYSIS OF DENSENET-201 MODEL

Class Name	Precision	Recall	F1-score
Anger	0.89	0.89	0.89
Disgust	0.77	0.67	0.71
Fear	0.96	1.00	0.98
Happy	0.91	0.85	0.88
Sad	0.90	0.90	0.90
Surprise	0.86	1.00	0.92

TABLE VI. PREDICTION RESULT ANALYSIS OF INCEPTION-RESNET-V2 MODEL

Class Name	Precision	Recall	F1-score
Anger	0.83	0.93	0.88
Disgust	0.75	0.80	0.77
Fear	0.79	0.96	0.86
Happy	1.00	0.85	0.92
Sad	0.89	0.81	0.85
Surprise	0.81	0.72	0.76

TABLE VII. PREDICTION RESULT ANALYSIS OF VGG-16 MODEL

Class Name	Precision	Recall	F1-score
Anger	0.89	0.93	0.91
Disgust	0.76	0.87	0.81
Fear	0.92	0.96	0.94
Happy	0.96	0.79	0.87
Sad	0.81	0.81	0.81
Surprise	0.95	0.94	0.89

F1-score refers harmonic mean of model’s precision and recall. A good F1-score refers that the model predicts less false positives and false negatives.

$$F1Score = 2 \times \frac{Recall \times Precision}{Recall + Precision} \quad (11)$$

Eq. 9, 10, and 11 are applied to predict results obtaining from models to calculate the precision, recall and F1-score, respectively. Tables V, VI and VII contain class wise precision, recall and F1-score of testing data obtained from DenseNet-201, InceptionResNetV2 and VGG-16, respectively.

TABLE VIII. CONFUSION MATRIX OF DENSENET-201 MODEL WITH EYE EMOTION DATASET

Expressions	Angry	Disgust	Fear	Happy	Sad	Surprise
Angry	24	1	1	0	1	0
Disgust	3	10	0	2	0	0
Fear	0	0	23	0	0	0
Happy	0	1	0	29	1	3
Sad	0	1	0	1	19	0
Surprise	0	0	0	0	0	18

B. Error Analysis

Table VIII contains the confusion matrix of the DenseNet-201 model with the eye emotion dataset. Confusion matrix or error matrix is a kind of mode’s prediction summary refers the

classification problems. Overall, 89.13% accuracy is achieved to classify the human emotion from the eye and its surrounding features. Here in Table VII, the actual 'Disgust' class several times is predicted as 'Anger' and 'Happy'. There are some common features in the Disgust, Anger, and Happy classes shown in Fig. 9. These features are important parameters for all of the classes [15]. Sometimes, these common features are so much prominent to other features of the classes that the model confused with the actual class to other classes.

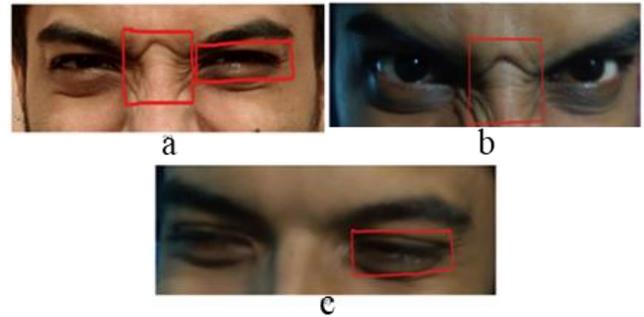


Fig. 9. Feature Similarities among (a) Disgust, (b), Angry, and (c) Happy Classes.

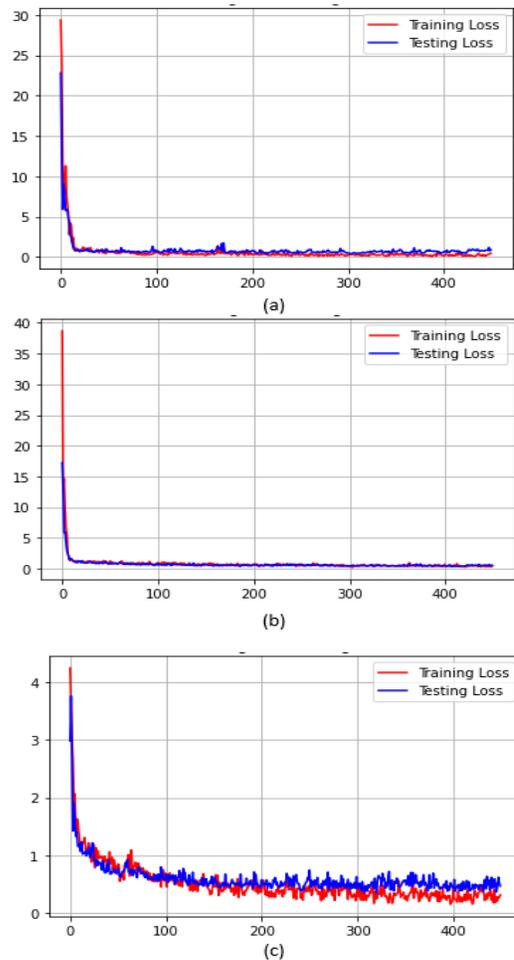


Fig. 10. Loss Graph of DenseNet-201(a), InceptionResNet-V2 (b) and VGG-16(c).

### VIII. COMPARATIVE ANALYSIS

As mentioned earlier (Section II), many studies have been done to find out the human emotion recognition using machine learning, deep learning, and other techniques based on data (s) from different facial expressions of people.

TABLE IX. COMPARISON OF THE PRIOR METHODS WITH THE PROPOSED METHOD

Studies	Methods	Accuracy	Datasets
G Verma, et al.[10]	Hybrid CNN	97.07% of FER2013 and 94.12% of JAFFE	FER2013, JAFFE
S. A. Fatima et al. [11]	Mini-Xception, CNN	95.60% from Mini-Xception	FRR2013, Real Time Data
N. Jain et al. [13]	Hybrid Convolutional-RNN	94.91% of JAFFE, 92.07% of MMI	JAFFE, MMI
A. H. Mary et al. [14]	Deep CNN	92.81%	Universal and Personal data
Xuanyu He et al. [17]	CNN	64.6%	Universal data, ArtPhoto, Paintings
S. Palaniswamy et al. [19]	Viola-jones, Active Shape Model, AdaBoost	96%	CMU-MultiPIE, Survey data

Some notable information of the previous studies is shown in Table IX. Many authors have used various methods such as Hybrid CNN, Deep CNN, Hybrid RNN, Viola Jones model and they showed accuracy: 97%, 92%, 94.91%, and 96% respectively. It is worth noting that these studies considered the entire face to recognize the human emotions. However, this study mainly focuses on the data from the eyes and its surrounding areas only. The whole face detection system can identify a human face present in an image/video – it cannot identify that person, but the eyes and its surrounding area can give more precision and accuracy to recognize the person. Subsequently, in the proposed approach we achieved better accuracy 95.3% using Inception ResNet-V2 and the outcomes are comparable with the previous studies in terms accuracy and precision.

### IX. CONCLUSION

Nowadays, automated emotion recognition from facial expressions has become a challenging topic of computer vision but we focus specifically on eye expression of facial expression [38]. We proposed a customized model of deep neural network architecture for eye expression. It takes eye images as input then classifies them into either of six eye expressions: happiness, sadness, anger, disgust, fear, surprise. To get higher accuracy we have trained our dataset with pre-trained weights and used a confusion matrix to analyze the prediction. Our top accuracy rate is 91.78% in DenseNet-201 and contains less overfitting of 0.0265.

### X. LIMITATION OF THE STUDY AND FUTURE DIRECTION

Challenges like partial occlusions, facial incompleteness, the pose of the face, invariance to pose, poor image quality,

continuously changing emotions, backlight, illumination variation, and many additional factors in the real-time detection will be under our investigation and further can be explored our in future studies to improve the recognition rate [19]. We strive to improve and develop our proposed system in several directions. Some other primary and secondary facial expressions will be added to our dataset and other advanced deep learning models with superior learning capabilities, better performance, shorter operation time, and higher classification accuracy can be implemented for testing and comparing the accuracy and ensuring more accurate recognition of emotions.

### REFERENCES

- [1] V. S. Johnston, Why we feel: The science of human emotions. Perseus Publishing, 1999.
- [2] R. Yamashita, M. Nishio, R. K. G. Do, and K. Togashi, "Convolutional neural networks: an overview and application in radiology," *Insights Imaging*, vol. 9, no. 4, pp. 611–629, 2018.
- [3] M. M. Hassan, S. Huda, J. Yearwood, H. F. Jelinek, and A. Almogren, "Multistage fusion approaches based on a generative model and multivariate exponentially weighted moving average for diagnosis of cardiovascular autonomic nerve dysfunction," *Inf. Fusion*, vol. 41, pp. 105–118, 2018.
- [4] M. M. Hassan, M. G. R. Alam, M. Z. Uddin, S. Huda, A. Almogren, and G. Fortino, "Human emotion recognition using deep belief network architecture," *Inf. Fusion*, vol. 51, pp. 10–18, 2019.
- [5] G. Lee, M. Kwon, S. K. Sri, and M. Lee, "Emotion recognition based on 3D fuzzy visual and EEG features in movie clips," *Neurocomputing*, vol. 144, pp. 560–568, 2014.
- [6] E. Kanjo, E. M. G. Younis, and N. Sherkat, "Towards unravelling the relationship between on-body, environmental and emotion data using sensor information fusion approach," *Inf. Fusion*, vol. 40, pp. 18–31, 2018.
- [7] Z. Liu et al., "A facial expression emotion recognition based human-robot interaction system," 2017.
- [8] A. S. Al-Waisy, R. Qahwaji, S. Ipson, S. Al-Fahdawi, and T. A. M. Nagem, "A multi-biometric iris recognition system based on a deep learning approach," *Pattern Anal. Appl.*, vol. 21, no. 3, pp. 783–802, 2018.
- [9] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 4700–4708.
- [10] G. Verma and H. Verma, "Hybrid-Deep Learning Model for Emotion Recognition Using Facial Expressions," *Rev. Socionetwork Strateg.*, vol. 14, no. 2, pp. 171–180, 2020.
- [11] S. A. Fatima, A. Kumar, and S. S. Raof, "Real Time Emotion Detection of Humans Using Mini-Xception Algorithm," in *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1042, no. 1, p. 12027.
- [12] T. Wiatowski and H. Bölskei, "A mathematical theory of deep convolutional neural networks for feature extraction," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1845–1866, 2017.
- [13] N. Jain, S. Kumar, A. Kumar, P. Shamsolmoali, and M. Zareapoor, "Hybrid deep neural networks for face emotion recognition," *Pattern Recognit. Lett.*, vol. 115, pp. 101–106, 2018.
- [14] A. H. Mary, Z. B. Kadhim, and Z. S. Sharqi, "Face Recognition and Emotion Recognition from Facial Expression Using Deep Learning Neural Network," in *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 928, no. 3, p. 32061.
- [15] T. Chen, D. Borth, T. Darrell, and S.-F. Chang, "DeepSentibank: Visual sentiment concept classification with deep convolutional neural networks," *arXiv Prepr. arXiv1410.8586*, 2014.
- [16] Md. Ashiqul Islam; Md. Nymur Rahman Shuvo; Muhammad Shamsoljaman; Shazid Hasan; Md. Shahadat Hossain; Tania Khatun, "An Automated Convolutional Neural Network Based Approach for

- Paddy Leaf Disease Detection,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 1, 2021, doi: 10.14569/IJACSA.2021.0120134.
- [17] X. He and W. Zhang, “Emotion recognition by assisted learning with convolutional neural networks,” *Neurocomputing*, vol. 291, pp. 187–194, 2018.
- [18] A. Mahmood, S. Hussain, K. Iqbal, and W. S. Elkilani, “Recognition of facial expressions under varying conditions using dual-feature fusion,” *Math. Probl. Eng.*, vol. 2019, 2019.
- [19] S. Palaniswamy and S. Tripathi, “Emotion Recognition from Facial Expressions using Images with Pose, Illumination and Age Variation for Human-Computer/Robot Interaction.,” *J. ICT Res. Appl.*, vol. 12, no. 1, 2018.
- [20] C. Reddy, U. Reddy, and K. Kishore, “Facial Emotion Recognition Using NLPCA and SVM.,” *Trait. du Signal*, vol. 36, no. 1, pp. 13–22, 2019.
- [21] D. G. R. Kola and S. K. Samayamantula, “A novel approach for facial expression recognition using local binary pattern with adaptive window,” *Multimed. Tools Appl.*, pp. 1–20, 2020.
- [22] P. Tarnowski, M. Kołodziej, A. Majkowski, and R. J. Rak, “Emotion recognition using facial expressions,” *Procedia Comput. Sci.*, vol. 108, pp. 1175–1184, 2017.
- [23] W.-L. Zheng, W. Liu, Y. Lu, B.-L. Lu, and A. Cichocki, “Emotionmeter: A multimodal framework for recognizing human emotions,” *IEEE Trans. Cybern.*, vol. 49, no. 3, pp. 1110–1122, 2018.
- [24] A. B. Sargano, P. Angelov, and Z. Habib, “A comprehensive review on handcrafted and learning-based action representation approaches for human activity recognition,” *Appl. Sci.*, vol. 7, no. 1, p. 110, 2017.
- [25] A. Kartali, M. Roglić, M. Barjaktarović, M. Đurić-Jovičić, and M. M. Janković, “Real-time Algorithms for Facial Emotion Recognition: A Comparison of Different Approaches,” in *2018 14th Symposium on Neural Networks and Applications (NEUREL)*, 2018, pp. 1–4.
- [26] V. Pandit, M. Schmitt, N. Cummins, and B. Schuller, “I see it in your eyes: Training the shallowest-possible CNN to recognise emotions and pain from muted web-assisted in-the-wild video-chats in real-time,” *Inf. Process. Manag.*, vol. 57, no. 6, p. 102347, 2020.
- [27] J.-J. Guo, R. Zhou, L.-M. Zhao, and B.-L. Lu, “Multimodal emotion recognition from eye image, eye movement and eeg using deep neural networks,” in *2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2019, pp. 3071–3074.
- [28] M. A. Nicolaou, H. Gunes, and M. Pantic, “A multi-layer hybrid framework for dimensional emotion classification,” in *Proceedings of the 19th ACM international conference on Multimedia*, 2011, pp. 933–936.
- [29] D. Borth, R. Ji, T. Chen, T. Breuel, and S.-F. Chang, “Large-scale visual sentiment ontology and detectors using adjective noun pairs,” in *Proceedings of the 21st ACM international conference on Multimedia*, 2013, pp. 223–232.
- [30] J. Machajdik and A. Hanbury, “Affective image classification using features inspired by psychology and art theory,” in *Proceedings of the 18th ACM international conference on Multimedia*, 2010, pp. 83–92.
- [31] S. Zhao, Y. Gao, X. Jiang, H. Yao, T.-S. Chua, and X. Sun, “Exploring principles-of-art features for image emotion recognition,” in *Proceedings of the 22nd ACM international conference on Multimedia*, 2014, pp. 47–56.
- [32] X. Lu, P. Suryanarayan, R. B. Adams Jr, J. Li, M. G. Newman, and J. Z. Wang, “On shape and the computability of emotions,” in *Proceedings of the 20th ACM international conference on Multimedia*, 2012, pp. 229–238.
- [33] S. Liu and W. Deng, “Very deep convolutional neural network based image classification using small training sample size,” in *2015 3rd IAPR Asian conference on pattern recognition (ACPR)*, 2015, pp. 730–734.
- [34] 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.
- [35] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition (2015),” *arXiv Prepr. arXiv1512.03385*, 2016.
- [36] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. Alemi, “Inception-v4, inception-resnet and the impact of residual connections on learning,” in *Proceedings of the AAAI Conference on Artificial Intelligence*, 2017, vol. 31, no. 1.
- [37] A. T. Lopes, E. de Aguiar, A. F. De Souza, and T. Oliveira-Santos, “Facial expression recognition with convolutional neural networks: coping with few data and the training sample order,” *Pattern Recognit.*, vol. 61, pp. 610–628, 2017.
- [38] J. Z. Lim, J. Mountstephens, and J. Teo, “Emotion recognition using eye-tracking: taxonomy, review and current challenges,” *Sensors*, vol. 20, no. 8, p. 2384, 2020.

# Novel Data Oriented Structure Learning Approach for the Diabetes Analysis

Adel THALJAOU

Department of Computer Science and Information, College of Science at Zulfi  
Majmaah University, Al-Majmaah 11952  
Saudi Arabia

**Abstract**—Diabetes mellitus is considered a significant disease an ever rising epidemic. Accordingly this disease represents a worldwide public-health-crisis. Several classification techniques have been recently employed for diabetes diagnosis, however only few researches have been dedicated to facilitating its analysis based on knowledge representation using probabilistic modelling. Bayesian Network as a probabilistic graphical model is considered as one of the most effective techniques of classification. Bayesian Network (BN) is widely employed in several domains like risk analysis, medicine, bioinformatics and security. This probabilistic graphical model represents an effective formalism to reason under uncertainty. The construction of the BN model goes through two learning phases of structure and parameter. The first learning phase of BN skeleton has been assessed as complex problem (NP-hard problem). Accordingly, several methods have been introduced amongst which the score based algorithms that are considered as one of the most powerful methods of structure learning. In this paper, we introduce a novel algorithm based on graph theory and the information theory combination. The proposed algorithm called GIT algorithm for Parents and children detection for BN structure learning. In addition, we evaluate the obtained results and using the reference networks, we prove the efficiency of the proposed GIT algorithm in terms of accuracy. Furthermore, we apply our algorithm in a real field, especially for detecting the interesting dependencies which are useful for the diabetes analysis.

**Keywords**—Classification; Bayesian Network; structure learning; score oriented approach; diabetes analysis

## I. INTRODUCTION

In this century, the diabetes mellitus represents a serious health problem [1] [2]. The International Diabetes Federation (IDF) reveals that by 2040 it is expected to have 642 million adults who are diabetic and during the next two decades, our world will attend an important increase of 10.4%. The estimated percentage of the undiagnosed diabetes is about 0.497 of all affected people where the highest values were discovered respectively in Africa (70), South-East of Asia (60) and regions of Western Pacific (54) [3]. Consequently, and considering the importance of these diagnostics, correct and rapid analysis for diabetes detection using an intelligent technique has been considered as a crucial necessity [1] [4] [5].

The BN is a classification technique based on the graphical representation mode and the probabilistic reasoning. This technique is deemed as consistent formalism for making a

model for the complex systems [6]. This classification technique is included in the most extensively used category of probabilistic-graphical models [7]. Therefore, and because of its potent abilities in reasoning using graphical representation, the BN has been effectively applied in several research areas like image processing [8], risk analysis [9], medical diagnosis [10], image processing [11], bioinformatics [12], etc. The construction of the BN model consists of two learning stages of its structure and its parameter. The structure learning phase allows the specification of the dependency set between the variables (random). In fact, it permits to create a directed acyclic graph (DAG), which consists of nodes and edges representing the dependency relation between Parents and children nodes while the parameter learning stage allows these dependencies' quantification.

The aim of the first learning phase is to generate the optimal structure which is judged as an NP-hard problem due to the intractable space of search [13]. In order to solve this problem, two main methods have been proposed: data oriented method and the second one is based on the expert knowledge [14] which is time consuming. In this paper, we propose a score driven algorithm, called GIT algorithm, which is based on the Information Theory IT (precisely the Mutual Information MI exchanged between nodes) and the Graph Theory GT. The proposed BN was experimented while assisting in the exploration of the medical database for diabetes diagnosis in the Zulfi hospital of Saudi Arabia [5].

Section II is dedicated to the fundamental concept's introduction which is useful for our proposal description. Section III is devoted to the proposed GIT algorithm representation. In Section IV, we represent an illustrative example. Section V introduces the experimental results and its evaluation using the well-known benchmarks. In Section VI, we present the application of the proposed data oriented method in the medical field, precisely for the diabetes diagnosis. In the last section which is our conclusion, we summarize the main ideas of the paper.

## II. PRELIMINARIES

Since our purpose is to propose a novel BN structure learning algorithm based on the IT and the GT, we have to introduce the interrelated notions before highlighting the proposed idea.

### A. Structure Learning of the BN

The Bayesian network is a Direct Acyclic Graph (DAG) that allows the representation of the distribution of the conditional probabilities over a set of variables. The DAG is composed of a set of nodes (random variables) and edges representing the dependencies between the nodes. The BN is illustrated as a couple (G, P) where the G is the directed graph and P designates the probabilities distribution, and the graph can be denoted as a couple (N, E), in which N is the nodes (or the random variables) and the E designates the edges between the nodes. The variable value can be discrete or continuous. As indicated in the following equation, the joint probability distributions are computed as the product of the local conditional probabilities:

$$P(N_1, N_2, \dots, N_n) = \prod_{i=1}^n P(N_i | P_a(N_i)) \quad (1)$$

Where  $N_i$  is the node  $i$  and  $P_a(N_i)$  represents its parent.

The construction of the BN model consists of two learning phases of the structure and the parameter. The learning of the BN structure allows us to obtain the graphical representation of the qualitative knowledge in which we are focusing on in this paper. The structure learning phase aims to represent explicitly the causal relationship among the random variables (is the answer of the “what if?” question) [15].

In the last two decades, several algorithms of BN structure-learning have been proposed which can be categorized into score oriented approach, conditional independency based approach and hybrid approach. (1) The conditional independency based methods perform a qualitative study of the variables dependency, and the generated skeleton represents these dependency relationships. The well-known algorithms of this approach are the PC (Predictive Causation) algorithm and IC (Inductive Causation) algorithm. (2) The score oriented approach is based on the score metric and it aims to determine the learned graph that maximizes the used score. This metric is defined as a fit measure between the data and the graph. The main goal of the algorithms based on the score is to produce the structure having the highest score. For instance, we can cite the MWST (Maximum Weight Spanning Tree) algorithm, GS (Greedy Search) algorithm, SEM (Structural Expectation Maximization) algorithm and K2 algorithm. Different score metrics have been proposed such as the BIC (Bayesian Information Criterion), BDe (Bayesian Dirichlet Equivalent), MDL (Minimum Description Length) and the AIC (Akaike Information Criterion). (3) The hybrid approach combines the advantages of both cited methods in learning the correct BN skeleton. As examples, we can cite the MMB (Max Min Markov Blanket) algorithm and MMPC (Max Min Parents Children) algorithm.

In the last decade, many researches proved that the methods based on score represent the widely used algorithms like Amirkhani et al. [16] (2016), Tabar et al. [17] (2018) and Benmohamed et al. [18] (2019) [19](2020), Accordingly, the present study introduces a novel score based algorithm as explained in the following section.

### III. PROPOSED SCORED-ORIENTED-ALGORITHM

The proposed GIT method (Fig. 1) is divided into two main phases. The first phase allows the extraction of the dependencies between the different random variables within the dataset in order to create an undirected acyclic graph. To obtain this latter, we have to avoid the cyclic structure and the weak dependencies between the nodes. Henceforth, the extracted graph is used to determine the list of parent and children nodes. The generated oriented acyclic graph is not only important for correct parameter learning and instances classification but it also provides a graphical representation of useful knowledge that allows a better analysis of the dataset.

For extracting the undirected acyclic graph, we used the information theory IT, precisely the calculation of the mutual information MI in order to eliminate the cyclic structure. Basing on the graph theory GT, we start by avoiding the cycle between each tree nodes forming the graph because of the acyclic characteristic of the BN. In our algorithm called IT and GT based structure learning algorithm (GIT), the MI is calculated to determine the weak dependencies for erroneous edge elimination. Between each two variables A and B, the MI noted  $I(A,B)$  is calculated as follows:

$$I(A, B) = H(A) - H(A | B). \quad (2)$$

$H(A)$  is the entropy of A, and  $H(A|B)$  represents the conditional entropy of A given B. The entropy of the variable A is defined by:

$$H(A) = -\sum_{i=1}^n P(A_i) \log(P(A_i)) \quad (3)$$

Mathematically, the  $H(A|B)$  is defined by the following equation:

$$H(A | B) = \sum_{i=1}^n \sum_{j=1}^m P(A = a_i, B = b_j) \times \log(P(A = a_i, B = b_j)) \quad (4)$$

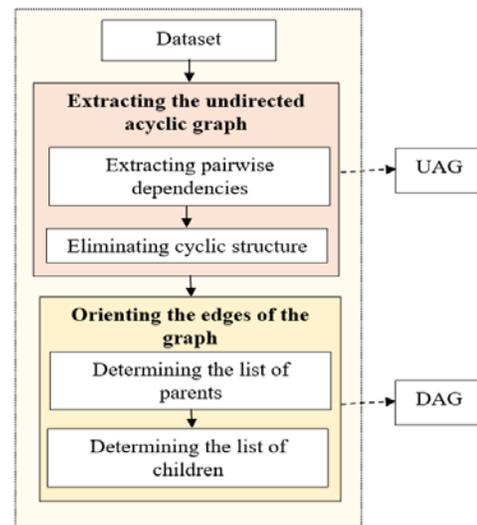


Fig. 1. Schematic Representation of the Proposed GIT Algorithm.

For learning the BN structures, we used in the algorithm the mutual information MI which is significantly used in the literature for structure learning. The proposed sub-algorithm for undirected graph extraction (Algorithm 1) included two phases, for the detection of the dependencies between nodes and for cyclic structure elimination as described in the rest of this section.

---

**Algorithm 1** Undirected graph learning

---

**Input:** Dataset

**Output:** UAG (dag)

1. Repeat for i from 1 to N do
  2. Repeat for j from i+1 to N do
  3. K= 1, OK=True
  4. if i ≠ j then
  5. Repeat while OK==True and k<=N do
  6. if (k ≠ i) && (k ≠ j) then
  7. MI<sub>ij</sub> ← calc\_mutual\_information(i, j);
  8. MI<sub>ki</sub> ← calc\_mutual\_information(k, i);
  9. MI<sub>jk</sub> ← calc\_mutual\_information(j, k);
  10. if MI<sub>ij</sub> > MI<sub>ki</sub> || MI<sub>ij</sub> > MI<sub>jk</sub> then
  11. ok ← True;
  12. else
  13. ok ← False;
  14. end if
  15. end if
  16. k=k+1;
  17. end while
  18. if (k>N) then
  19. dag(i,j) ← 1
  20. end if
  21. end for
  22. end for
- 

As shown in Algorithm 1, for each pairwise (X, Y) we verify the existence of a third node Z forming a cycle. As defined in the graph theory, the path can form a cycle if the start node (ni) represents the final node in the path (with the number of nodes is greater or equal to 1). In order to avoid the circuit formed by the three nodes X, Y and Z, we eliminate the weak dependency. In fact, if the condition cannot be reached, the specified nodes will form a cycle and the edge between the original pairwise should be eliminated as shown in Fig. 2:

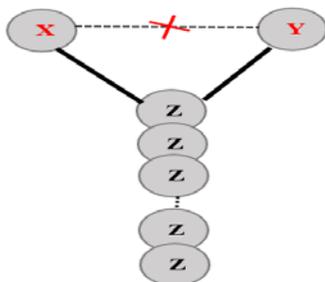


Fig. 2. Elimination of the Edge with Weak Dependency.

As a matter of fact, we use the obtained graph to determine the orientation of each edge. Indeed, the lists of parents and children can be created the final graph which are acyclic and

oriented. These tasks are reached by Algorithm 2 which consists of two phases for parent and children detection. In [20], the dependence criteria used to determine the parent or the children node between two dependent nodes (X and Y) is calculated as:

$$OE(Y \rightarrow X) = \frac{H(X|Y)}{H(X) \times |X|}, X \neq Y \quad (5)$$

Where OE determines the orientation of the edge from Y to X (Y node represents the node parent) and the possible values' number of the variable X is |X|. In addition, we combine this criteria with the condition based on the value of the Maximum Mutual Information (MMI) for the edge orientation. For the determining of the parent and child, we propose an amelioration of the OE metric as follows:

The node X represents the parent if this condition is satisfied:

$$\frac{H(Y|X)}{H(Y) \times |Y|} + I(X) > \frac{H(X|Y) + I(Y)}{H(X) \times |X|} + (\alpha \times MMI(X))$$

Where  $\alpha \geq 0.5$

If the node Y is the child and the orientation of the edge is (Y → X), the following condition should be satisfied:

$$\frac{H(X|Y)}{H(X) \times |X|} + I(Y) > \frac{H(Y|X) + I(X)}{H(Y) \times |Y|} + (\alpha \times MMI(Y))$$

These steps is explained in the algorithm2:

---

**Algorithm 2** Orienting the edges

---

**Input:** Undirected Acyclic Graph (UAG)

**Output:** set of candidate parents and children

1. for i from 1 to N-1
  2. for j from i+1 to N do
  3. calculateMaxMI(i) ← Max(MI(i,j))
  4. end for
  5. end for
  6. for i from 1 to N-1 do
  7. for j from i+1 to N do
  8. OE<sub>ij</sub> ← calc\_OE(i,j);
  9. OE<sub>ji</sub> ← calc\_OE(j,i);
  10. MI<sub>ij</sub> ← calc\_mutual\_information(i, j);
  11. if (OE<sub>ij</sub> + MI<sub>ij</sub> > OE<sub>ji</sub> +  $\alpha$  \* MaxMI[i]) then
  12. CandidateParents [j] ← i;
  13. CandidateParents [i] ← j;
  14. else if (OE<sub>ji</sub> + MI<sub>ij</sub> > OE<sub>ij</sub> +  $\alpha$  \* MaxMI[j]) then
  15. CandidateParents [i] ← j;
  16. CandidateParents [j] ← i;
  17. end if
  18. end if
  19. end for
  20. end for
-

In this section, we describe our method for learning the BN structure through data oriented approach. The learned dependencies obtained by the execution of the first algorithm are oriented basing on the second algorithm for generating the final directed acyclic graph. The main idea for the structure learning is based on the mutual information and the graph theory. The following section will be dedicated to the representation of the experimental results.

#### IV. EXPERIMENTAL RESULTS

##### A. Used Datasets

To test the proposed GIT algorithm on the well-used benchmark networks, firstly we represent these datasets and then the used performance measures. Thus, the test of the novel algorithm, is done using the three well-known datasets: ASIA, CANCER and ALARM. The algorithm is executed on an Intel i5-5300U with 8G of memory (64-bit system). In the following table, we expose the datasets description (Table I):

In the next sub-section, the evaluation metrics of the GIT algorithm's performance and the gained results will be described.

##### B. Used Metrics and Experimental Results

The evaluation of the proposed algorithm, which is based mainly on the MI and the GT demonstrates its efficiency in resolving the structure learning problem. Moreover, to present the obtained results, we use the metrics shown in Table II.

The experimental results, shown in Fig. 3, Fig. 4 and Fig. 5, will be described using the difference between the original structure and the learned one (terms: CE, AE, DE, RE, SD).

To verify the effectiveness of the GIT algorithm, it was executed on the datasets shown in Table II for 1000, 2000, 3000, 5000 and 10000 cases. Fig. 3, Fig. 4 and Fig. 5 show the experimental results basing on structures difference between the obtained skeleton and the original. In Fig. 4, we show the gained results for ASIA network for different cases which are seven correct edges, one reversed edge and zero deleted and added edge. In fact, for this latter, we obtain sensitive values when changing the number of cases from 1000 to 10000. In addition, for CANCER network, we obtain four correct edges for 1000, 2000 and 3000 cases with one added edge. However, for ALARM network, our method can correctly detect thirty four edges, four edges are wrongly deleted, one reversed edge, and eleven are added incorrectly for ALARM-1000, ALARM-2000 and ALARM-3000. For the rest of the cases, our GIT algorithm produces just one reversed edge, four deleted edges and twelve added edges; accordingly, we obtain seventeen erroneous edges in comparison to the original ALARM network.

TABLE I. USED DATASETS IN THE EXPERIMENTS

Dataset	Number of cases	Number of nodes	Number of edges
CANCER	1000/2000/3000/ 5000/10000	5	4
ASIA	1000/2000/3000/ 5000/10000	8	8
ALARM	1000/2000/3000/ 5000/10000	37	46

TABLE II. THE USED EVALUATION METRICS

Metric	Description
RE	The reversed edge: is the correct edge with the inversed orientation
CE	The correct edge: exists in the original and the learned graph
AE	The added edge: does not exist in the original network
DE	The deleted edge: exists in the learned structure and does not exist in the original graph
SD	The erroneous edges: represent the structural difference (RE+AE+DE).

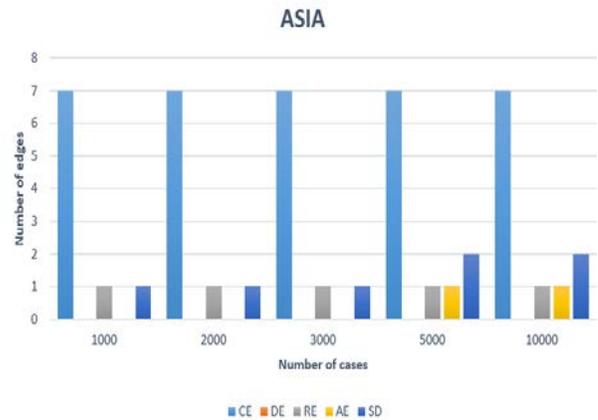


Fig. 3. Experimental results for ASIA network

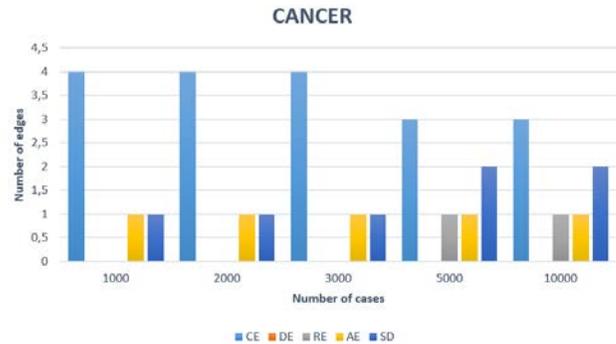


Fig. 4. Experimental results for CANCER network

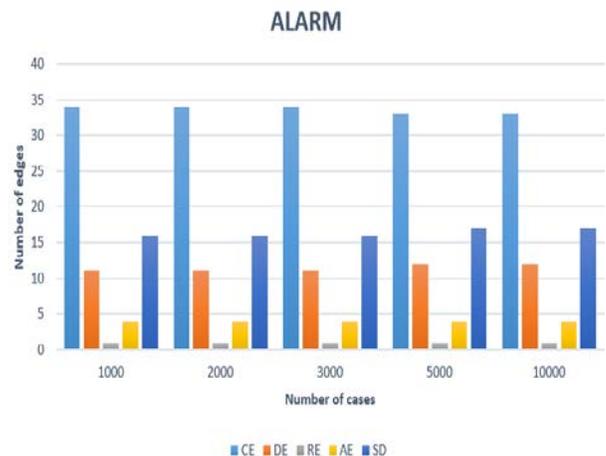


Fig. 5. Experimental results for ALARM network

Furthermore, we use the accuracy metric (Acc) [21] in order to present the performance of our GIT algorithm and this factor is defined as follows:

$$Acc = \frac{CE}{CE + SD}$$

In the following figure, we introduce the values of accuracy for the 1000, 2000, 3000, 5000 and 10000 cases for CANCER, ASIA and ALARM networks.

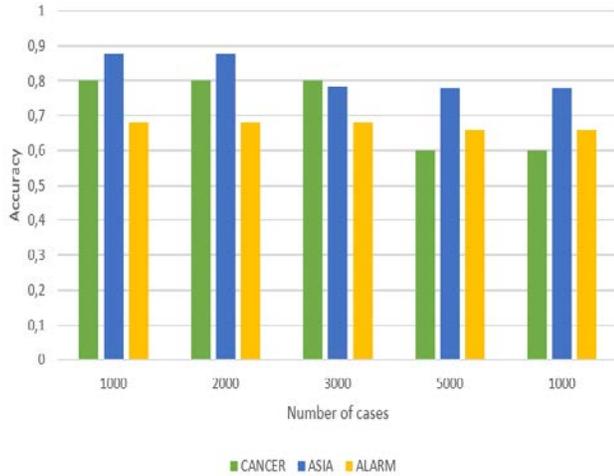


Fig. 6. Accuracy for Various Datasets.

As shown in Fig. 6, the proposed method produces better accuracy values for ASIA network which are respectively for ASIA (1000, 2000 and 3000) 0.875 and for ASIA (5000 and 10000) 0.778. In addition for CANCER network, for 1000, 2000 and 3000 is 0.8 and for CANCER-5000 and CANCER-10000 equals to 0.6. As shown, for ALARM-1000, ALARM-2000, ALARM-3000, ALARM-5000 and ALARM-10000, all values are greater than 0.65 and decrease with the increase of the number of samples. The produced results allow the demonstration of the reliability of the proposed algorithm for learning the structure of CANCER, ASIA and ALARM networks. Besides, for GIT algorithm efficiency demonstration, we present a comparison section of the gained results with the other methods results for the resolution of the BN structure-learning problem.

### V. EXPERIMENTAL RESULTS

The gained results produced by the GIT algorithm are introduced in Table III and Table IV for respectively ASIA and ALARM networks. The terms CE, AE, DE and RE designate the number of correct edges and respectively the number of accidentally added, deleted and reversed edges. The tables show the evaluation of our results compared to the NDPSO-BN [22], Ko and Kim [23], Tabar et al. [ ] and Ai [24] algorithms for ASIA and ALARM networks for 1000, 2000, 3000, 5000 and 10000 cases. To highlight the results, the bold value represents the best value and the starred value depicts the second potential value.

In Table III, we present the different experimental results describing the difference between the original topology and the learned structure using respectively our algorithm, NDPSO-BN, Ko and Kim, Tabar et al. and Ai algorithms. As exhibited, our GIT algorithm allows the gaining of the best or the second best results for ASIA-1000, ASIA-2000 and ASIA-3000. Comparing to the NDPSO-BN method, our algorithm produces the same number of erroneous edges, which equals to one edge. The GIT algorithm detects the eight correct edges but with one incorrect oriented edge while the NDPSO-BN cannot determine it for ASIA-1000 and ASIA-3000. In addition, the other methods give between three to six erroneous edges. In Table IV, we present the experimental results comparisons among the five algorithms for ALARM-1000, ALARM-2000, ALARM-3000, ALARM-5000 and ALARM-10000.

TABLE III. STRUCTURES COMPARISONS AMONG FIVE ALGORITHMS ON ASIA NETWORK

Cases	Edge type	GIT	NDPSO-BN	Ko and Kim	Tabar et al.	Ai
1000	CE	<b>7</b>	-	5	4	4
	DE	<b>0</b>	1	0	0	1
	RE	<b>1*</b>	0	3	4	2
	AE	<b>0</b>	0	1	0	3
	SD	<b>1</b>	1	4	4	6
2000	CE	<b>7</b>	-	5	5	4
	DE	<b>0</b>	-	0	0	1
	RE	<b>1</b>	-	3	3	2
	AE	<b>0</b>	-	1	0	3
	SD	<b>1</b>	-	4	3	6
3000	CE	<b>7</b>	-	5	5	4
	DE	<b>0</b>	1	0	0	1
	RE	<b>1*</b>	0	3	3	2
	AE	<b>0</b>	0	1	0	3
	SD	<b>1</b>	1	4	3	6
5000	CE	<b>7</b>	-	5	5	4
	DE	<b>0</b>	-	0	0	1
	RE	<b>1</b>	-	3	3	1
	AE	<b>1</b>	-	1	1	3
	SD	<b>2</b>	-	4	4	6
10000	CE	<b>7</b>	-	5	6	5
	DE	<b>0</b>	-	0	0	1
	RE	<b>1</b>	-	3	3	1
	AE	<b>1</b>	-	1	1	3
	SD	<b>2</b>	-	4	4	5

TABLE IV. STRUCTURES COMPARISONS AMONG FIVE ALGORITHMS ON ALARM NETWORK

Cases	Edge type	GIT	NDPSO-BN	Ko and Kim	Tabar et al.	Ai
1000	CE	34*	-	38	38	23
	DE	11	2	4	2	3
	RE	1	1	4	8	28
	AE	4*	2	9	4	34
	SD	16	6	17	14	59
2000	CE	34*	-	39	39	23
	DE	11	2	2	1	3
	RE	1*	0	4	8	21
	AE	4*	2	9	4	34
	SD	16	4	15	13	55
3000	CE	34	-	-	-	-
	DE	11	1	-	-	-
	RE	1	0	-	-	-
	AE	4	1	-	-	-
	SD	16	3	-	-	-
5000	CE	33	-	40	41	24
	DE	12	1	2	1	2
	RE	1*	0	4	8	21
	AE	4*	1	13	7	32
	SD	17	2	19	16	55
10000	CE	33	-	40	41	24
	DE	12	-	2	1	2
	RE	1	-	4	8	20
	AE	4	-	15	7	30
	SD	17*	-	21	16	52

From the first observation, we can demonstrate that the proposed algorithm produces sensitive results when increasing the dataset's size. Besides, we obtain the lowest or the second best number of accidentally RE and AE for ALARM-1000, ALARM-2000, ALARM-5000 and ALARM-10000 (Table IV). The proposed GIT algorithm cannot extract the correct number of correct edges and gives thirty four or thirty three CE and eleven or twelve DE. For ALARM network for 1000 and 2000 cases, our method produces the second greatest number of CE. Moreover, the results presented above allows us to declare that the GIT algorithm learns the BNs' topologies with sensitivity to the increasing of the number of cases. In the next section, we will use the proposed BN to model the features of diabetes dataset and the extracted causality relationships which represent the main factor for helping in the diabetes diagnostics.

#### VI. APPLICATION OF GIT ALGORITHM FOR THE DIABETES DIAGNOSTICS

Data classification techniques have an important role in medical field. These intelligent techniques help physicians to

analyse and explore large amount of datasets. In our case study, as explained above 47.7% of diabetes patients are not diagnosed. Therefore, basing on the probabilistic graphical model, we aim to represent the cause-effect relationships between the characteristic features in the diabetes dataset. In Table V, we introduce the features description and the used samples (for training and test) in the diabetes dataset.

The proposed GIT algorithm is implemented using FULLBNT project in Matlab.

The application of our proposal in the training diabetes dataset (368 samples) allows the generation of the structure shown in Fig. 7 in which the class node A1Cg represents the parent node for all given variables. These extracted dependency relationships means that being diabetic affects directly or indirectly the rest of the used features. In addition, the calculated K2 score of the generated graph is -99543,25.

The directed acyclic graph reported in Fig. 7 describes the dependency relationships between the used variables of the diabetic dataset. Specifically, the class variable (A1Cg) has a direct connection with CIMT, PT SPT, Ba and AgeG variables. The age, A1C and DiP nodes are connected to the A1Cg variable through CIMT node. Furthermore, the rest of the variables are connected to the main variable through the nodes 1 and 6. Once these connections are broken, the physician cannot analyse correctly the cause and effect relationships. The efficiency of our GIT algorithm has to be validated and improved basing on the expert knowledge. Indeed, completing the BN model construction with the conditional-probability tables allows the provability of our proposal's importance. Moreover, this latter can be demonstrated relating to the GIT algorithm's ability in the improvement of the classification of results.

TABLE V. USED DATASET DESCRIPTION

Feature No	Feature description	Range	
1	CIMT	0.40-0.90	
2	A1C	4.5-11	
3	AgeG	1-6	
4	Age	18-72	
5	RI	0.52-0.85	
6	SPT	125-255	
7	PT	0.59-0.92	
8	DiP	0.50-0.78	
9	ba	0.52-0.80	
10	PPT	93.75-191.25	
11	DT	218.75-446	
12	SP	0.61-0.94	
13	A1Cg	Class: Diabetic or Not diabetic	
Sample	Training	368	80%
	Test	92	20%

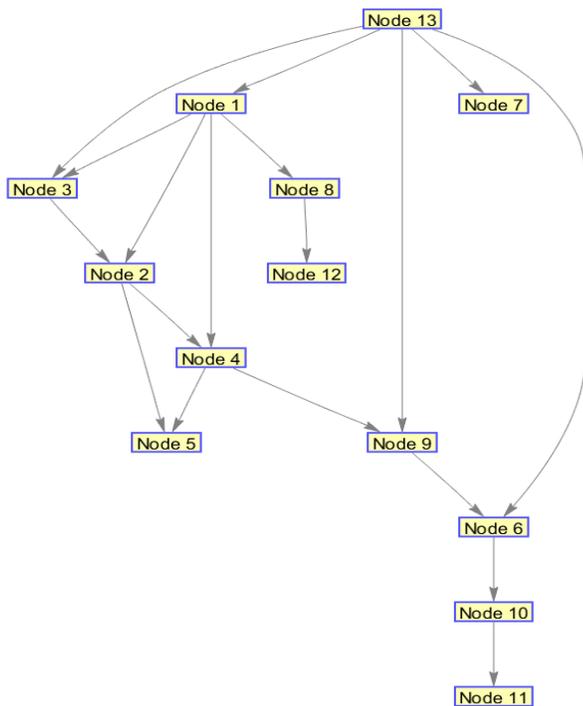


Fig. 7. DAG of the Diabetic Dataset.

## VII. CONCLUSIONS

In this paper, we propose a novel algorithm based on the Information Theory and the Graph Theory in order to solve the Bayesian network structure learning problem. Furthermore, testing the GIT algorithm on the well-known networks produced important results which were compared to four proposed algorithms.

The gained results exhibit the efficiency of our method in learning the structure of small network (ASIA with 8 nodes).

For this network, our GIT algorithm is superior in terms of the correct edges detection and the erroneous edges learning. Besides, for ALARM network, our method generated acceptable results and comparing to the other algorithms, it produced the smaller number of reversed and added edges.

To summarize, our proposal represents an effective data driven method for BN structure learning. As for future works, we will complete to BN model construction to prove the effects of the learned skeleton on the classification of data. Moreover, we will concentrate on the model validation by the experts and we will further explain its efficiency for diabetes diagnostic.

## REFERENCES

- [1] Singh, N., Singh, P., & Bhagat, D. (2019). A rule extraction approach from support vector machines for diagnosing hypertension among diabetics. *Expert Systems with Applications*, 130, pp.188-205, 2019.
- [2] K. Kannadasan, E. Damodar, and K. Venkatanaresbhabu, "Type 2 diabetes data classification using stacked autoencoders in deep neural networks," *Clinical Epidemiology and Global Health*, 2018.
- [3] Nanditha, A., Ma, R. C., Ramachandran, A., Snehalatha, C., Chan, J. C. N., Chia, K. S., et al. (2016). *Diabetes in Asia and the Pacific: Implications for the global epidemic*. *Diabetes Care*, 39(3), 472–485 Retrieved from. doi:10.2337/dc15-1536.

- [4] Prasad, D. Venkata Vara, et al. "An efficient pre-processing method for improved classification of diabetics using decision tree and artificial neural network." *AIP Conference Proceedings*. Vol. 2161. No. 1. AIP Publishing LLC, 2019.
- [5] Qawqzeh, Y. K. Neural Network-based Diabetic Type II High-Risk Prediction using Photoplethysmogram Waveform Analysis. *IJACSA International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 12, 2019.
- [6] O. Gevaert, F. De Smet, E. Kirk, B. Van Calster, T. Bourne, S. Van Huffel, Y. Moreau, D. Timmerman, B. De Moor, G. Condous, "Predicting the outcome of pregnancies of unknown location: Bayesian networks with expert prior information compared to logistic regression", *Human Reproduction*, vol. 21, no. 7, pp. 1824–1831, 2006, <https://doi.org/10.1093/humrep/del083>.
- [7] Wang, J., & Liu, S. A novel discrete particle swarm optimization algorithm for solving bayesian network structures learning problem. *International Journal of Computer Mathematics*, 96(12), 2423–2440, 2019.
- [8] S. Nikolopoulos, G.T. Papadopoulos, I. Kompatsiaris, I. Patras, "Evidence-driven image interpretation by combining implicit and explicit knowledge in a bayesian network", *IEEE Trans. Syst. Man Cybern. Part B (Cybernetics)* 41, pp. 1366–1381, 2011.
- [9] B. Yet, A. Constantinou, N. Fenton, M. Neil, E. Luedeling, K. Shepherd, "A bayesian network framework for project cost, benefit and risk analysis with an agricultural development case study", *Expert Syst. Appl*, pp. 141–155, 2016.
- [10] P. Suchánek, F. Marecki, and R. Bucki, Self-learning bayesian networks in diagnosis, *Procedia Comput. Sci.* 35 (2014), pp. 1426–1435.
- [11] L. Zhang and Q. Ji, A bayesian network model for automatic and interactive image segmentation, *IEEE Trans. Image Proc. A Publ. IEEE Signal Process. Soc.* 20(9) (2011), pp. 2582–2593.
- [12] F. Liu, S.W. Zhang, W.F. Guo, Z.G. Wei, and L. Chen, Inference of gene regulatory network based on local bayesian networks, *PLoS Comput. Biol.* 12(8) (2016), pp. 1–17.
- [13] W. Buntine, "A guide to the literature on learning probabilistic networks from data," *IEEE Trans. Knowl. Data Eng.*, vol. 8, no. 2, pp. 195–210, 1996.
- [14] H. S. Sousa, F. Prieto-Castrillo, J. C. Matos, J. M. Branco, & P. B. Lourenço, "Combination of expert decision and learned based Bayesian Networks for multi-scale mechanical analysis of timber elements". *Expert Systems with Applications*, vol. 93, pp. 156-168, 2018.
- [15] M. Velikova, J.T. van Scheltinga, P.J. Lucas, M. Spaanderman, "Exploiting causal functional relationships in bayesian network modelling for personalized healthcare", *Int. J. Approximate Reasoning* 55 (1) , pp. 59–73, 2014.
- [16] Amirkhani, H., Rahmati, M., Lucas, P. J., & Hommersom, A. Exploiting experts' knowledge for structure learning of bayesian networks. *IEEE transactions on pattern analysis and machine intelligence*, 39(11), 2154–2170, 2016.
- [17] V. R. Tabar,, F. Eskandari, S. Salimi, et al. "Finding a set of candidate parents using dependency criterion for the K2 algorithm". *Pattern Recognition Letters*, vol. 111, pp. 23-29, 2018.
- [18] E. Benmohamed. H. Ltifi, M. Benayed. A Novel Bayesian Network Structure Learning Algorithm: Best Parents-Children. In proceeding. *IEEE ISKE, the 14th International Conference on Intelligent Systems and Knowledge Engineering*, 2019.
- [19] E. Benmohamed. H. Ltifi, M. Benayed. Hybrid data analysis approach based on improved K2PC algorithm and expert knowledge Application for assessing the phosphate laundry effluents impact. In proceeding. *ICDAR, International Conference on Document Analysis and Recognition*, 2020.
- [20] J. Jiang, J. Wang, H. Yu, H. Xu, Poison identification based on Bayesian network: a novel improvement on K2 algorithm via markov blanket. In *International Conference in Swarm Intelligence*. Springer, Berlin, Heidelberg, 2013, pp.173-182.
- [21] M. Scutari, C. E. Graafland & J. M. Gutiérrez, "Who learns better Bayesian network structures: Accuracy and speed of structure learning

- algorithms". *International Journal of Approximate Reasoning*, vol. 115, pp. 235-253, 2019.
- [22] J. Wang et S. Liu, "A novel discrete particle swarm optimization algorithm for solving bayesian network structures learning problem". *International Journal of Computer Mathematics*, pp. 1-18, 2019.
- [23] S. KO et DW. KIM., "An efficient node ordering method using the conditional frequency for the K2 algorithm". *Pattern Recognition Letters*, vol. 40, p. 80-87, 2014.
- [24] X. Ai, "Node importance ranking of complex networks with entropy variation", *Entropy*, vol. 19, no 7, pp. 303, 2017.

# Optimal Routing based Load Balanced Congestion Control using MAODV in WANET Environment

Kanthimathi S<sup>1</sup>, Dr JhansiRani P<sup>2</sup>

Department of Computer Science CMR Institute of Technology  
VTU Research Center, Bengaluru, India

**Abstract**—A decentralized sort of network that can allow the nodes to communicate with them lacking any central controller is Wireless Ad hoc Networks (WANET). Network Congestions can befall on account of nodes' restricted Bandwidth (BW) together with dynamic topology. Network Congestions brings about data loss as it makes the Data Packets (DP) be dropped on the network. Therefore, in order to lessen Network Congestions, it is necessary to model Congestion Control (CC) systems aimed at the WANET. Thus, this paper offers an optimal routing centered CC scheme utilizing the Modified Ad hoc on-demand Distances Vector (MAODV) Routing Protocol (RP) aimed at the WANET. Here, primarily, the Source Node (SN) together with Destination Nodes (DN) is initialized, and after that, the MAODV discovers the multiple routing paths. Subsequently, Stochastic Gradients Descent Deep Learning Neural Network (SGD-DLNN) identifies the Congestion Status (CS) of every node in the discovered paths. In addition, the MAODV allocates the traffic over the optimum congestion-free routing path if congestion befalls. The Levy Flight Based Black Widow Optimization (LF-BWO) algorithm chooses the optimal routing paths as of congestion-free paths. Centered upon path lifetime, residual energy, link cost, together with path distance, this algorithm enhances the Data Transmission (DT) performance by means of discovering a path. The experimentation's outcomes are rendered to exhibit the proposed RP's effectiveness.

**Keywords**—Routing; congestion control; Wireless Ad Hoc Networks (WANET); Modified Ad hoc on-demand Distance Vector (MAODV); Levy Flight based Black Widow Optimization (LF-BWO); Stochastic Gradient Descent Deep Learning Neural Network (SGD-DLNN)

## I. INTRODUCTION

WANETs consist of various mobile wireless nodes that could travel arbitrarily with the capacity to connect or depart the network [1]. A WANET can be utilized in various applications, namely, disaster recovery, search, and also rescue operations. The specific characteristics of WANET are asymmetry, dynamic network topology, multiple-hop communication, along with limited BW as well as energy resources [2]. Obstruction is occurred in WANETs on account of the Packet Loss (PL), and it can well be effectively reduced by involving a CC scheme, which includes a routing algorithm and flow control on a network layer [3]. The intensive streaming traffic in WANETs can result in more packet loss, longer delay, and Quality of Service (QoS)-related performance degradation caused by congestion. When the present traffic load surpasses the existing transmission ability at every point within the network, congestion takes place. Congestion has a completely adverse ramification on the

WANET's performance [4, 5]. Congestion particularly obtains the excess of node buffers, the degradation of the overall channel quality, and the increase of both loss rates and transmission delays [6].

Different methods are created, which tells the SN about the CS for augmenting the capacity of WANETs and to lessen clogging. An SN retransmits or delays the transmission in accordance with the CS. Packets are circulated evenly amongst every node which participates in transmission [7]. A series of specific congestion-related issues had been detected and also located, involving intense Throughput (TP) degradation as well as immense fairness problems [8]. The end-to-end CC has a strong reliance on round-trip time, which certainly leads to PL. In contrast, the hop-by-hop CC protocol has a faster response speed [9]. Therefore, the best way is chosen to avoid the CC. Routing is the process of choosing a suitable path from SN to DN to send DP [10]. Analysis of traditional mobile ad hoc RP shows that these protocols are not efficient for Wireless networks [11].

The utmost significant reasons of these topology-centered RP explicitly, Dynamic Sources Routing (DSR), Ad hoc on Demands Distances Vectors Routing (AODV) [12], along with Optimized Links-States Routing (OLSR) [13] is that their route uncertainty owing to the higher speed vehicle nodes [14]. Ad hoc On-Demand Multi-path Distances Vector (AOMDV) is amongst the most well-known WANET reactive-RP [15, 16, and 17]. Hence, researchers have extensively modified this protocol to enhance their performance [18]. The multipath concept is utilized by the AOMDV in the routing process. SN chooses the shortest way to a DN. The selection of congested nodes inside an active path degrades network performance which lessens Packet Delivery Ratios (PDR), TP, PL and increases overhead in the network. Congested nodes take up more power resources of the network. Therefore, to develop the performance parameters within the network, an effectual CC is needed [19, 20]. An effective Congestion Detection (CD) and optimal routing-based CC is proposed by this paper in a WANET environment.

## II. RELATED WORK

Devarajan Krishnamoorthy et al. [21] suggested an efficient CC system for MANET. An algorithm was utilized by the system to resolve the congestion problem centered on the Relative Traffic Links Matrix Routing to obtain a solution with an enhanced PDR along with decreased overhead. The selected traffic matrix technique's effectiveness was examined

by contrasting its performance with Capacity Optimized Cooperative communications (COCO). The traffic matrix method considerably enhanced the accuracy to acquire the traffic patterns on MANET as suggested by the experiments. The simulation outcomes had shown that the system performed well when contrasted to the COCO method. But the system offered a low efficiency and had a certainty environment.

R. Vadivel and V. Murali Bhaskaran [22] offered an adjustable dependable and CC protocol for MANET. The shortest route was found for effective DT among the many paths which were constructed. The congestion was identified through the employment and capability of links and paths. When congestion was detected by SN on a link along the route, it had spread traffic over the different routes by regarding the path availability threshold and used a traffic splitting function. If the congestion was not solved by a node, it signaled its neighbors based on the congestion's indication bit. The system showed that it was dependable and achieved more TPs with abridged packet drops and also overhead as per the simulation. But the system was somewhat difficult to prove the system's performance when contrasted with less existing methodologies.

Jogendra Kumar et al. [23] introduced a CC load balancing adjustable RP for a random waypoint model in MANET to decrease delay, system routing overhead, congestion, and improved the life of network in MANET. Every mobile node in the system considered the newest traffic load and preserved an estimated record for every locality in the transmitting table called the locality table. The system was contrasted with the current RP of MANET with respect to TP, end-to-end delay (EED), packet drops average jitter, PDR, and normalized routing overhead on the network. This system exceeded the existing methods, but the system was unable to identify the congestion.

M. S. Gowtham et al. [24] presented a CC and also packet recovery aimed at the cross-layer method in MANET. The characteristics of this model were localized packet recovery, deterministic, ability to trade-off efficiency, and peer-to-peer recovery. The system was able to reclaim the lost packets via storing a duplicate of the packet. Data traffic congestion rates of high as well as low priority packets were maintained by allocating priority orders to the packets. The higher priority flow would be developed to get desired access to the medium and its flow rate of low priority was altered to have a high flow rate of higher priority. Therefore, the total performance had provided a better outcome than the prevailing method.

Ammar Alhosainy et al. [25] recommended a joint optimal congestion, multiple-path routing, along with contentions control for WANET. A splitting factor was utilized by the system to replace the linearity in the relationship within each session and its multipath routes that extended earlier models to include routing over potentially multiple paths in the optimization framework. The new variable, proper transformation and the used Ohm's law analogy led to a convex and decoupled optimization framework that found the optimum solution in a distributed form. A distributed algorithm that found the best solution for general concave

utility functions was utilized by the system. The results have exhibited that the system had achieved an optimum solution when contrasted with conventional methods. But the costs of delay, queue length, along with available energy in each node were not taken into consideration, thus better route decisions were not given by the system.

Amit Sharma and Khushboo Pawar [26] presented an approach called CRAODV which was utilized for CC in mobile ad-hoc networks. The Setup process was started at each node as an agent. A process running on the node was the agent and started with the routing agent. CD was the mechanism utilized for recognizing the problem that had already occurred or else going to occur. The final action taken was the Congestion Handling / Optimal route discovery Mechanism, with which the node or the sink gave feedback to the network to take some action relative to the problem and Congestion aware scheme. This scheme was affected by hop-to-hop CD, in contrast, to end to end. The system had provided improved performance with reference to packet drop ratio as per the simulation results. But the system had focused on only '1' metric. It was not contrasted with other qualitative metrics.

### III. PROPOSED OPTIMAL ROUTING BASED CONGESTION CONTROL IN WANET

A WANET is basically a wireless network that functions free of any fixed infrastructure. Here, the nodes function both as the hosts and the routers forwarding DP. Ad hoc networks (AHN) are primarily employed in military applications, disaster recoveries, together with emergency operations owing to their self-organizing manner. The Network Congestions occurs on account of the nodes' restricted BW together with dynamic topology. If a network node or link is carrying more data than it can handle, there is a chance for Network Congestions, which will in-turn affect the communication by initiating data loss. An apt way must be adopted to model a CC system that can evade the PL on the WANET. Thus, this paper proposes a CD and optimal routing-centered CC scheme aimed at WANET. The proposed work encompasses '5' phases: i) node initialization, ii) SN and DN generation, iii) route discovery, iv) CS identification, and v) load-balanced CC centered on optimal routing path selection. These phases are elucidated below in a meticulous manner. Fig. 1 evinces the flow of the proposed congestion control system.

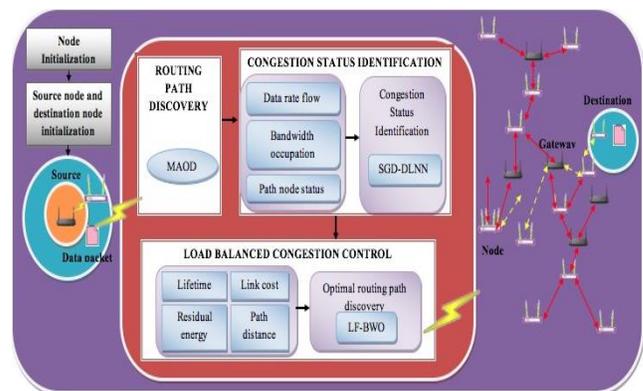


Fig. 1. Block Diagram of Proposed Congestion Control Algorithm.

A. Node Initialisation

At first, the wireless nodes along with their counts are initialized. A wireless node is basically an internet-linked device placed in the WANET, and its location along with the point of attachment to the internet might regularly be varied. The wireless node ( $N_k$ ) is exhibited as,

$$N_k = \{N_1, N_2, N_3, \dots, N_N\} \tag{1}$$

Wherein,  $N_N$  implies the n-number of wireless nodes.

B. Initialisation of Source and Destination Node

The SN along with DN is defined here. The network is self-configuring as the nodes could connect or leave it and move without restraint according to their need. If a node  $N_s$  transmits a DP to a node  $N_d$ , the SN and DN are exhibited as,

$$(N_s, N_d) \in N_k \tag{2}$$

Wherein,  $N_s$  and  $N_d$  signifies the source and destination nodes.

C. Routing Path Discovery

Here, a routing path for sending a DP as of the SN to DN is discovered. Most ADN mainly focuses on discovering a single routing path betwixt the SN and DN, which is not efficient. If the primary path breaks or NC occurs, then the intermediate nodes will immediately drop the packets since there are no alternating paths available for the destination. Thus, the proposed system finds manifold routing paths betwixt SN and DN. The proposed work employs the MAODV protocol for discovering all the probable paths to the DN. In the MAODV, the routing path discovery commences with the generation of the Route Request (R\_REQ) packet. R\_REQ packet is sent to the neighboring node once an SN wishes a path to the DN and then waits on the Route Reply (R\_REP) packet as of the DN. The R\_REQ packet format is exhibited in Table I.

TABLE I. PACKET FORMAT OF R\_REQ

Source Address	Source Sequence Number	Broadcast_id	Destination Address	Destination Sequences Number	Hop_Count
----------------	------------------------	--------------	---------------------	------------------------------	-----------

Once the neighbor node attains the R\_REQ packet, it accepts the request for instantaneous transmission. Then, a reverse path to the SN is set by means of taking the former hop of the R\_REQ as the subsequent hop. In a similar manner to the intermediate nodes, a reverse-path is set by the DN subsequent to attaining the initial copy of a R\_REQ packet. As the R\_REP advances towards the SN, it institutes a forward path to the DN at every hop. Table II evinces the packet format of R\_REP.

TABLE II. PACKET FORMAT OF R\_REP

Source Address	Destination Address	Destination Sequence Number	Hop_Count	Life_Time
----------------	---------------------	-----------------------------	-----------	-----------

An SN might get manifold R\_REP messages with disparate paths. The routing entries will be updated presuming that the R\_REP has a bigger sequence number, that is, fresh information. In MAODV, once the path is chosen, it will not be expired until the DT is finished. Thus, all the probable routing paths betwixt SN and DN are discovered.

In general, the AODV for the intention of storing routing information employs Routing Tables (RT). These encompass the subsequent fields (columns): source address, source sequence number, broadcast id, a destination address, destination sequence number, hop\_count, and life\_time. However, in the proposed work, '3' more columns: DR, Path Node (PN) status, together with BW Size are included. Here, the Mobile Agent (MA) is initialized to monitor and update the DR, PN status, and BW size of all nodes on the AODV aimed at CS identification. Thus, the MA is joined with the AODV. This protocol is labelled as MADOV. The RT of MAODV encompasses the subsequent fields:

<source\_address,source\_sequence\_number,broadcast\_id,destination\_address,destination\_sequence\_number,hop\_count,life\_time,data\_rate,bandwidth\_size,path\_node\_status>

In the MAODV, the RT is maintained on every node. The discovered multiple routing paths by means of MAODV is mathematically represented as,

$$P(R)_k = \{ P(R)_1, P(R)_2, \dots, P(R)_n \} \tag{3}$$

Wherein,  $P(R)_k$  implies the discovered routing paths and  $P(R)_n$  signifies the n-number of routing paths. The SN, by utilizing these routing paths, sends DP to DN. NC can occur at any time, which leads to PL when the number of DP reaching the node surpasses its buffer capacity. It is vital to make out the CS of every node on the routing paths beforehand to evade such congestion, which is estimated in the subsequent phase.

D. Congestion Status Identification

To find the whole traffic present across disparate routing paths, the CS of every node should be calculated which is done by this phase. The total packets in the queue at any specified time  $t$  is the Queue Load (QL) of a node. NC will befall when the QL augments. Thus, the QL ought to be kept to a least so as to evade this. It is vital to know the nodes' CS in the network for keeping the QL minimum. The proposed work utilizes '3' metrics: DR, PN status, and BW size for identifying the CS of all nodes.

1) Path node status: The MA monitors the PN-status on the base of its communication range. Here, to detect if the node is dropping or forwarding the packets, the PN-status is monitored as well as estimated.

$$N_k \xrightarrow{\text{Forwarding D with } T_i} N_{k+1} \tag{4}$$

Wherein,  $D$  signifies the data packet and  $T_i$  implies the DT time. The PN-status is identified centered on the subsequent conditions.

if  $N_k$  forward  $D$  to  $N_{k+1}$  &&  $T_d \geq T$

$$\text{Path\_Node\_Trust} = \text{Low} \quad (5)$$

if  $N_k$  drops  $D$  or  $T_d > T$

$$\text{Path\_Node\_Trust} = \text{High} \quad (6)$$

Wherein,  $T$  signifies threshold value. The proposed method has a fixed '1' threshold value, when  $T_d$  of the node is larger than that threshold value or  $N_k$  failed to forward the packet to  $N_{k+1}$ , the PN trust level is high, otherwise low.

2) *Data rate*: The total DP transmitted amid a particular time period  $t$  over a network is termed the DR. To evade congestion, there should be a balance betwixt the SN and DN by means of knowing the QL at SN and DN. The DR of the  $k$ -number of nodes is computed by,

$$\text{DR}_k = A(D) / t \quad (7)$$

Wherein,  $A(D)$  signifies the amount of DP. DR should be on the lower side for lossless packet transmission. The SN, by means of augmenting the DR, should quickly send the packets once the DP-load augments. Thus, if the DR is augmented, then the DP-load at that node is higher, which can bring about NC. Centered on a fixed threshold value, the DR status of every node is computed similar to the QL.

if  $\text{DR}_k \geq T$

$$\text{Data\_rate\_flow} = \text{High} \quad (8)$$

if  $\text{DR}_k < T$

$$\text{Data\_rate\_flow} = \text{Low} \quad (9)$$

3) *Bandwidth rate*: The potential of a particular node to send as well as receive data in a precise period of time is called the Node BW rate. Amid the DT, the QL augments once congestion happens, and when it goes beyond the threshold, the BW occupation of the specific node will be augmented. Thus, the node must have the least BW occupation for a congestion-free node. The BW of the  $k$ -number of nodes ( $BW_k$ ) is expressed mathematically as,

$$BW_k = \{BW_1, BW_2, BW_3, \dots, BW_N\} \quad (10)$$

Wherein,  $BW_N$  implies the 'N'-number of BW rate. The BW rate status is computed utilizing the subsequent conditions.

if  $BW_k \geq T$

$$\text{Bandwidth\_rate\_occupation} = \text{High} \quad (11)$$

if  $BW_k < T$

$$\text{Bandwidth\_rate\_occupation} = \text{Low} \quad (12)$$

Aimed at diverse factors like PN status, DR, and BW rate, the fixed threshold value is changed. Centered on these '3'

factors, each node's CS is identified. Every time the node receives a R\_REQ packet as of the other node, their DR and BW rate are supervised by the MA in the MAODV that updates this information into the RT. After enumerating every node's DR and BW rate, the final outcome, explicitly, the node's CS is predicted by using the Deep Learning Neural Network (DLNN).

4) *Stochastic gradient descent deep learning neural network*: DLNN originated from the Artificial Neural Network (ANN) family and it is considered to comprise more than one Hidden Layer (HL). Incrementing the number of HLs can lessen the neural network training error. The various HLs (deep learning) train themselves to process as well as study the data intensely by the filtering of information via the multiple HLs. If the neural network studies intensely, then the detection performance will automatically increment. It is the feed-forward network that is normally trained by employing the back-propagation technique. However, this back-propagation design causes higher training time. The Stochastic Gradient Descent (SGD) weight updating can be hybridized with the DLNN for evading the back-propagation issues by executing weight updating process in DLNN. Hence, the proposed scheme is called "SGD-DLNN". SGD-DLNN's common structure is showcased in Fig. 2. The proposed SGD-DLNN is trained to find the nodes' CS centered on various rules that are given in the Table III as:

For CS identification, at first, the  $DR$ , BW rate, along with the PN status values are inputted into the input layer neurons. After getting the inputted values, corresponding weight values are arbitrarily created aimed at every input. The inputted values as well as their equivalent weight values are articulated as,

$$C_k(F) = \{C_1(F), C_2(F), C_3(F), \dots, C_N(F)\} \quad (13)$$

$$C_k(F) \rightarrow \sum(DR_k, BW_k, NS_k) \quad (14)$$

$$\psi_k = \{\psi_1, \psi_2, \psi_3, \dots, \psi_N\} \quad (15)$$

Here,  $C_k(F)$  signifies the CD factors like DR, BW rate, along with the PN status, and  $\psi_k$  implies the arbitrarily initialized weight values. For evading back-propagation issue, the weight values have been initialized utilizing the SGD as,

$$\hat{\psi}_k = \psi_k + \chi \quad (16)$$

Here,  $\hat{\psi}_k$  signifies the novel weight values initialized via SGD and  $\chi$  stands for the step size that is computed as,

$$\chi = G_d * \gamma \quad (17)$$

Here,  $G_d$  implies the inputted value's gradients and  $\gamma$  signifies the learning rate. Low learning rates make the algorithm to reach nearer to the targeted output. Thus, always it is better to glue to a lesser learning rate like 0.01.

TABLE III. RULES INVOLVED IN CONGESTION STATUS PREDICTION

Rule Details			Congestion Status
Data Rate Flow	Bandwidth Occupation	Path Node Trust	
High	High	High	High Congestion
High	High	Low	High Congestion
High	Low	High	Medium congestion
High	Low	Low	High Congestion
Low	Low	Low	Medium Congestion
Low	Low	High	No Congestion
Low	High	Low	Medium Congestion
Low	High	High	Medium Congestion

After attaining the updated weight values, the inputted values  $C_k(F)$  and the novel weight values  $\hat{\psi}_k$  have been provided to the HL. Next, these '2' values are individually multiplied and after that those values are completely added in the HL.

$$\Phi(h)_k^i = \sum_{k=1}^N C_k(F) \hat{\psi}_k \quad (18)$$

Here  $\Phi(h)_k^i$  symbolizes the input of the HL. Next, the Gaussian activation function is created in the hidden nodes, which is articulated as,

$$G(\Phi(h)_k^i) = \exp(\Phi(h)_k^i)^2 \quad (19)$$

Here,  $G(\bullet)$  signifies the Gaussian activation function. The HL's output is computed centered on the  $G(\bullet)$  together with the bias value  $\phi$ .

$$\Phi(h)_k^o = \phi + \sum G(\Phi(h)_k^i) \quad (20)$$

Here,  $\Phi(h)_k^o$  implies the HL's output. At last, in the outputted layer, the total inputted signals' weights are summed aimed at obtaining the value of outputted layer neurons.

$$\Phi(o)_k^o = \phi + \sum \Phi(h)_k^o \hat{\psi}_k \quad (21)$$

Here,  $\Phi(o)_k^o$  signifies the classifier output unit that comprises '3' classes: High congestion, medium congestion, and low congestion. Centered on the rules mentioned above, each node's CS is identified. After that, the load-balanced CC is done to evade PL.

### E. Load Balanced Congestion Control

The routing protocol's potential to balance the traffic amid the multiple routing paths is called Load balancing. If the SN desires to converse with the DN, it examines its RT aimed at a valid routing path to the DN. If it is identified, the MAODV examines the congestion status of the PN utilizing the SGD-DLNN. If congestion is present in any node, the paths that

comprise those congested nodes are evaded aimed at the upcoming packet transmission until the attainment of standard traffic condition. The MADOV begins to distribute the traffic over the other congestion-free paths for attaining the normal traffic condition aimed at evading congestion. For achieving a lossless packet transmission, minimal transmission delay, minimal energy consumption, along with the maximal TP, the routing paths must be highly energy-efficient, consistent and shortest as of the SN to the DN. Hence, for obtaining an optimal routing path, the proposed MADOV employs LF-BWO Algorithm.

An optimal routing path discovery is employed aimed at spotting the effective link quality path for transferring data as of the SN towards the DN. The LF-BWO technique is implemented aiming at the optimal routing path discovery. The proposed LF-BWO chooses the optimal path centered on the factors namely lifetime, link cost, residual energy, and route distance, which are elucidated as,

1) *Life time*: The lifetime of routing path is alternatively stated as to which extent the path survives in the entire network that is enumerated as,

$$L_f = \rho(L(t_0) + L(t_0 + t_{\max})); \quad t_{\max} = t_{p1p3} \quad (22)$$

Here,  $\rho(L(t_0) + L(t_0, t_{\max}))$  signifies the probability that the path continuously will be available as of time  $t_0$  to  $(t_0 + t_{\max})$ ,  $L(t_0)$  and  $L(t_0, t_{\max})$  represents the path availability whilst '2' nodes' velocity remained unaltered and altered, correspondingly and  $t_{p1p3}$  signifies the time consumed by the node  $N_1$  for travelling as of node position  $p1$  to  $p3$ .

$$L(t_0) = \exp(-2\eta t_{\max}) \quad (23)$$

$$L(t_0 + t_{\max}) = \frac{1 - \exp(-2\eta t_{\max})}{2\eta t_{\max}} + \frac{\eta t_{\max} \exp(-2\eta t_{\max})}{2} \quad (24)$$

Here,  $\eta$  stands for the carrier's wavelength.

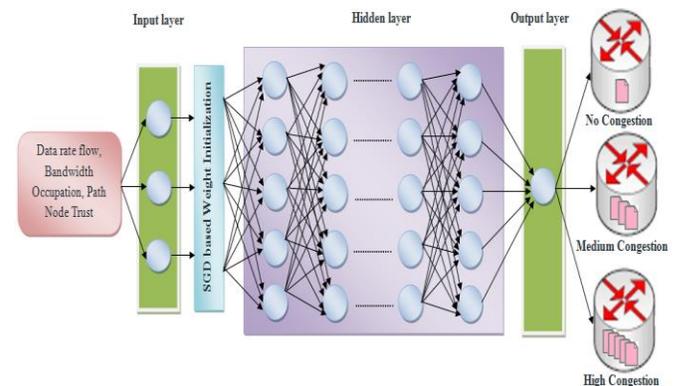


Fig. 2. Structure of SGD-DLNN.

2) *Link cost*: The Link Cost has been measured by splitting the reference BW via the interface BW. The full cost

towards the DN is the individual links' cost in the path towards destination.

$$L_c = \sum_{k=N_s}^{N_d} \left[ \frac{BW_R}{BW_I} \right]_k \quad (25)$$

Here,  $BW_R$  and  $BW_I$  represents the reference BW and interface BW.

3) *Residual energy*: The energy which stayed past the packet transmission is termed the Residual Energy, which is,

$$E_R = E_I - E_C \quad (26)$$

Here,  $E_R$  signifies the Residual Energy,  $E_I$  stands for initial energy and the  $E_C$  signifies the consumed energy throughout the DT. The  $E_C$  is articulated as,

$$E_C = N_D \times (E_T + E_P) \quad (27)$$

Here,  $N_D$  implies the number of DP and the  $E_P$  represents the energy needed aimed at packet processing and the  $E_T$  symbolizes the transmitting energy aimed at a packet that is articulated as,

$$E_T = \frac{D_s \times D_{TP}}{BW} \quad (28)$$

Here,  $D_s$  indicates the DP size,  $D_{TP}$  signifies the packet transmitting power, and the  $BW$  signifies the wireless link BW.

4) *Path distance*: The distance betwixt the SN and the DN is the route distance, which is articulated as,

$$R_{dist} = N_H(N_s, N_d) \quad (29)$$

Here,  $R_{dist}$  signifies the route distance and the  $N_H(N_s, N_d)$  represents the number of hops betwixt node  $N_s$  and  $N_d$ , respectively. The lowest hop count signifies the smallest routing path. The least distance paths offer rapid DT along with less processing time.

The '4' factors mentioned above are fixed as the fitness function aimed at the LF-BWO method for locating the optimal routing path. BWO has been enthused by the black widow spiders' distinct mating features. The BWO sustains a balance betwixt the exploitation as well as exploration phases, and also offers fast convergence speed; as well as evades the local optima issue. Nevertheless, a fast convergence speed can't be assured aimed at every databases type owing to the random parent selection. To avoid this issue, the Levy Flight (LF) distribution is utilized in the BWO algorithm for parent selection. So, the proposed protocol is termed LF-BWO.

At first, the black widow population is structure as an array that is articulated as,

$$A[Y_{widow}] = [Y_1, Y_2, Y_3, \dots, Y_N] \quad (30)$$

Here,  $A[Y_{widow}]$  signifies the population array and is regarded as  $p_{p1}$ . After that compute each black widow's fitness; in which, all black widow solution is regarded as paths. Hence, each solution's fitness is regarded as the maximum lifetime, maximum residual energy, minimum link cost, and minimum path distance, that is articulated in Eq. (31),

$$F_{optimal\ path} = \left\{ \begin{array}{ll} \max(L_f); & \text{Maximum life time} \\ \max(E_R); & \text{Maximum residual energy} \\ \min(L_c); & \text{Minimum link cost} \\ \min(R_{dist}); & \text{Minimum route distance} \end{array} \right\} \quad (31)$$

After evaluating the fitness, all candidates are sorted by their fitness value and then stocked in  $p_{p1}$ . Then parents' pairs are chosen utilizing the LF Distribution aimed at executing the procreating process. In LF-BWO's every generation, the most excellent individuals are chosen as parents  $Y_1$  and  $Y_2$  in accordance to LF Distribution.

$$L(Y) = t(-Y), \quad 1 < Y < 3 \quad (32)$$

Here,  $L(Y)$  signifies the LF Distribution. Next children pair is generated by employing the below equation,

$$off_1 = \varpi \times Y_1 + (1 - \varpi) \times Y_2 \quad (33)$$

$$off_2 = \varpi \times Y_2 + (1 - \varpi) \times Y_1 \quad (34)$$

Here,  $off_1$  and  $off_2$  represents the children pair; this procedure has been repeated aimed at  $N/2$  times. After that, the children along with the mom are sorted via their fitness value and then added on to the array ( $p_{p2}$ ). In accordance with which the number of survivors is set on, fix the cannibalism rating (CR). The fitness value is utilized for deciding the weak and strong black widows. Demolish the weaker solutions and then restore the remaining solution in the  $p_{p2}$ . After the selection of one solution as of the  $p_{p1}$ , mutate that solution's one chromosome and then create a novel solution; save the new solution in the  $p_{p3}$ . At last,  $p_{p2}$  and  $p_{p3}$  solutions are stocked in the novel array  $O_{p_p}$ .

$$O_{p_p} = p_{p2} + p_{p3} \quad (35)$$

As of the  $O_{p_p}$  array, the finest solution is chosen by analogizing each solution's fitness values. The LF-BWO method's Pseudocode is displayed below in Fig. 3.

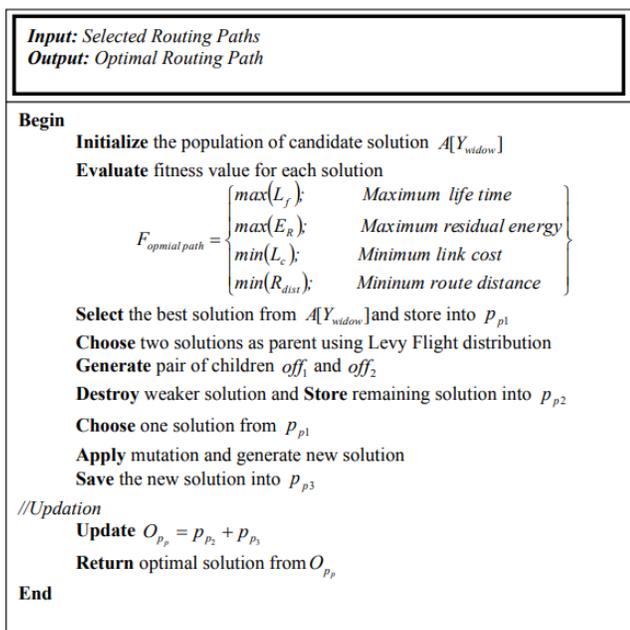


Fig. 3. Pseudocode of LF-BWO.

Thus, every path's fitness value can be analyzed and analogized with the fitness values of another path; and then the optimal routing paths are chosen centered upon the fitness values. The optimal path means the path which comprises a higher lifetime, higher energy level, low link cost, and a lesser number of hops. Priority can be offered to the energy level and lifespan. If the routing path comprises the greatest lifespan along with energy level however doesn't comprise the least link cost and distance, it is chosen nevertheless with low priority. At last, the routing process commences to spread the traffic packets over the chosen optimal paths. The packet drop is drastically evaded by transmitting DPs via the optimal congestion-free routing paths. Fig. 4 exhibits the routing path's optimal selection.

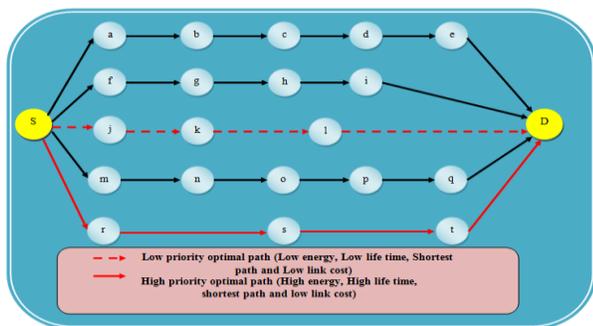


Fig. 4. Optimal Routing Path Selection.

#### IV. RESULTS AND DISCUSSIONS

Here, the proposed Congestion Control system's performance utilized aimed at PL avoidance between the SN and the DN is analyzed by performing the different experiments on the Network Simulation Tool-Version 2 (NS2). The proposed MADOV performance is weighted against few conventional existent RPs centered on a few quality metrics.

#### A. Performance Metrics

The MADOV's performance is analyzed centered on the below metrics,

- 1) Packet Delivery Ratio: It is the ratio betwixt the number of DPs received by the destination and the whole number of DP sent as of the source.
- 2) End to End Delay: It is regarded as the time that is utilized aimed at the transmission of a DP as of the SN to DN over the WANET.
- 3) Energy Consumption: Energy consumption elucidates the amount of energy consumed by the network nodes aimed at transmitting a DP as of the source towards the destination.
- 4) Throughput: TP defines the average efficient delivery of DPs to the destination in specific simulation time.
- 5) Reliability: Reliability determines the metric that calculates the system's lifespan aimed at a period. It is reciprocally proportional to the PL.

Here, the PDR, EED, energy consumption, TP, and reliability of the proposed and existent RPs are calculated and the comparative examination of proposed and existent RPs is provided below.

#### B. Comparative Performance Analysis

The experimental setup for the network is mentioned in Table IV.

The proposed MADOV's performance is weighted against the conventional RPs like the AODV-RP, DSR, Temporally Ordered Routing Algorithm (TORA), and the BW-Aware Routing Strategy (BARS) in reference to PDR, EED, energy consumption, TP, and reliability.

Fig. 5 exhibits the performance analogy of the proposed and existent RPs with regard to PDR. Whilst the PDR is high, the DP transmission's performance attains more proficiency, and the transmitted DPs are sent to the destination with no PL. The PDR is computed by changing the time as of 10ms to 50ms. In which, the MAODV attains a PDR of 95%, 95.5%, 96.2%, 96.7%, and 96.9%. However, the existent RPs attained a low PDR analogized with the MAODV. Even, no existent RP attained a PDR of more than 93%. This outcome clarified that the MAODV sent the DP to the destination successfully analogized with the other RPs.

Fig. 6 exhibits the examination of the EED of the MAODV and the existent AODV, DSR, TORA, and BWRS. In the BWRS, the delay is extremely high; whereas the AODV, DSR, and TORA comprise a minimal delay than the BWRS. Nevertheless, the proposed MAODV's EED is much less than the AODV, DSR and, TORA. Aimed at various times, the EED can be incremented although the proposed MAODV's delay is less analogized with the existent RPs as the MAODV suggested the optimal routing paths aimed at communication. By utilizing the optimal paths, the transmission delay is drastically decremented. Hence, the MAODV is proficient of delivering enhanced performance over the AODV, DSR, TORA, as well as BWRS on EED.

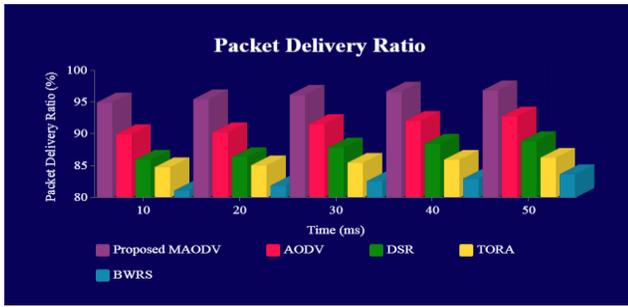


Fig. 5. Comparison of Packet Delivery Ratio for different Protocols.

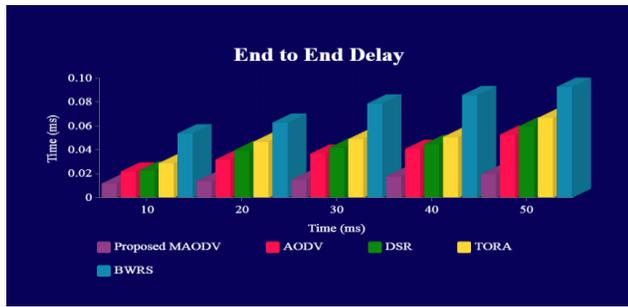


Fig. 6. Comparison of End to End Delay for different Protocols.

TABLE IV. EXPERIMENTAL SETUP

S. No	Parameters	Values
1	Simulator	NS 2
2	Network area	1500m x 1500m
3	Propagation	Two Ray Ground
4	Packet Size	500 bytes
5	Routing Protocol	MAODV
6	Speed of node	0-20 ms <sup>-1</sup>
7	Simulation time	100 s
8	Mobility Speed	2-20 m/s

Fig. 7 explicates the graphical performance examination of the proposed and existent RP in reference to energy consumption. The network’s energy consumption is calculated in terms of Jules (J). All the RPs’ energy consumption is enumerated centered on the variation of the number of nodes as of 20 to 100. The proposed MAODV’s energy consumption for 20 nodes is 1.2J, but the existent AODV, DSR, TORA, and BWRS comprise an energy consumption of 1.6J, 1.9J, 2.1J, and 2.29J that is more than the proposed RP. For efficient DT, the network’s energy consumption must be less for preventing the nodes as of a network failure. Aimed at the remaining number of nodes also, the MAODV consumes lesser energy analogized with the other RPs.

Fig. 8 exhibits the performance analogy of the MAODV and existent RPs concerning reliability. Reliability is enumerated with regards to percentage. Aimed at efficient DT’s performance, reliability must be high. Here, the reliability performance is taken aimed at the various time periods, and then the reliability is linearly augmented. Whilst reaching 50 ms, the MADOV’s reliability is 98%, but the AODV, DSR, TORA, and BWRS attain the reliability of 94%, 85%, 75%, and 73%, correspondingly. These outcomes

exposed that the network is extremely effective whilst employing the MAODV.

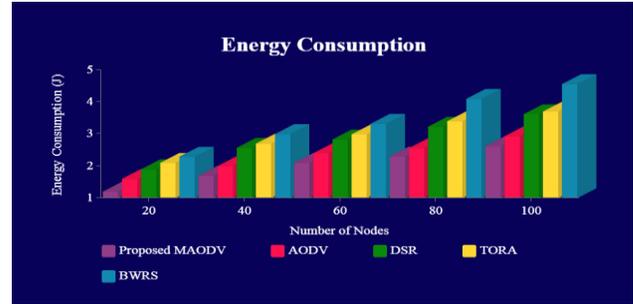


Fig. 7. Comparison of Energy Consumption for different Protocols.

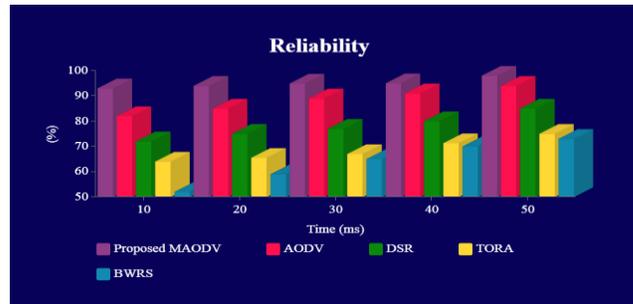
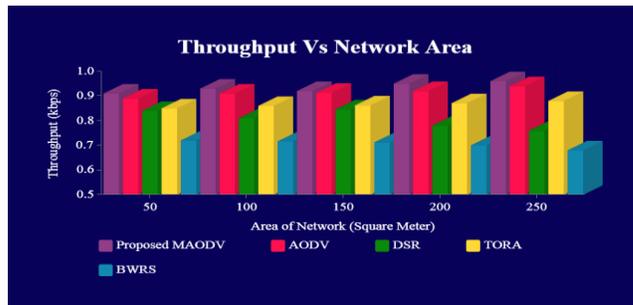


Fig. 8. Comparison of Reliability for different Protocols.



(a) Comparison of Throughput with Respect to Network Area for different Protocols.

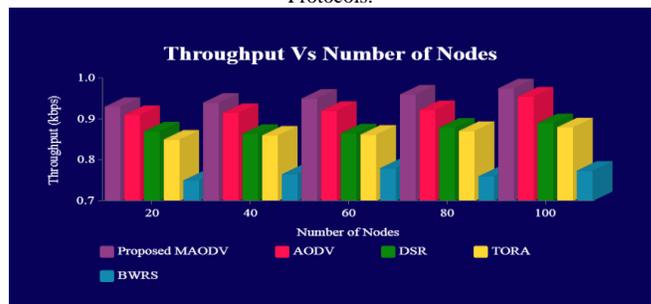


Fig. 9. (b) Comparison of Throughput with Respect to Number of Nodes for different Protocols.

Fig. 9(a) exhibits the TP analysis of the proposed with that of the prevailing protocols concerning network size. The MAODV attains a 0.93kbps TP when the number of nodes is 20. And for AODV, DSR, TORA protocol, the TP is 0.91kbps, 0.87 kbps, 0.85 kbps, and 0.75 kbps, correspondingly, whereas for BWRS, the TP is 0.75 kbps. From which, it can be said that the TP of these prevailing

protocols is lesser compared to the MAODV. The TP of MAODV is higher than others even for all the disparate nodes. And the Fig. 9(b) exhibits the TP of all the RP, which is gauged by means of differing network area. The proposed RP get a high TP compared to AODV, DSR, TORA, and BWRs protocol for disparate network area also. Thus, all the outcomes proved that the network is highly effective and consistent when utilizing MAODV.

## V. CONCLUSION

The WANET's data communication performance has been rigorously affected by the NC that gives rise to network connection loss and data PL. The optimal routing centered load-balanced congestion control utilizing the MAODV method is projected in this work aimed at the WANET environment for evading problems like this. Here, the path comprising congested nodes has been picked out and then isolated. After that, the network traffic is dispersed over the congestion-free optimal routing path employing the MAODV for evading the packet drop and attaining effective DT. The proposed protocol's performance is examined and evaluated via the analogy of its performance with the existent method's performance. The analogy's result declared that the MAODV centered network attains higher reliability, higher TP, higher delivery ratio, less energy consumption, and less end to end delay. The network's energy consumption aimed at 100 nodes employing the MAODV has been just 2.62J. The MAODV's end to end delay is 0.019ms; it obtained a 96.9% higher packet delivery ratio. This performance analogy proves that the MAODV method is much proficient aimed at suppressing the NC in WANET. The cryptographic techniques might be involved in the proposed MAODV in the upcoming days aimed at evading attacks in DT.

## REFERENCES

- [1] Nandakumar, S. D, and Thirunadana Sikamani K, "Congestion and SINR evaluation for improving traffic capacity in Ad Hoc wireless networks", In IOP Conference Series: Materials Science and Engineering, vol. 925, no. 1, pp. 012070, 2020.
- [2] Dimitris Kanellopoulos, "Congestion control for MANETs: An overview", ICT Express, vol. 5, no. 2, pp. 77-83, 2019.
- [3] Rajesh, M., and Gnanasekar J. M, "Congestion control using aodv protocol scheme for wireless ad-hoc network", Advances in Computer Science and Engineering, vol. 16, no. ½, pp. 19, 2016.
- [4] Chuang Ma, Jang-Ping Sheu, and Chao-Xiang Hsu, "A game theory based congestion control protocol for wireless personal area networks", Journal of Sensors, 2016, 10.1155/2016/6168535.
- [5] Imtiaz Mahmud, Geon-Hwan Kim, Tabassum Lubna, and You-Ze Cho, "BBR-ACD: BBR with advanced congestion detection", Electronics, vol. 9, no. 1, pp. 136, 2020.
- [6] Dionisis Kandris, George Tselikis, Eleftherios Anastasiadis, Emmanouil Panaousis, and Tasos Dagiuklas, "COALA: a protocol for the avoidance and alleviation of congestion in wireless sensor networks", Sensors, vol. 17, no. 11, pp. 2502, 2017.
- [7] Tayyaba Abdul Haq, Khwaja Mansoor, and Saba Mahmood, "Congestion avoidance adaptive routing protocol for manets using network coding", In International Conference on Communication Technologies (ComTech), IEEE, pp. 47-52, 2019.
- [8] Christian Lochert, Björn Scheuermann, and Martin Mauve, "A survey on congestion control for mobile ad hoc networks", Wireless communications and mobile computing, vol. 7, no. 5, pp. 655-676, 2007.
- [9] Jiashuai Wang, Xiaoping Yang, Ying Liu, and Zhihong Qian, "A contention-based hop-by-hop bidirectional congestion control algorithm for Ad-Hoc networks", Sensors, vol. 19, no. 16, pp. 3484, 2019.
- [10] Nousheen Akhtar, Muazzam A. Khan Khattak, Ata Ullah, and Muhammad Younus Javed, "Efficient routing strategy for congestion avoidance in MANETs", In 2017 International Conference on Frontiers of Information Technology (FIT), IEEE, pp. 305-309, 2017, 10.1109/FIT.2017.00061.
- [11] Juan Pablo Astudillo León, Thomas Begin, Anthony Busson, and J. Luis, "A fair and distributed congestion control mechanism for smart grid neighborhood area networks", Ad Hoc Networks, vol. 104, pp. 102169, 2020.
- [12] Rajesh Kumar, and Sudhir K. Routray, "Ant colony based dynamic source routing for VANET", In 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), IEEE, pp. 279-282, 2016.
- [13] Bata Krishna Tripathy, Swagat Kumar Jena, Padmalochan Bera, and Satyabrata Das, "An adaptive secure and efficient routing protocol for mobile Ad Hoc networks", Wireless Personal Communications, 2020, 10.1007/s11277-020-07423-x.
- [14] Rajesh, M., and Gnanasekar J. M, "Path observation based physical routing protocol for wireless ad hoc networks", Wireless Personal Communications, vol. 97, no. 1, pp. 1267-1289, 2017.
- [15] Masaru Yoshimachi, and Yoshifumi Manabe, "A new AODV route discovery protocol to achieve fair routing for mobile ad hoc networks", In 6th International Conference on Information Communication and Management (ICICM), IEEE, pp. 222-226, 2016.
- [16] Abdulaziz Al-Nahari, and Mohd Murtadha Mohamad, "Receiver-based ad hoc on demand multipath routing protocol for mobile ad hoc networks", Plos one, vol. 11, no. 6, pp. e0156670, 2016.
- [17] Rakesh Kumar Sahu, and Narendra S. Chaudhari, "Energy reduction multipath routing protocol for MANET using recoil technique", Electronics, vol. 7, no. 5, pp. 56, 2018.
- [18] Yefa Mai, Fernando Molina Rodriguez, and Nan Wang, "CC-ADOV: An effective multiple paths congestion control AODV", In IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, pp. 1000-1004, 2018.
- [19] Gagandeep Singh, Ashok Kumar Sharma, Onkar Singh Bawa, and Harneet Kaur, "Effective congestion control in MANET", In International Conference on Intelligent Engineering and Management (ICIEM), IEEE, pp. 86-90, 2020.
- [20] Hui Wang, Junyong Tang, and Bo Hong, "Research of wireless congestion control algorithm based on EKF", Symmetry, vol. 12, no. 4, pp. 646, 2020.
- [21] Devarajan Krishnamoorthy, Padmathilagam Vaiyapuri, Ayyasamy Ayyanar, Y. Harold Robinson, Raghendra Kumar, Hoang Viet Long, and Le Hoang Son, "An effective congestion control scheme for MANET with relative traffic link matrix routing", Arabian Journal for Science and Engineering, pp. 1-11, 2020, 10.1007/s13369-020-04511-9.
- [22] Khalid Awan, M., Nadeem Ashraf, Muhammad Qaiser Saleem, Osama E. Sheta, Kashif Naseer Qureshi, Asim Zeb, Khalid Haseeb, and Ali Safaa Sadiq, "A priority-based congestion-avoidance routing protocol using IoT-based heterogeneous medical sensors for energy efficiency in healthcare wireless body area networks", International Journal of Distributed Sensor Networks, vol. 15, no. 6, 2019, pp. 1550147719853980.
- [23] Vadivel, R., and V. Murali Bhaskaran, "Adaptive reliable and congestion control routing protocol for MANET", Wireless Networks, vol. 23, no. 3, pp. 819-829, 2017.
- [24] Jогendra Kumar, Annapurna Singh, and H. S. Bhadauria, "Congestion control load balancing adaptive routing protocols for random waypoint model in mobile ad-hoc networks", Journal of Ambient Intelligence And Humanized Computing, 2020, 10.1007/s12652-020-02059-y.
- [25] Gowtham, M. S., and Kamalraj Subramaniam, "Congestion control and packet recovery for cross layer approach in MANET", Cluster Computing, vol. 22, no. 5, pp. 12029-12036, 2019.
- [26] Ammar Alhosainy, and Thomas Kunz, "Joint Optimal Congestion, Multipath Routing, and Contention Control for Wireless Ad Hoc Networks", IEEE Communications Letters, vol. 21, no. 12, pp. 2670-2673, 2017.

# Smart Digital Forensic Framework for Crime Analysis and Prediction using AutoML

Sajith A Johnson<sup>1</sup>

M. Tech, Department of Computer Science and Engineering  
(Cyber Security and Digital Forensics), Koneru Lakshmaiah  
Education Foundation, Vaddeswaram - 522502, Guntur  
Andhra Pradesh, India

S Ananthakumaran<sup>2</sup>

Associate Professor, Department of Computer Science and  
Engineering, Koneru Lakshmaiah Education Foundation  
Vaddeswaram - 522502, Guntur  
Andhra Pradesh, India

**Abstract**—Over the most recent couple of years, the greater part of the information, for example books, recordings, pictures, clinical, forensic, criminal and even the hereditary data of people are being pushed toward digitals and cyber-dataspaces. This problem requires sophisticated techniques to deal with the vast amounts of data. We propose a novel solution to the problem of gaining actionable intelligence from the voluminous existing and potential digital forensic data. We have formulated an Automated Learning Framework ontology for Digital Forensic Applications relating to collaborative crime analysis and prediction. The minimum viable ontology we formulated by studying the existing literature and applications of Machine learning has been used to devise an Automated Machine Learning implementation to be quantitatively and qualitatively studied in its capabilities to aid intelligence practices of Digital Forensic Investigation agencies in representing, reasoning and forming actionable insights from the vast and varied collected real world data. A testing implementation of the framework is made to assess performance of our proposed generalized Smart Forensic Framework for Digital Forensics applications by comparison with existing solutions on quantitative and qualitative metrics and assessments. We will use the insights and performance metrics derived from our research to motivate forensic intelligence agencies to exploit the features and capabilities provided by AutoML Smart Forensic Framework applications.

**Keywords**—Forensic investigation; digital forensic; automated machine learning; smart forensic framework

## I. INTRODUCTION

The overall utilization of portable savvy gadgets has expanded dramatically in the course of recent decades and now is essential in the running and preservation of every aspect of our day to day life. The gadgets range from the assortment of devices that incorporate cell phones, tablets, GPS, etc. The ubiquity of these digital gadgets is expanded essentially because of their utility, immense capacities and abilities and furthermore the depreciation in their prices as production becomes cheaper. Subsequently, they can hold the huge measure of business and private client's information. These gadgets are now a fundamental aspect of our day by day life since they contain private and basic data of clients [1]. In any case, these gadgets are additionally helpless against aggressors and are regularly turning into the significant vector of crimes, IP burglary, interruptions, security dangers, counterfeit reproductions and identity theft and etc. The quantity of

advanced wrongdoings similarly increments as the new innovations, for example advanced gadgets and web increments. Therefore, these devices are turning into the vulnerable objectives for different sorts of cybercrimes and advanced assaults. However, Thanks to advancements in the field of Digital Forensics we get ways to also combat the ever encroaching aspect of criminal wrongdoing that pervades into our lives.

We will use a working definition for the term Digital Forensics Investigations (DFI) as, “The use of objective analysis toward the conservation, aggregation, validation, recognition, interpretation, documentation and representation of digital evidence got from digital sources for the intent of reconstruction of occurrences found to be illegal, or helping to predict events shown to be disruptive to peace or functioning of society”.

## II. RESEARCH PROCESS OUTLINE

Our study will be conducted in three phases:

1) Outlining a divergent meta study of the current research in the field ranging in their application potential and efficacy. This is outlined in our survey and commentary on the mentioned relevant literature on the subject. This will inform us in our second phase in finding applications and testable implementations of principles outlined. We will also use this to construct an accessible minimum viable ontology for collaborative and universal DFI practices based on the insights of the survey.

2) The assessments we made in the first phase will be used to propose architecture for our machine learning experimentations in this phase. We will describe the algorithms and review their capabilities amongst themselves. We will expand upon our methodology of collecting records of forensic & criminal data to test out the algorithms in terms of the accuracy in dealing with these large datasets.

3) From the results obtained by the techniques outlined in phase II, we conduct further review and analyses on the practicality of application and efficacy of the algorithms and also give further commentary on the contextual advantages and disadvantages of the analysed techniques. This will lead into using the learnings from the previous phases of research to implement a version of our proposed framework. We will

then use this implementation to comment on real world use case scenarios and test the practical feasibility of such a formulation of Forensic Framework after validation of proposed system along the mentioned quantitative and qualitative performance indices.

We will then finally conclude consolidating our learnings and insights during the process of our research and implementation and outline the scope and certain key directions for future research for our problem definition.

### III. LITERATURE SURVEY

Literature survey is a valuable step in software development workflows. Here we outline the general conceptions of machine learning approaches to this problem of parsing varied and voluminous digital and criminal forensic data for knowledge representation and getting actionable insights for DFI practices [2].

Knowledge Discovery shows smart computing at its finest, and is an interesting end-product of advancements in Information Technology. The ability to parse and to extract intelligence from data is a task that is of crucial importance to many fields of human development [3]. There is a lot of hidden synthesis waiting to be uncovered, this is the potential created by today's surplus of rich data. Data Mining and Knowledge Discovery Handbook, Second Edition organizes some current ideas, theories, notions, methodologies, and applications of data mining and knowledge discovery in databases (KDD) into a unified and comprehensive repository. Such KDDs provide additional intelligence utility ranging from preliminary on-field forensic assessments to mobile network flow and community cluster analysis.

Tensor Flow is an interface for expressing algorithms in machine learning and an implementation for such algorithms to be implemented. On a wide range of heterogeneous systems, from mobile devices such as phones and tablets to large-scale distributed systems with hundreds of machines and thousands of computing devices such as GPU cards, computations represented using machine learning can be performed with little to no modification, This paper describes the machine learning interface and an implementation of that interface that they have built at Google [4]. The system is versatile and may be accustomed specific a good sort of algorithms, as well as coaching and logical thinking algorithms for deep neural network models, and it's been used for conducting analysis and for deploying machine learning systems into production across over a dozen areas of engineering and alternative fields, as well as mechatronics, speech recognition, data retrieval, computer vision, natural language processing (NLP), geographic data extraction, and automated drug discovery.

Examining Deep Learning Architectures for Crime Classification and Prediction, A detailed study is presented on the classification and prediction of crime utilising deep learning architectures [5]. We analyse the efficacy of deep learning algorithms in this field and include suggestions for the design and training of deep learning systems using open data from police reports to predict areas of crime. A comparative analysis of 10 state-of-the-art methods against 3 different deep learning configurations is performed as a training data time

series of crime types per venue. We show that the deep learning-based methods consistently outperform the current best-performing methods in our experiments with five publicly accessible datasets. In addition, in the deep learning architectures, we evaluate the effectiveness of different parameters and provide insights for configuring them in order to achieve improved performance in the classification of crime and ultimately prediction of crime.

H2O is machine learning and data analysis applications. A number of well-known businesses are using H2O for their processing of big data, and over 5000 organizations are currently using it, the website states. The main things H2O brings to R and Python developers, who already feel they have all the machine learning libraries they need, are ease of use and efficient scalability for datasets that are too large to fit into a large machine's memory. One of the things that make the H2O APIs so efficient and simple to use is that a large part of their interface is common to each of the machine learning algorithms. This allows the ensemble to model different learning architectures via trained submodels [6]. H2O also offers some changes in the quality of life, such as being able to manually or parametrically stop training until the model achieves acceptable user quality. It also comes with scalable and robust algorithm implementations, such as a multitude of feature encoding options, modelling options, hyperparameter tuning, scoring, etc. These algorithms also help to exploit the advantages of cluster computing and model ensemble preparation, but H2O lacks complete support for options for GPU computing. Although the latter can be applied via Java or C++ or via the implementations of TensorFlow.

Review: From our meta study on these publications and their methodologies and proposed architectures, we will be taking some of these approaches to DFI and ensure that our proposed system will be able to provide similar capabilities. Before building the proposed system, the techniques and consideration from these papers are also taken into account for the experiment implementation and validation.

### IV. PROPOSED WORK

The assessments we made in the Literature Survey will be used to propose architecture for our machine learning experimentations in this phase. We will describe the ontology modelling and the pipeline methodology and review their capabilities. We will expand upon our methodology of collecting records of forensic & criminal data to test out the algorithms.

#### A. Operational Ontology

In each step of the process, the system is based on Machine Learning principles and uses AI to ensure that decisions made by instruments have minimal false positives. However, a 100% precise and intelligent system cannot be conceptualised, the possibilities cannot be ignored for errors and false positives. Rigorous testing before use will be needed for the working model. While user inputs can be minimised at all possible levels, it is desirable to verify at each step to avoid errors, especially the system-generated report should be validated and cross-checked with objects before it is submitted to the court of law.

An abstract representation of our proposed Smart Machine Learning Digital Forensic framework is shown in Fig. 1.



Fig. 1. Smart Digital Forensic Framework.

The proposed system is case-based and is considered to be a single package capable of resolving all three digital forensic method steps [7]. Most of the current instruments support these three measures, but they lack the rich interoperable intelligence described in our proposed system formulation, and this is the drawback we want to mitigate. Our structure is built with widely recognized traditional programming, AI and ML processes and toolkits, where existing data sets from previous forensic investigations are trained in the framework. These sets of data are useful for the system to understand what decision to take in which case. The probability of integration of AI at each point is discussed in the following subsections. In this context, the measures are called smart because they act on the basis of their knowledge and learning from it. Each phase needs to be retrained after training to see reliable outcomes. The test data sets can be used to validate the learning process and the instrument can be rigorously trained with more training data sets based on contextual performance metrics needed [11].

### B. Automated Machine Learning (AutoML)

The most important aspects of making a prediction model is being able to use domain expertise and iterated learning (either by an intelligent human agent or meta learning methods) to find out what the important features are for the prediction task and how to optimize the hyperparameters of the learning algorithms for successful learning over large databases, which cannot be pruned or cleaned by a human data scientist.

We will be using the H2O AutoML framework for our proposed implementation. It is capable of doing Categorical Ensembling in a live production environment. This allows it to effectively combine multiple trained pipelines and use the combined data of previous user runs of Smart Forensic (SF) Analysis as shown in Fig. 2, where new data is appended to trained models of previous runs.

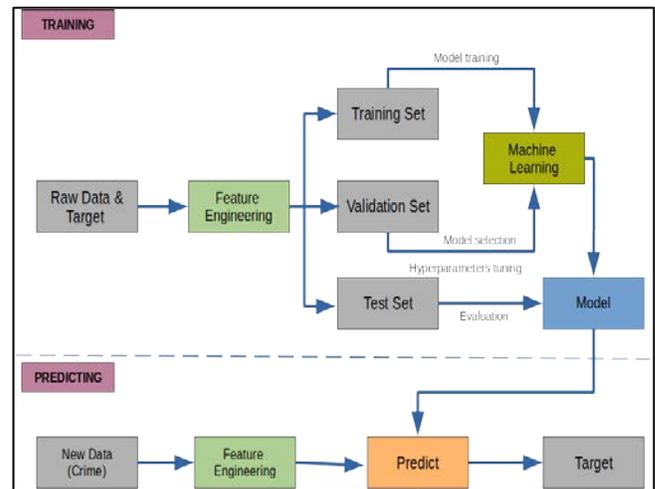


Fig. 2. Experiment Pipeline Steps.

This is where good implementations of AutoML pipelines will help us in satisfying the basic requirements for our SF framework. In addition, open-source libraries that implement AutoML techniques are available, focusing on the particular data transformations, models, and hyperparameters used in the search space and the types of algorithms used to traverse or optimise the possibilities of the search space, with the most popular being variants of Bayesian Optimization [8]. However by using H2O we also get access to state-of-the-art techniques like pruned decision trees, Gradient Boosting and even tuned Deep Learning Algorithms and advanced encoding and feature preprocessing methods.

There are hyperparameters in any machine learning system, and the most basic task in AutoML is to set these hyperparameters to optimise performance automatically.

It has capabilities to:-

- Reduce the human effort needed for machine learning to be implemented. In the sense of AutoML, this is especially important.
- Improve the efficiency of machine learning algorithms (by adapting them to the problem at hand); this has led to new state-of-the-art performances in many studies for significant machine learning benchmarks.
- Improving the reproducibility of scientific experiments and their justice. Clearly, automated HPO is more reproducible than manual search. It makes reasonable comparisons simpler since different approaches can only be equally compared if they all obtain the same degree of tuning at hand for the problem.

Fig. 3 shows the description of processes through the lens of our SF Acquisition pipeline.

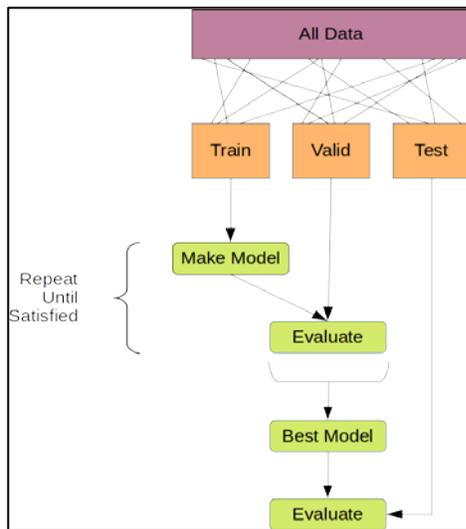


Fig. 3. SF Acquisition Pipeline.

These algorithms are also robust for transfer learning implementations and combining dataframes for better modelling and richer feature space definition derived from the merged datasets. Fig. 4 shows the overview of the server architecture used for our work.

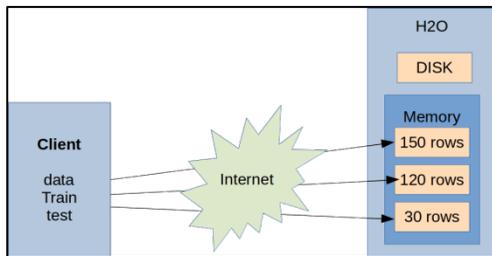


Fig. 4. Client Server Architecture.

### C. Implementation Specification

We posit that an H2O based implementation would be extremely effective for SF Analysis and SF Acquisition and by an effective user interface as per the UX pertaining to different use case and ethno-social differences. A SF application based on our ontology and framework description seems promising for the tasks of distributed data mining and forensic analysis for agencies and Investigator across all levels of hierarchy upto policy makers and field agents. As the autoML computation pipeline also supports TensorFlow which also enables distributed computing applications [9]. However, this is not supported “out of the box” and requires additional engineering to implement robustly.

H2O's REST API allows all H2O capabilities to be accessed via JSON over HTTP from an external programme or script. H2O's web interface (Flow UI), R binding (H2O-R), and Python binding are used for the rest of the API (H2O-Python).

We will use its REST API via its driverless.ai cloud implementation to construct our pipeline via the “codeless” interface provided by the proprietary driverless.ai web interface through a 2 hour evaluatory trial that can be accessed here <https://www.h2o.ai/try-driverless-ai/>.

### D. Experiment Overview

We built a LightGBM Model using Driverless AI to predict RAPE given 32 original features from the input dataset “01\_District\_wise\_crimes\_committed\_IPC\_2001\_2012.csv”. This regression experiment was completed in 41 minutes and 13 seconds (0:41:13), using 1 of the 32 original features, and 2 of the 2 engineered features.

### E. Data Overview

The dataset is obtained from [www.data.gov.in](http://www.data.gov.in), a government website; the data being provided by the National Crime Records Bureau (NCRB).

9017 rows and 13 columns of 1.3 MiB file size are included in the crime datasets we used for our experiment.

### F. Experiment Pipeline

For this experiment, Driverless AI performed the following steps (shown in Fig. 5) to find the optimal final model:

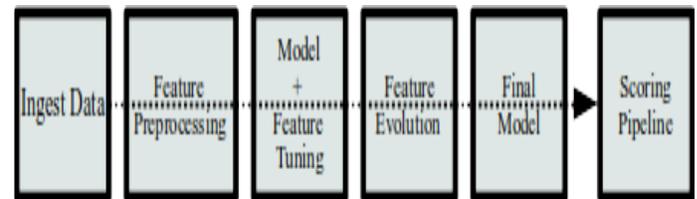


Fig. 5. Experiment Pipeline Steps.

The steps in this pipeline are described in more detail below:

- 1) *Ingest data*: detected column types
- 2) *Feature preprocessing*: turned raw features into numeric
- 3) *Model and feature tuning*: This stage combines random tuning of hyperparameters with selection and generation of characteristics. Features are modified in each iteration using variable significance as a probabilistic from the previous iteration before determining what new features to build. The best performing model and features are then passed to the feature evolution stage.
  - Identified the optimal parameters for constant, decision tree, lightgbm and xgboost methods by training models with different variables.
  - The best parameters will be those who produce the least root mean square error (RMSE) on the internal validation data.
  - To evaluate features and prediction models, 105 models were trained and scored.
- 4) *Feature evolution*: To find the best set of model parameters and feature transformations to be used in the final model, this stage uses a genetic algorithm.
  - Found the best representation of the data for the final model training by creating and evaluating 2 features over 34 iterations.

- Trained and Scored 116 models to further evaluate engineered features.

5) *Final model*: created the best model from the feature engineering iterations.

- No stacked ensemble is done because a time column was provided.

6) *Create scoring pipeline*: created and exported the Python scoring pipeline

Driverless AI trained models throughout the experiment in an effort to determine the best parameters, model dataset, and optimal final model. The processes are shown in Table I.

TABLE I. DRIVERLESS AI EXPERIMENT STAGES

Driverless AI Stage	Timing (seconds)	Number of Models
Data Preparation	20.81	0
Model and Feature Tuning	799.57	105
Feature Evolution	1,322.19	116
Final Pipeline Training	142.09	1

### G. Experiment Settings

Table II shows the settings selected for our experiment. The Defined Parameters represents the high-level parameters.

TABLE II. PARAMETERS AND SELECTED VALUES

Parameter	Value
num prediction periods	1
num gap periods	0
accuracy	7
time	5
gpus enable	True
is image	False
seed	False
is timeseries	True
is classification	False
interpretability	interpretability

### H. Supported Algorithms

We specify here the ML algorithms used as candidate models for our AutoML SF Framework which includes the following algorithms.

1) *LightGBM*: LightGBM is a Microsoft-developed gradient boosting framework that uses tree-based learning algorithms. It was specifically designed for lower memory consumption and greater performance and faster training speed. Analogous to XGBoost, it is among the highest quality implementations for gradient boosting. It also is used within Driverless AI for the fitting of Random Forest, DART (experimental algorithm), and Decision Tree approaches.

2) *XGBoost*: XGBoost is a supervised learning model that enacts a method to make accurate models called boosting.

Boosting alludes to the ensemble teaching technique of sequentially constructing many models, with each latest model attempting to rectify the inadequacies in the previous version [10]. In tree boosting, a decision tree is each new model that is added to the ensemble. XGBoost offers parallel tree boosting (identified as GBDT, GBM) that quickly and accurately accomplishes many challenges of data science. XGBoost is one of today's best gradient boosting machine (GBM) frameworks for several issues. Driverless AI implements the DART (experimental algorithm) methods of XGBoost GBM and XGBoost.

3) *Decision Tree (DT)*: A DT is a binary (single) tree model dividing the population of training data into leaf nodes (sub-groups) with consistent conclusions. No column or row sampling is undertaken, and hyper-parameters [12] monitor the depth of the tree and the growth method (depth-wise or loss-guided).

4) *Constant model*: The algorithm Constant Model predicts same constant value for any input data. By optimising the given scorer, the constant value is computed. For example, for MSE/RMSE, the constant is the target column's (weighted) mean. It is the (weighted) median for MAE. For other scorers, such as MAPE or custom scorers, an optimization process finds the constant. For classification issues, the constant probabilities are the priors identified. A constant model is considered as a baseline reference model. A warning will be issued if it ends up being used in the final pipeline, because it shows vulnerability in the dataset or target (e.g. in attempting to predict a stochastic possibility).

5) *Follow The Regularized Leader (FTRL)*: A DataTable implementation [13] of the FTRL-Proximal online learning algorithm suggested in [16] is Follow the Regularized Leader (FTRL). For parallelization, such an implementation utilises a hashing trick and a Hogwild approach [15]. For categorical targets, FTRL facilitates binomial and multinomial classification, along with regression for continuous targets.

6) *RuleFit*: Through first adapting a tree model and then fitting a Lasso (L1-regularized) GLM model, the RuleFit [14] algorithm creates an optimum set of decision rules to create a linear model composed of the most crucial tree leaves (rules).

## V. RESULTS

We will now display the quantitative metrics of our implementation's performance on the prediction and analysis tasks. Further in the discussion we will elucidate briefly on the performance of the implementation on its quantitative metrics and further comment on its capabilities and viability with respect to qualitative concerns of DFI and how our formulation fares in those regards.

### A. Model Tuning

Driverless AI automatically split the data into training and validation data, ordering the data by YEAR. The experiment predicted 131536000 seconds ahead with no gap between training and forecasting.

Table III shows the score and training time of the constant, decision tree, lightgbm and xgboost models evaluated by AI. Following table also shows the top 10 parameter tuning models evaluated, ordered based on a combination of least score and lowest training time.

TABLE III. SCORES AND TRAINING TIME OF ALGORITHMS

job order	booster	nfeatures	scores	training times
17	lightgbm	127	10.021	11.7719
10	lightgbm	39	10.0522	10.5283
1	lightgbm	38	38.2283	12.4251
3	lightgbm	33	39.3688	7.5582
19	lightgbm	116	45.1921	11.2392
21	lightgbm	98	51.531	8.3811
15	gbtree	66	58.8309	15.0382
13	lightgbm	70	60.9843	7.9107
4	gbtree	33	82.8789	6.5336
16	decision tree	77	90.2014	5.2849

More detailed information on the parameters evaluated for each algorithm is shown in the following tables, (Table IV Constant tuning, Table V Decision Tree tuning, Table VI LightGBM tuning and Table VII gbtree tuning).

B. Feature Evolution

During the Model and Feature Tuning Stage, we evaluate the effects of different types of algorithms, algorithm parameters, and features. The goal of the Model and Feature Tuning Stage is to determine the best algorithm and parameters to use during the Feature Evolution Stage.

In the Feature Evolution Stage, Driverless AI trained lightgbm models (116) where each model evaluated a different set of features. The Feature Evolution Stage uses a genetic algorithm to search the large feature engineering space. The graph in Fig. 6 shows the effect the Model and Feature Tuning Stage and Feature Evolution Stage had on the performance.

TABLE IV. CONSTANT TUNING

job order	booster	nfeatures	scores	training times
23	constant	1	215.4763	2.1245

TABLE V. DECISION TREE TUNING

tree method	grow policy	max depth	max leaves	nfeatures	scores	training times
gpu_hist	depth wise	8.0	128.0	77	90.202	5.285
gpu_hist	loss guide	6.0	128.0	58	90.205	4.977
gpu_hist	loss guide	8.0	64.0	74	90.208	5.282
gpu_hist	loss guide	10.0	128.0	91	90.268	5.299
gpu_hist	loss guide	4.0	32.0	35	90.319	4.706

TABLE VI. LIGHTGBM TUNING

tree method	grow policy	max depth	max leaves	n features	scores	training times
gpu_hist	depthwise	6.0	0.0	127	10.021	11.772
gpu_hist	depthwise	6.0	0.0	39	10.053	10.529
gpu_hist	lossguide	0.0	1024.0	38	38.228	12.426
gpu_hist	depthwise	10.0	0.0	33	39.369	7.5582
gpu_hist	depthwise	10.0	0.0	116	45.192	11.239
gpu_hist	loss guide	0.0	1024.0	98	51.531	8.3811
gpu_hist	loss guide	0.0	1024.0	70	60.985	7.9107
gpu_hist	depthwise	6.0	0.0	35	10.587	10.116
gpu_hist	depthwise	10.0	0.0	38	10.645	12.5988
gpu_hist	depthwise	6.0	0.0	35	11.566	9.3648

TABLE VII. GBTREE TUNING

tree method	grow policy	max depth	max leaves	nfeatures	scores	training times
gpu_hist	loss guide	0.0	1024.0	66	58.83	15.04
gpu_hist	depth wise	10.0	0.0	33	82.88	6.534
gpu_hist	loss guide	0.0	1024.0	111	112.49	5.176
gpu_hist	depth wise	6.0	0.0	35	26.821	23.9731

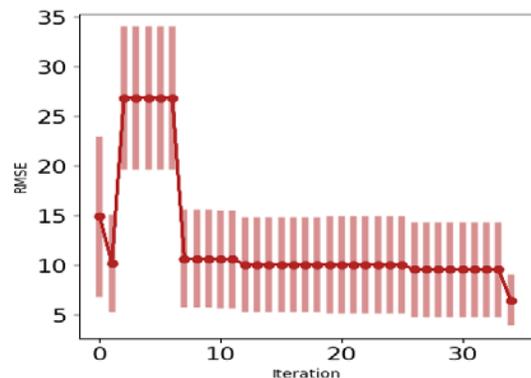


Fig. 6. Feature Evolution Graph.

C. Feature Transformations

Table VIII, ordered by value, the top features used in the final model are shown. The characteristics in the table are limited to the top 50 and are restricted to those with relative significance equal to or greater to 0.003. The function is an original column if no transformer has been applied.

TABLE VIII. TOP FEATURES USED IN FINAL MODEL

no.	Feature	Description	Transformer	Relative Importance
1	29_InteractionAdd: CUSTODIAL RAPE: OTHER RAPE	[CUSTODIAL RAPE] + [OTHER RAPE]	Interaction	1.0
2	22_OTHER RAPE	OTHER RAPE (Original)	None	0.9322
3	29_InteractionSub: CUSTODIAL RAPE: OTHER RAPE	[CUSTODIAL RAPE] - [OTHER RAPE]	Interaction	0.5503

Fig. 7 shows the bar graph of Features and Relative Feature Importance.

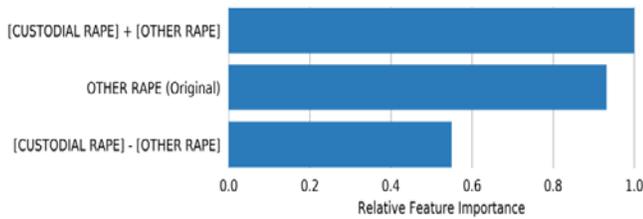


Fig. 7. Features and Relative Importance.

#### D. Final Model

Final pipeline of LightGBMModel with ensemble level is equal to 0 Transforming 30 initial characteristics. In each of 1 model, 3 characteristics each suit on time-based hold-out. Fig. 8 shows the Final Model Pipeline Feature.

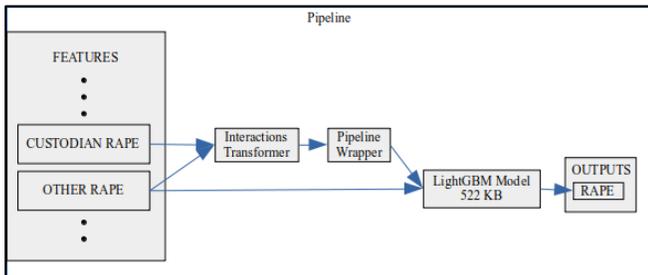


Fig. 8. Feature to Pipeline.

Details:

- The fitted features of the final model are the best features found during the feature engineering iterations.
- The target transformer indicates the type of transformation applied to the target column.

Table IX describes final model transformation details. Model Index: 0 has a weight of 1 in the final ensemble.

TABLE IX. FINAL MODEL TRANSFORMATION DETAILS

Model Index	Type	Model Weight	Fitted features	Target Transformer
0	LightGBMModel	1	3	log

TABLE X. PERFORMANCE OF FINAL MODEL

Scorer	Better score is	Final ensemble scores on validation (internal or external holdout(s)) data	Final ensemble standard deviation on validation (internal or external holdout(s)) data
RMSE	lower	6.478455	2.335938

Performance of the final model is shown in Table X. The scorer we used here is RMSE.

Fig. 9 shows the graph of performance for Actual vs predicted.

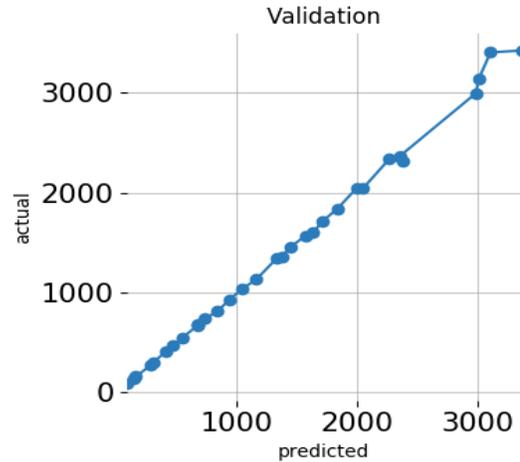


Fig. 9. Performance (Actual vs Predicted).

#### E. Alternative Models

During the experiment, we trained 27 alternative models using Driverless AI. The following Table XI shows the algorithms were evaluated during our experiment.

An array of algorithms, including but not limited to the Constant, Decision Tree, Light GBM, gbtree, XGBoost GLM, XGBoost GBM, XGBoost Dart, RuleFit, Tensorflow, and FTRL models, can be tested by Driverless AI. Table XII below illustrates why, if any, such algorithms for the final model were not chosen.

TABLE XI. DETAILS ABOUT ALGORITHMS EVALUATED IN EXPERIMENT

algorithm	package	version	documentation
constant	custom package	1.9.0	reference model that predicts a constant aimed at minimizing the given scorer
decision tree	light gbm	2.2.4	LightGBM, Light Gradient Boosting Machine. Contributors: <a href="https://github.com/microsoft/LightGBM/graphs/contributors">https://github.com/microsoft/LightGBM/graphs/contributors</a> .
lightgbm	light gbm	2.2.4	LightGBM, Light Gradient Boosting Machine. Contributors: <a href="https://github.com/microsoft/LightGBM/graphs/contributors">https://github.com/microsoft/LightGBM/graphs/contributors</a> .
gbtree	xgboost	1.1.0	XGBoost: eXtreme Gradient Boosting library. Contributors: <a href="https://github.com/dmlc/xgboost/blob/master/CONTRIBUTORS.md">https://github.com/dmlc/xgboost/blob/master/CONTRIBUTORS.md</a>

TABLE XII. DETAILS ABOUT ALGORITHM SELECTION IN FINAL MODEL

algorithm	selection
gblinear	algorithm not evaluated due to experiment configuration
rulefit	algorithm not evaluated due to experiment configuration
tensorflow	algorithm not evaluated due to experiment configuration
ftrl	algorithm not evaluated due to experiment configuration
dart	algorithm not evaluated due to experiment configuration
gbtree	Due to low performance during the model tuning process, not selected
decision tree	Due to low performance during the model tuning process, not selected
lightgbm	selected for final model

### F. Deployment

For our experiment, Python Scoring Pipelines are available for productionizing the final model pipeline for a given row of data or table of data.

Python Scoring Pipeline pack provides an assembled model and samples of the Python 3.6 code base to generate models designed with H2O Driverless AI. Below is the Python Scoring Pipeline:

- admin/h2oai\_experiment\_21c8e18c-059c-11eb-833e-0242ac110002/scoring\_pipeline/scorer.zip.

In this package, the files allow us to transform and score new data in a few different ways:

- We can import a scoring module from Python 3.6, then use the module to convert and score on updated data.
- We can use the TCP/HTTP scoring service included with this package for other applications and scripts to call the scoring pipeline module via remote procedure calls (RPC).

## VI. DISCUSSION

We have provided the quantitative measurements as a comparison between the algorithms as they offer multiple varied expressions of our SF Framework and the real world value of the three implementations but they cannot be assessed by raw performance alone [17]. However, the general improvements provided by an AutoML engine can be assessed from the quantitative results provided. There is significant improvement in training time and prediction accuracy because of the appropriate algorithm selection and hyper-parameter optimization capabilities of the AutoML engine. This also validates our assumption that H2O autoML can be a well-rounded candidate for a simple and generalized metalearner for DFI by using our SFI Framework Ontology.

The report generated by SF framework also provided the performance metrics we have referenced in this paper. This generated report demonstrates the SF Report Generation aspect of a well-rounded SF Framework. One of the main scaling problems of our traditional legal is justice and bureaucratic sluggishness. The major factor of this bottleneck is the inability of human agents involved in such institutions to process the data effectively and manually create paperwork. If we augment

the SF Reporting with scripts and templates to interface with existing legal protocols we will be able to greatly improve efficiency and efficacy of forensic agencies, with minimal feature re-tooling. Such elegant yet exhaustive SF Acquisition and SF Reporting implementation provides an easy way to bridge the gap and aid the traditional institutions to translate and transition into more appropriate mechanisms and institutions for our current needs for law enforcement and judicial systems.

Hence, we see how well our H2O implementation fares in our proof of concept in a well-rounded qualitative assessment of its capabilities in our three pronged ontology of SF Framework. We have provided the quantitative measurements as a comparison between the algorithms as they offer multiple varied expressions of our SF Framework and the real world value of the three implementations but they cannot be assessed by raw performance alone. We posit that H2O autoML provides us the most well rounded candidate for a simple and generalized metalearning for DFI by using our SFI Framework Ontology. Such smart report generation capabilities of the DFI framework is crucial in avoiding opaque and dangerous black boxes and can help illustrate the workings and reasoning behind the models learning biases. This is extremely important for real world applications in judicial or criminal and forensic use.

## VII. CONCLUSION

The topic of DFI is increasingly complex, and is blossoming to be a field that usually requires a huge abundance of complex data to be parsed and acquired from the scene of forensic interest. DFI practices include evaluating the digital evidence about the committed crime to be used as legal proof in the court of law. In this cycle, AI can be seen as an ideal way to deal with and take care of the issues that exist in the computerized criminology field. Different AI calculations and strategies can be valuable during the time spent separating and breaking down computerized proof. Automates Machine Learning Frameworks will improve this cycle by managing a lot of information in a brief timeframe range. It is clear that these improvements will be capable of providing solutions for taking vast volumes of forensic data and representing the data to make practical and highly intelligent investigative actions and prosecution decisions with a high degree of precision and good outcome consistency. In the forensic analysis phases, investigators are encouraged to use these methods as they give them the opportunity to counter various forms of crimes far beyond what is actually capable of doing so.. Well defined and minimum viable collaborative ontologies of Digital Forensic Investigations, provide avenues for advancements in the field of Machine Learning and Artificial Intelligence a way to be incorporated with ease into traditional Criminal and Forensic Agencies.

## REFERENCES

- [1] A. Guarino, "Digital forensics as a big data challenge," in ISSE 2013 securing electronic business processes: Springer, 2013, pp. 197-203.
- [2] Iqbal, Salman & Alharbi, Soltan. (2019). Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensic 10.5772/intechopen.90233. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

- [3] Maimon, Oded & Rokach, Lior. (2010). Data Mining and Knowledge Discovery Handbook, 2nd edition.
- [4] TensorFlow (2016): Large-Scale Machine Learning on Heterogeneous Distributed Systems.
- [5] Stalidis, Panagiotis & Semertzidis, Theodoros & Daras, Petros. (2018). Examining Deep Learning Architectures for Crime Classification and Prediction.
- [6] Practical Machine Learning with H2O by Darrencook, Released December 2016, Publisher(s): O'Reilly Media, Inc. ISBN: 9781491964606.
- [7] Rughani, Dr. Parag. (2017). Artificial Intelligence Based Digital Forensics Framework. International Journal of Advanced Research in Computer Science. 8. 10-14.10.26483/ijarcs.v8i8.4571.
- [8] Z. Li et al., "A Blockchain and AutoML Approach for Open and Automated Customer Service," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3642-3651, June 2019, doi:10.1109/TII.2019.2900987.
- [9] J. P. Ono, S. Castelo, R. Lopez, E. Bertini, J. Freire and C. Silva, "PipelineProfiler: A Visual Analytics Tool for the Exploration of AutoML Pipelines," in IEEE Transactions on Visualization and Computer Graphics, vol. 27, no. 2, pp. 390-400, Feb. 2021, doi: 10.1109/TVCG.2020.3030361.
- [10] Z. Wen, J. Shi, B. He, J. Chen, K. Ramamohanarao and Q. Li, "Exploiting GPUs for Efficient Gradient Boosting Decision Tree Training," in IEEE Transactions on Parallel and Distributed Systems, vol.30, no. 12, pp. 2706-2717, 1 Dec. 2019, doi: 10.1109/TPDS.2019.2920131.
- [11] Yuki, Jesia & Sakib, Md. Mahfil & Zamal, Zaisha & Habibullah, Khan & Das, Amit. (2019). Predicting Crime Using Time and Location Data. 124-128. 10.1145/3348445.3348483.
- [12] J. R. J. M. I. Quinlan, "Induction of decision trees," vol. 1, no. 1, pp. 81-106, 1986.
- [13] DataTable for Python, Z. <https://github.com/h2oai/datatable>.
- [14] J. Friedman, B. Popescu. "Predictive Learning via Rule Ensembles". 2005. <http://statweb.stanford.edu/~jhf/ftp/RuleFit.pdf>.
- [15] Niu, Feng, et al. "Hogwild: A lock-free approach to parallelizing stochastic gradient descent." Advances in neural information processing systems.2011.<https://people.eecs.berkeley.edu/~brecht/papers/hogwildTR.pdf>
- [16] McMahan, H. Brendan, et al. "Ad click prediction: a view from the trenches." Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2013. <https://research.google.com/pubs/archive/41159.pdf>.
- [17] Agarwal R., Kothari S. (2015) Review of Digital Forensic Investigation Frameworks. In: Kim K. (eds) Information Science and Applications. Lecture Notes in Electrical Engineering, vol 339. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-662-46578-3\\_66](https://doi.org/10.1007/978-3-662-46578-3_66).

# Multi-level Protection (Mlp) Policy Implementation using Graph Database

Lingala Thirupathi<sup>1</sup>, Dr. Venkata Nageswara Rao Padmanabhuni<sup>2</sup>

Research Scholar, CSE Dept, GITAM (Deemed to be University) Vizag, INDIA<sup>1</sup>

Asst. Professor, CSE Dept, Stanley College of Engineering and Technology for Women, Abids, Hyderabad, INDIA<sup>1</sup>

Professor, CSE Dept, GITAM (Deemed to be University) Vizag, INDIA<sup>2</sup>

**Abstract**—By defining and testing the Bell-LaPadula access control environment within it, this paper implements a Multi-Level Protection (MLP) lattice model architecture based on a graph database. By leveraging Bell-LaPadula security concepts and the MLP lattice model, the graph database (Neo4j) is used as a method for enforcing MLP policy. A formal structure in which Bell-LaPadula protection concepts are applied to track the information flow within a single domain after checking that the MLP lattice model is correctly represented in the graph database. Finally, we expand and improve the formal structure so that for the MLP multi-domain context, an MLP security access control policy can be defined. With the new enhanced model, we can conduct a query to verify if the subject in one domain can access the object in another domain, while a trust relationship connects the two domains.

**Keywords**—Database; graph; protection; multi-level

## I. INTRODUCTION

Information security, not only for private sectors but also for government, remains a critical component. This is clear from analyzing the serious impacts on cases such as the Marriott breach [1] as well as the US Office of Personnel Management [2][3] and the 2016 presidential election intervention.

In [4] aims to empower security with improved data transfer capabilities that are efficiently speedy and stable in an existing network. The strategy for managing traffic congestion with the help of vehicle-to-vehicle and vehicle-to-infrastructure contact is established in Real World Traffic [5]. Also in cloud computing, the use of a third part content as a trusted coprocessor is sensitively acceptable in the key works following this family [6], minimizing the outstanding role of the storage nodes [7]. In [8], social media is used primarily to deal with crisis situations, but there is not much talk about security. A model for preventing and detecting cryptographic operations in business organizations and security frameworks to avoid such attacks has been proposed [9].

A new protected approach that includes block chain, honeypot, edge or cloud computing techniques for IoT devices was proposed in [10-12] to avoid this attack by using the combination of OTP and passtext. The investigation tests for WSN in security applications have been demonstrated in [13]. Several algorithms to unpack malware using application level emulation have been proposed in [14]. They suggested an algorithm in [15] on the ideas of parallel iterative solution of linear equations and the theory of electrical networks. GBL is

an efficient supplier of a broad variety of methods and tools for tutors to use in their practices [16].

Cyber security practitioners rely heavily on comprehensive security protocols, legislation, and guidance to protect distributed networks from attacks such as these in the state. In addition, the E-Government Act (2002), the Federal Information Security Management Act (2002), and the Federal Information Security Modernization Act (2014) require certain requirements, regulations, and guidelines, such as those in the Risk Management Framework, since there is a need to create a basis for government work processes and systems [17].

In addition to the Risk Management Structure implemented by the federal government, MLP policies are often used by the public sector to allow only approved employees, systems, or processes to access resources considered sensitive. Access control rules, known as the Bell-LaPadula (BLP), must be used in order to completely use the MLP regulation. In an abstracted view through vertices and edges, a lattice model by [18] reflects such policies and we are aware of the nature of the graph database that can take advantage of such structure. These questions came to mind, therefore:

- Can MLP policies be represented in a database of graphs?
- Could the graph database detect information leaks?
- If one topic can access another object in another domain, can we query it?
- What are potential by-products of this research?

The overall consistency of the policy is affected by its brevity (e.g., length), transparency (e.g., ease of understanding), and scope (e.g., degree of guidance on infringement ramification), according to [19], which leads us to conclude that security policies can be interpreted differently from the original intentions of the writer.

Even a deficiency in one of the three categories listed can be challenging when it comes to enforcing the policies when perceived by security professionals, which can lead to a leak of information. In order to provide a shared basis for security policy writers and security practitioners using a graph database, certain critical policies can be visually represented.

The remaining sections of this paper are divided into five sections. Literature and topics studied in the past are reviewed

in Section 2. The MLP lattice model is introduced in Section 3 and discusses possibilities in the graph database. Section 4 presents how, by exploiting security principles in the database, information leaks can be detected between MLP domains with a pre-defined information sharing agreement. Section 5 illustrates our expanded structure that allows us to check whether an object in another domain in an MLP can be accessed by the subject in one domain. The conclusion and future work are found in Section 6.

## II. LITERATURE SURVEY

### A. Multi-Level Protection

To address MLP and Mandatory Access Control, the BLP model is used (MAC). MAC (Examples 1 and 2) is a method focused on data sensitivity, along with a need-to-know requirement, to restrict the access of an object from a subject.

There is also the BLP model [20] which restricts the flow of information from a lower security label to a higher security label to only flow upward to mitigate compromising information confidentiality.

A previous study was carried out to formally make the structure of MLP as a lattice model [18], shown in Fig. 1, which defines the properties of BLP. The MLP is commonly used by the federal government agencies and third-party defense procurement industries in the United States to allow access to classified information.

With vertices linked by edges, the structure of the lattice model is created. Two sets of vertices with different colors were also differentiated by their levels in Fig. 1. Vertices covering the red region are marked as top secret or "TS" and vertices covering the orange region are marked as secret or "S".

Two components consist of protection labels (SL(Si,Ci)). A degree of sensitivity is the first part (Example 1). Sensitivity level has a spectrum from "Unclassified" to "Classified" to "Secret" and "Top Secret" and countries and organizations have a common hierarchy structures which are connected by the risk of the information being revealed [21].

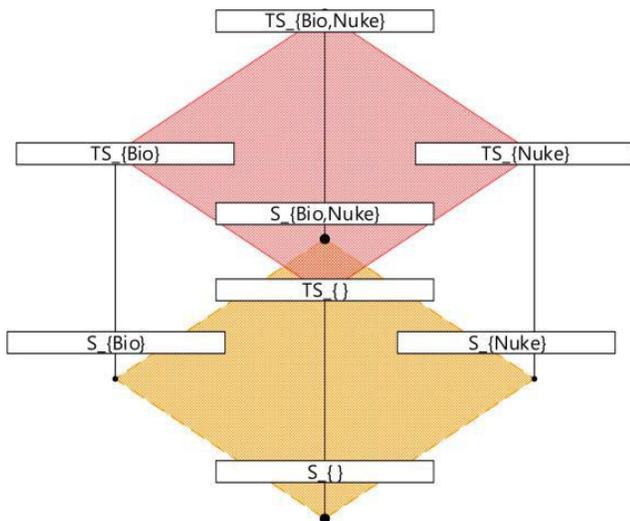


Fig. 1. Lattice Model.

Example 1: TS {} is considered to be a higher classification than S {} or TS {} S {}, based on Fig 1. Therefore, TS {} is able to read from S {} and S {} can write to TS {}, allowing knowledge to flow from a lower classification to a higher classification. At the same time, TS{} is unable to write down to S{} or S{} is unable to read up to TS{}, allowing knowledge to flow in reverse.

The second component is based on the component (c) known as compartments, the need to know (Example 2). A series of compartments will be associated with each sensitivity level to detail the protection mark that an individual has in possession.

Example 2: TS {} cannot read from or write to S {Nuke} on the basis of Fig. 1. While the Top Secret (TS{}) classification is greater than the Secret (S{Nuke}) classification, similar to Example 1, the TS{} classification does not need to be identified since the {Nuke} compartment is missing.

This is the second condition to be formally fulfilled as  $SL(S_i, C_i) \supseteq SL(S_j, C_k)$ , which in this instance is not met. Access becomes even more restrictive by creating compartments, such as {Nuke} or {Bio}, as if there is another layer of protection. Simply getting the highest security clearance will not give anything to a person [18].

With the two components, for two objects to be comparable, each component must satisfy a criterion indefinitely and determine to rule the other security mark  $SL(S_i, C_i) \geq SL(S_j, C_k)$  [21]. Labels such as  $SL(S_i, C_j)$  may be moved to  $SL(TS\{Bio, Chem\})$  or  $SL(TS, \{Bio, Chem\})$  or  $SL(TS)$ .

Another is if and only if  $SL(S_i) \geq SL(S_j)$  and  $SL(C_i) \supseteq SL(C_j)$  to give one security mark dominates, but if  $SL(C_i)$  is {} then it could only be considered as  $SL(S_i)$  or  $S_i$ . BLP security conditions are used to complete the Multi-Level Protection principle represented in the lattice model when the two are compared and the relationship between the two objects is proven.

In order for the two safety labels to be equivalent, as seen above, the two conditions indicated by MAC must be met (Examples 1 & 2). However, the two security properties of the BLP models need to be met in order to prevent information from leaking. Simple security property and star property are the two basic security assets.

The two properties together ensure that data flows from low to high (Fig. 2). The protection policies are based on the definition of subjects (s) and objects (o).

Simple security property (Easy protection property), the "no read up" at the same time states that an object with a security label cannot be able to read an object with a comparably higher security label. In other words, a subject(s) can read an object (o) if the object's security label (SL) is less than or equal to the subject's level [1].

$$SL(s) \geq SL(o)$$

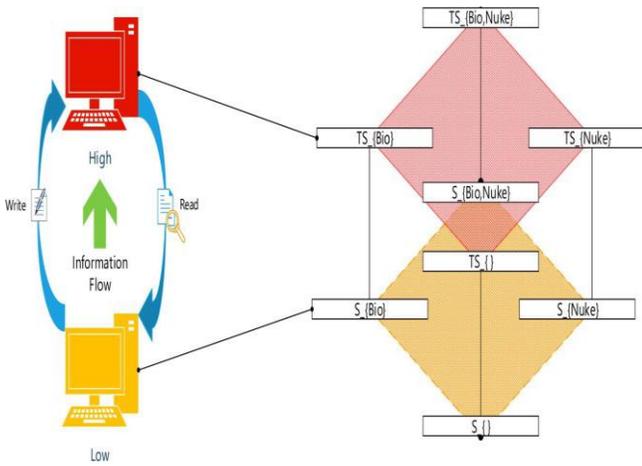


Fig. 2. Information Flow with BLP.

### B. MLP Modeling using a Graph Database

The definition of graphs dates back to the early 18th century, they laid the foundation for mathematics and the theory of graphs cGraphs, although graphs originated in mathematics, are pragmatic tools to model and analyze data. A graph consists of two components: vertices and edges.

As shown in Fig. 3, it will form a graphical relationship by connecting two vertices that represent an entity with an edge. The simple graph will produce a few sentences providing the intended information and it is possible to transmit the graph into data by observing, "John drives the blue car that his employer, the MLP Company, offers him".

A simple pragmatic theory, such as this, increases the ability of a graph database when designing and expressing access control models. The architecture itself focuses on relationships and does not use any expensive JOIN operations to measure relationships used by the SQL database [25].

#### Neo4j: Nodes, Relationships, and Graph Algorithms

Neo4j Graph database analytically supports the processing of graph data [22]. It was chosen because it uses easy-to-understand ASCII-based commands and comes with integrated tools that provide different uses for successful access. In Neo4j, in the database, the two fundamental elements that make a graph are identified as nodes (vertices) and relationships (edges).

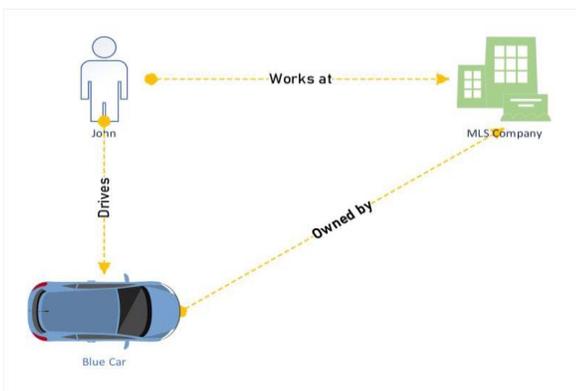


Fig. 3. A Graph Database Example.

In graph database models, nodes store data about an object, while relationships convey data about the significance between the two objects. Labels and attributes are another construct used by Neo4j to create more accurate models. Graph databases make it possible to group the nodes and explain relationships using labels. Attributes are used in depth or in a special way to define the nodes and to apply numerical measures to a relationship. The four constructs mentioned should establish a comprehensive model in order to mention details that can be ignored in abstract diagrams.

There is one limitation when developing a model, since all relationships are unidirectional, so it is important to define the direction of the relationship, but a symmetrical relationship could express a bidirectional relationship. When describing the safety status of networked systems using a symmetric relationship, a case study [23], showed a similar relationship.

According to [24], in order for two arbitrary nodes  $x$  and  $y$  with the sorted pairs of  $(x, y)$  and  $(y, x)$ , the orientation of the relationship can be directed in two separate directions.

For example,  $D_x$  marks the relationship to  $D_y$  as  $[:TRUSTS]$  in Fig. 4(a) while attempting to communicate an established trust relationship that we see in two distinct domains, and the same relationship could be expressed back by labeling  $D_y$  to have the  $[:TRUSTS]$  relationship as system  $D_x$  as seen in Fig. 4(b).

By adding examples of (a) and (b) to represent two nodes that trust each other, a symmetric  $[:TRUSTS]$  relationship can be formed between the  $D_x$  and  $D_y$  nodes shown in Fig. 4(c).

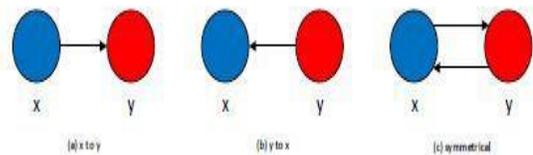


Fig. 4. Examples of Directed Graphs.

The Neo4j database comes with built-in algorithms to analyze graphical representations of physical models. The three algorithms used are path finding, centrality, and group algorithm detection [22]. One algorithm is experimented with the database after exploring the use cases of each algorithm: algorithm path finding.

The path finding algorithm is constructed in the database on top of a graph search algorithm. Path finding algorithms are used to identify optimum routes in a graph that requires quantitative values to be allocated to each relationship. Without such quantitative value for relationships, the path finding algorithm could not be used entirely, but an alternative search and log query was generated that was originally intended to store the results of a minimum spanning tree algorithm.

### III. GRAPH DATABASE FOR SPECIFYING MLP LATTICE

#### A. Lattice Model Formation Inside a Graph Database

The usability of the graph database to express MLP through two experiments will be tested in this segment.

Afterwards, logs of the direction it takes to present all available paths within the MLP lattice model will be observed via an additional Cypher query for path finding algorithms.

In the section, transitive properties will be used to formally prove that by going through pre-defined relationships, a security label (a) dominates another security label (b). Using the lattice model expressed in the Neo4j graph database, the test will be carried out in Fig. 5. To build this model, every Security Label Node was generated with three attributes: UID, Sensitivity Level, and Compartment. Furthermore, each node representing a protection label has a one-directional relationship pointing to another node, labeled “[: DOMINATES]” to demonstrate that it has a higher safety label than the other label. The MLP model was developed with the Cypher in Fig. 5.

- Create Security Labels

CREATE

```
(:Label {sensitivityLevel: 'Top Secret', compartment: 'Bio, Nuke', UID: 'TS {Bio, Nuke}'}),
```

```
(:Label {sensitivityLevel: 'Top Secret', compartment: 'Bio', UID: 'TS {Bio}'}),
```

```
(:Label {sensitivityLevel: 'Top Secret', compartment: 'Nuke', UID: 'TS {Nuke}'}),
```

```
(:Label {sensitivityLevel: 'Top Secret', compartment: ' ', UID: 'TS { }'}),
```

```
(:Label {sensitivityLevel: 'Secret', compartment: 'Bio, Nuke', UID: 'S {Bio, Nuke}'}),
```

```
(:Label {sensitivityLevel: 'Secret', compartment: 'Bio', UID: 'S {Bio}'}),
```

```
(:Label {sensitivityLevel: 'Secret', compartment: 'Nuke', UID: 'S {Nuke}'}),
```

```
(:Label {sensitivityLevel: 'Secret', compartment: ' ', UID: 'S { }'});
```

- Create Relationship with Same Compartment and Lower Level of Clearance

MATCH

```
(h:Label {sensitivityLevel: 'Top Secret'}), (l:Label {sensitivityLevel: 'Secret'})
```

WHERE h.compartment = l.compartment

CREATE (h)-[rel:DOMINATES]->(l);

- Create Relationship with Subset of Compartments

```
MATCH (h:Label {sensitivityLevel: 'Top Secret', compartment: 'Bio, Nuke'}), (l:Label {sensitivityLevel: 'Top Secret'})
```

WHERE l.compartment = 'Bio' or l.compartment = 'Nuke' CREATE (h)-[rel:DOMINATES]->(l);

```
MATCH (h:Label {sensitivityLevel: 'Top Secret'}), (l:Label {sensitivityLevel: 'Top
```

```
Secret', compartment: ' '})
```

WHERE h.compartment = 'Bio' or h.compartment = 'Nuke' CREATE (h)-[rel:DOMINATES]->(l);

```
MATCH (h:Label {sensitivityLevel: 'Secret', compartment: 'Bio, Nuke'}), (l:Label {sensitivityLevel: 'Secret'})
```

CREATE (h)-[rel:DOMINATES]->(l);

```
MATCH (h:Label {sensitivityLevel: 'Secret'}), (l:Label {sensitivityLevel: 'Secret', compartment: ' '})
```

CREATE (h)-[rel:DOMINATES]->(l);

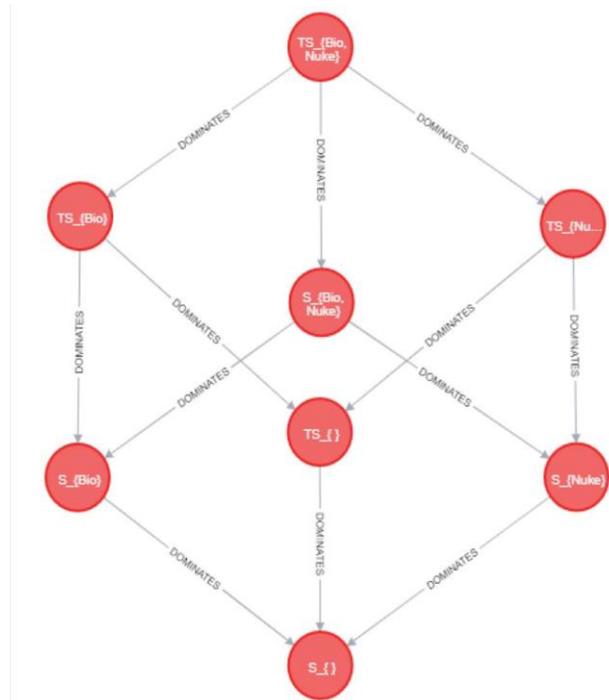


Fig. 5. MLP Model in Graph Database.

#### IV. IMPLEMENTATION OF POLICES IN MULTI-DOMAIN MLP STRUCTURE

##### A. Information Flow through Multi-Domains

For multiple areas to interact with each other, a shared trust must be established (sharing and editing confidential files). There are two steps to build trust between multiple domains. The initial step is to recognize and define the security labels each domain may use to form a relationship between the two domains. The next step is to settle on the existence of trust between the two domains. Afterwards, security violations may be identified by observing whether a loop of data flow has been formalized through trust relationships. Another domain ( $D_{CDC}$ ) was developed as a starting point in order to evaluate inter-domain collaboration test scenarios.

The object group on the left denotes  $D_{CDC}$ , and the object group on the right denotes  $D_{Army}$ . In addition, the information flow perceived in the tests is used in the graph to classify information leaks produced from diverse relationships between [ : DOMINATES ] and [ : TRUSTS ] (Fig. 7). Information flow has an inverse relation to the [ :

DOMINATES] relationship in the graph in a single domain. For instance, if a lower security label is dominated by a higher security label, the flow of information begins with the lower security label and ends with the higher security label. The result in Fig. 6 was created by entering a cypher statement that produces a flow of data in accordance with the relationship [: INFORMATION FLOW]:

```
MATCH (h:Label)-[:DOMINATES]->(l:Label)
CREATE (l)-[:INFORMATION FLOW]->(h);
```

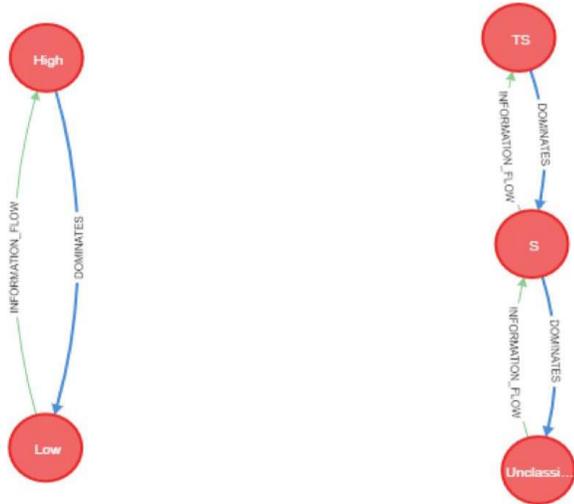


Fig. 6. Second Abstract Domain.

The final step is to identify and depend on the nature of trust (partial or full trust and one-way or two-way). This enables inter-domain mapping and allows cooperation between two domains. In Fig. 7, a matrix was formulated to explain the nature of trust that a two-domain can have in a one-way relationship. In addition, in a green arrow centered on the type of trust relationship, the information flow of each one way trust was named. As shown in Fig. 7, the [: INFORMATION FLOW] relationship is generated in accordance with how the [: TRUSTS] relationship was mapped in the database's multi-domain environment.

	One-way	Information Flow
<b>Full (Read/Write)</b>	One-way full trust X trusts Y Y can read from X Y can write to X 	One-way full trust result Info. flows from X to Y Info. flows from Y to X 
<b>Partial (Read)</b>	One-way partial (read) trust X trusts Y Y can read from X 	One-way partial (read) result Info. flows from X to Y 
<b>Partial (Write)</b>	One-way partial (write) trust X trusts Y Y can write to X 	One-way partial (write) result Info. flows from Y to X 

Fig. 7. One-Way Trust Matrix.

B. Test Scenario 1 (One-Way Full Trust)

In the graph database, a one-way, complete trust (read/write) relationship was established to reflect an incorrect inter-domain relationship (Fig. 8) to observe the flow of information. As a consequence of this wrong mapping:

- D<sub>Army</sub> Unclassified is able to read from D<sub>CDC</sub> High
- D<sub>Army</sub> Unclassified is able to write to D<sub>CDC</sub> High
- D<sub>Army</sub> Top Secret is able to read from D<sub>CDC</sub> Low
- D<sub>Army</sub> Top Secret is able to write to D<sub>CDC</sub> Low

The following Cypher statement was utilized to simulate the inter-domain relationships and information flows:

- Incorrectly Map Relationship from D<sub>CDC</sub> High to D<sub>Army</sub> Unclassified

```
MATCH (d1: Label {UID: 'High'}), (d2: Label {UID: 'Unclassified'})
```

```
CREATE (d1)-[:FULLY TRUSTS ONE WAY]->(d2);
```

- Incorrectly Map Relationship from D<sub>CDC</sub> Low to D<sub>Army</sub> Top Secret

```
MATCH (d1: Label {UID: 'Low'}), (d2: Label {UID: 'TS'})
```

```
CREATE (d1)-[:FULLY TRUSTS ONE WAY]->(d2);
```

- Create Information Flow Between D<sub>CDC</sub> and D<sub>Army</sub> by Utilizing The Wrong Mapping

```
MATCH (d1: Label)-[:FULLY TRUSTS ONE WAY]->(d2: Label)
```

```
CREATE (d1)-[:INFORMATION FLOW]->(d2), (d2)-[:INFORMATION FLOW]->(d1);
```

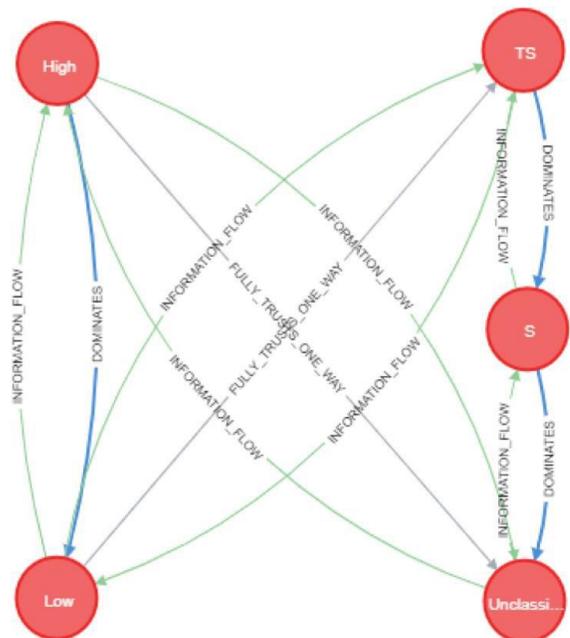


Fig. 8. Multi-Domain One-Way Full Trust.

First violation Detection (Fig. 9) and First violation Log (Fig. 10) was identified through a query if an information flow path exists from *DArmy TS* to *DArmy Unclassified* and the path was logged to identify how the violation was produced:

- Find Path

MATCH path = (: Label {UID: 'TS'})-[: INFORMATION FLOW]->(: Label {UID: 'Unclassified'})

RETURN path;

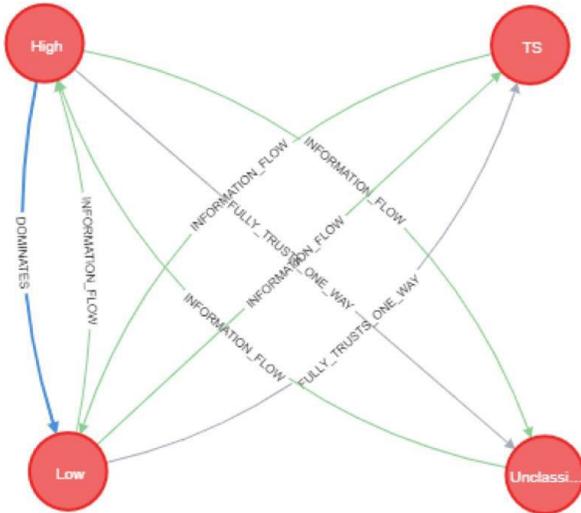


Fig. 9. Detection of First Full Trust Violation.

- Log Path

MATCH path = (h: Label {UID: 'TS'})-[: INFORMATION FLOW]->(l: Label {UID: 'Unclassified'}) WITH relationships (path) AS rels UNWIND rels AS rel WITH DISTINCT rel AS rel

RETURN startNODE(rel).UID AS source, endNODE(rel).UID AS destination;

"source"	"destination"
"TS"	"Low"
"Low"	"High"
"High"	"Unclassified"

Fig. 10. Log of First Full Trust Violation from Source to Unclassified.

A question defined a second violation if an information flow path from *D<sub>CDC</sub> High* to *D<sub>CDC</sub> Low* occurs. In this case, all nodes inside the graph were involved, so the performance looks the same as Fig. 8, and the route was logged to describe how the breach occurred:

- Find Path

MATCH path = (: Label {UID: 'High'})-[: INFORMATION FLOW]->(:Label {UID: 'Low'})

RETURN path;

- Log Path

MATCH path = (h: Label {UID: 'High'})-[: INFORMATION FLOW]->(l: Label {UID: 'Low'}) WITH relationships(path) AS rels UNWIND rels AS rel WITH DISTINCT rel AS rel

RETURN startNODE(rel).UID AS source, endNODE(rel).UID AS destination;

First violation Log (Fig. 11) is shown below.

"source"	"destination"
"High"	"Unclassified"
"Unclassified"	"S"
"S"	"TS"
"TS"	"Low"

Fig. 11. Log of First Full Trust Violation from Source to Low.

### C. Test Scenario 2 (One-Way Partial Trust to Read-Only)

One-way, partial trust (read) relationship was created in the graph database to depict an incorrect inter-domain relationship (Fig. 12). However, the mapping of *D<sub>CDC</sub> Low* to *DArmy Top Secret* provides no concern as *DArmy Top Secret* being able to read from *D<sub>CDC</sub> Low* is valid. However, a potential for an information leak will be observed as *DArmy Unclassified* is able to read from *D<sub>CDC</sub> High*. As a result of this incorrect mapping:

- DArmy Unclassified is able to read from *D<sub>CDC</sub> High*.
- DArmy Top Secret is able to read from *D<sub>CDC</sub> Low*.

The following Cypher statement was utilized to simulate the inter-domain relationships and information flows:

• Incorrectly Map Relationship from *D<sub>CDC</sub> High* to *DArmy Unclassified*.  
 MATCH (d1:Label {UID: 'High'}), (d2:Label {UID: 'Unclassified'})

CREATE (d1)-[:PARTIALLY TRUSTS ONE WAY READ ONLY]->(d2);

• Incorrectly Map Relationship from *D<sub>CDC</sub> Low* to *DArmy Top Secret*

MATCH (d1:Label {UID: 'Low'}), (d2:Label {UID: 'TS'})

CREATE (d1)-[:PARTIALLY TRUSTS ONE WAY READ ONLY]->(d2);

- Create Information Flow Between *D<sub>CDC</sub>* and *DArmy* by Utilizing the Wrong Mapping

```
MATCH (d1:Label)-[:PARTIALLY TRUSTS ONE WAY
READ ONLY]->(d2:Label)
CREATE (d1)-[:INFORMATION FLOW]->(d2);
```

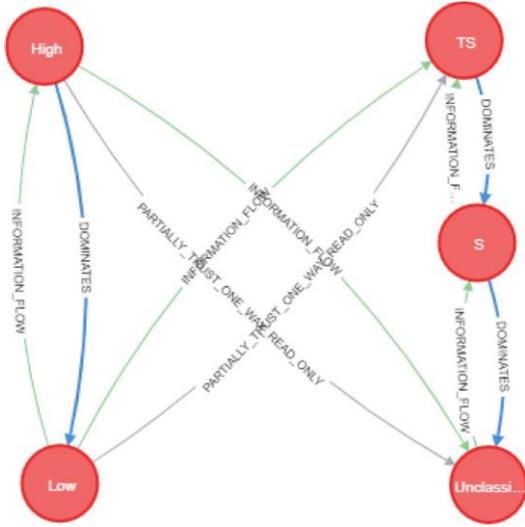


Fig. 12. Multi-Domain One-Way Trust to Read-Only.

No Information Leak Detected the MLP policies were not violated within their domains. However, the MLP policies of  $D_{CDC}$  were not upheld by  $D_{Army}$ . The lowest security label in  $D_{Army}$  (Unclassified) can obtain classified information from the highest security label from  $D_{CDC}$  (High), the entire  $D_{Army}$  can access classified information. When a query was utilized to observe all the nodes associated with the information flow to  $D_{Army}$  Unclassified, it displayed the same graph as Fig. 12.

#### D. Test Scenario (One-Way Partial Trust to Write-Only)

One-way, partial trust (read) relationship was created in the graph database to depict an incorrect inter-domain relationship. However, the mapping of  $D_{CDC}$  High to  $D_{Army}$  Unclassified being able to write to  $D_{CDC}$  High is valid. However, a potential for an information leak will be observed as  $D_{Army}$  Top Secret is able to write to  $D_{CDC}$  Low. As a result of this incorrect mapping as shown in Fig. 13:

- $D_{Army}$  Unclassified is able to write to  $D_{CDC}$  High
- $D_{Army}$  Top Secret is able to write to  $D_{CDC}$  Low

The following Cypher statement was utilized to simulate the inter-domain relationships and information flows:

- Incorrectly Map Relationship from  $D_{CDC}$  High to  $D_{Army}$  Unclassified

```
MATCH (d1: Label {UID: 'High'}), (d2: Label {UID:
'Unclassified'})
```

```
CREATE (d1)-[: PARTIALLY TRUSTS ONE WAY
WRITE ONLY]->(d2);
```

- Incorrectly Map Relationship from  $D_{CDC}$  Low to  $D_{Army}$  Top Secret

```
MATCH (d1: Label {UID: 'Low'}), (d2: Label {UID:
'TS'})
```

```
CREATE (d1)-[: PARTIALLY TRUSTS ONE WAY
WRITE ONLY] -> (d2);
```

- Create Information Flow Between  $D_{CDC}$  and  $D_{Army}$  by Utilizing the Wrong Mapping

```
MATCH (d1: Label)-[: PARTIALLY TRUSTS ONE
WAY READ ONLY]->(d2:Label)
```

```
CREATE (d2)-[: INFORMATION FLOW]->(d1);
```

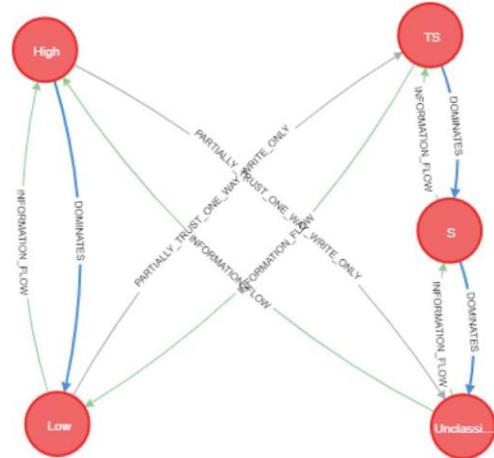


Fig. 13. Multi-Domain One-Way Trust to Write-Only.

No Information Leak Detected the MLP policies were not violated within their domains. However, the MLP policies of  $D_{Army}$  were not upheld by  $D_{CDC}$ . The lowest security label in  $D_{CDC}$  (Low) can obtain classified information from the highest security label from  $D_{CDC}$  (Top Secret), the entire  $D_{CDC}$  can access classified information.

## V. MLP MULTI-DOMAIN ACCESS CONTROL POLICY

### A. Controlled Model

By using the graph database across many methods, access control between a subject and an object can also be audited. In the following case, it is assumed that the audit protocol makes two assumptions that are in effect when the audit takes place:

- The terms of the trust agreement were decided by both parties (e.g., one-way or two-way trust and partial or full trust).
- Relationships are mapped correctly - no information leak.

From the assumption that the two conditions are met, a scenario with a skeletal model has been created to conduct the audit. Starting the model baseline to Fig. 6, the  $[:INFORMATION FLOW]$  between the security labels were initially taken out and more details were added for better interpretation as well as subjects and objects were added as an example in Fig. 14. In this scenario, *Tom* (Resource of  $D_{NSA}$ ) and *Monica* (Resource of  $D_{Army}$ ) are both subject each work for an entity (labeled as "Domain"). In this instance, *Tom* has a security level of  $D_{NSA}$  High and *Monica* has a security level of  $D_{Army}$  Secret. Objects were also added in this scenario, where *Foreign Intel File* is a resource of  $D_{NSA}$  and *Missile File* is a resource of the  $D_{Army}$  to see if objects are readable

from a subject from a different domain. The following Cypher statements were used to create the following model:

- Create correct trust mapping between *DNSA* and *DArmy*

```
MATCH (d1: Label {UID: 'High'}), (d2: Label {UID: 'TS'})
```

```
CREATE (d1)-[:PARTIAL TRUST ONE WAY READ ONLY]->(d2);
```

```
MATCH (d1: Label {UID: 'Low'}), (d2: Label {UID: 'Unclassified'})
```

```
CREATE (d1)-[: PARTIAL TRUST ONE WAY READ ONLY]->(d2);
```

- Create domain nodes

```
CREATE (: Domain {UID: 'NSA'}), (:Domain {UID: 'Army'})
```

- Attach security labels to domains

```
MATCH (d:Domain {UID: 'NSA'}), (l:Label)
```

```
WHERE l.UID = "High" OR l.UID= "Low"
```

```
MATCH (d:Domain {UID: 'Army'}), (l:Label)
```

```
WHERE l.UID = "TS" OR l.UID = "S" OR l.UID = "Unclassified"
```

```
CREATE (d)-[:SECURITY LABEL]->(l);
```

- Create subjects Tom and Monica

```
CREATE (: Subject {UID: 'Tom'}), (: Subject {UID: 'Monica'})
```

- Create objects Foreign Intel File and Missile File

```
CREATE (: Object {UID: 'Foreign Intel File'}), (:Object {UID: 'Missile File'})
```

- Create relationships between subject and objects with other nodes

```
MATCH (s:Subject {UID: 'Tom'}), (d:Domain: {UID: 'NSA'}), (l: Label {UID: 'High'})
```

```
CREATE (s)-[:RESOURCE OF]->(d), (s)-[:SECURITY LEVEL]->(l);
```

```
MATCH (s:Subject {UID: 'Monica'}), (d:Domain: {UID: 'Army'}), (l: Label {UID: 'S'})
```

```
CREATE (s)-[:RESOURCE OF]->(d), (s)-[:SECURITY LEVEL]->(l);
```

```
MATCH (s:Object {UID: 'Foreign Intel File'}), (d:Domain: {UID: 'NSA'}), (l: Label {UID: 'Low'})
```

```
CREATE (s)-[:RESOURCE OF]->(d), (s)-[:SECURITY LEVEL]->(l);
```

```
MATCH (s:Object {UID: 'Missile File'}), (d:Domain: {UID: 'Army'}), (l: Label {UID: 'S'})
```

```
CREATE (s)-[:RESOURCE OF]->(d), (s)-[:SECURITY LEVEL]->(l);
```

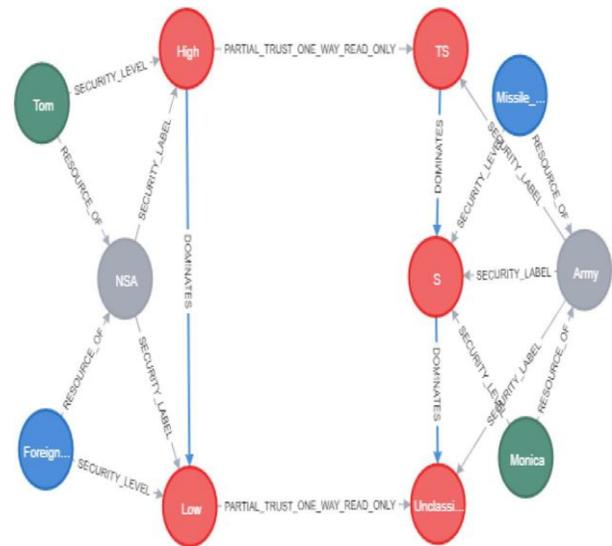


Fig. 14. Skeletal Model of Scenario.

## VI. DISCUSSIONS

To enforce, track, and audit MLP policies from a single domain to multi-domains, graph databases can be used. This conclusion was reached after exploiting the safety concepts and confidence relationships of Bell-LaPadula with the flow of knowledge inside the lattice structure. The database can not only identify errors in the policy implemented, but can also give researchers the opportunity to document the direction they took to reach a certain end point to correct the modeling problem or the policy writer's agreement. A means of formalizing written security policies can be given by modeling the MLP policies in the database.

In order to detect the most sensitive nodes in relation to MLP policy or networked systems, the spectrum of centrality algorithms can be explored. As a consequence, authorities responsible for the security, honesty and availability of information may be in a position to devote adequate limited resources to safeguard systems or information.

The study of the two-way confidence process is another potential work that can be performed. Although the principle is similar to a one-way trust agreement, two-way trust makes the exchange of knowledge even more complex and complicated. The graph database could be able to help detect errors that may have been shown to be viable by enforcing MLP policies.

## REFERENCES

- [1] Sanger, D. E., Perloth, N., Thrush, G., & Rappoport, A. (2018). Marriott data breach is traced to chinese hackers as u.s. readies crackdown on beijing. The New York Times. <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html>.
- [2] Davis, J. H. (2015). Hacking of government computers exposed 21.5 million people. <https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html>.
- [3] Koerner, B. I. (2016). Inside the cyberattack that shocked the US government. <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>.
- [4] Lingala Thirupathi and P.V. Nageswara Rao, 2020. Developing a Multi-Level Protection Framework Using EDF. International Journal of

- Advanced Research in Engineering and Technology (IJARET). Volume:11, Issue: 10, Pages: 893-902.
- [5] Lingala Thirupathi, Galipelli Ashok and Thanneru Mahesh, "Traffic Congestion Control through Vehicle-to-Vehicle and Vehicle to Infrastructure Communication", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, no. 4, pp. 5081-5084, 2014.
- [6] Reddemma, Y., Thirupathi, L., & Gunti, S. (2009). A Secure Model for Cloud Computing Based Storage and Retrieval. SIGCOMM Computer Communication Review, 39(1), 50-55.
- [7] Sunanda Nalajala, Lingala Thirupathi, N.L.Pratap,"Improved Access Protection of Cloud Using Feedback and De-Duplication Schemes ", Journal of Xi'an University of Architecture & Technology, Volume XII, Issue IV ( 2020).
- [8] Thirupathi Lingala, Sandeep Ravikanti, "Social Media: To Deal Crisis Circumstances", International Journal of Innovations & Advancement in Computer Science (IJACS), Volume 6, Issue 9 (2017).
- [9] Lingala Thirupathi, P.V. Nageswara Rao, "Understanding the Influence of Ransomware: An Investigation on its Development, Mitigation and Avoidance Techniques", GRENZE International Journal of Engineering and Technology, Issue 3, Grenze ID -01.GIJET.4.3.25, pages: 123-126.(2018)
- [10] Lingala Thirupathi, Venkata Nageswara Rao Padmanabhuni, "A Secured Framework to Identify and Mitigate Attack", International Journal of Inventive Engineering and Sciences (IJIES), ISSN: 2319-9598, Volume-5 Issue-8 (2020).
- [11] Lingala Thirupathi, Dr. Venkata Nageswara Rao Padmanabhuni, "A protected framework to detect and mitigate attacks", International journal of analytical and experimental modal analysis, volume XII, Issue-VI,(2020) Page No: 2335-2337, DOI:18.0002.IJAEMA.2020.V12I6.200001.0156858943.
- [12] V.Srividya, P.Swarnalatha, L.Thirupathi, "Practical Authentication Mechanism using PassText and OTP" in Grenze International Journal of Engineering and Technology, Special Issue,Grenze ID: 01.GIJET.4.3.27,© Grenze Scientific Society, 2018.
- [13] L. Thirupathi, G. Rekha, "Future drifts and Modern Investigation Tests in Wireless Sensor Networks" in International Journal of Advance Research in Computer Science and Management Studies, Volume 4, Issue 8 (2016).
- [14] Mr. Md. Rehaman Pasha , Mrs. Y Prathima, Mr. L. Thirupati, "Malwise System for Packed and Polymorphic Malware" in International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 167– 172 (2014),Special Issue of ICETETS.
- [15] M.Swathi, L.Thirupathi, "Algorithm For Detecting Cuts In Wireless Sensor Networks" in International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue10 (2013).
- [16] Lingala Thirupathi, MD Rehaman Pasha, Gopu Srikanth Reddy, "Game Based Learning (GBL), International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 4 (2013).
- [17] Ross, R., Pillitteri, V. Y., Dempsey, K., Takamura, E., Jacobs, J., Brewer, J., & Goren, N. (2020). Fisma background, <https://csrc.nist.gov/Papers/risk-management/detailed-overview>.
- [18] Denning, D. E. (1976). A lattice model of secure information flow. *Communications of the ACM*, 19(5), 236–243. <https://dl.acm.org/doi/pdf/10.1145/360051.360056>.
- [19] Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework, *European Journal of Information Systems*, 26(6), 605–641.
- [20] Bell, D. E. (2005). Looking back at the bell-la padula model, In *Computer security applications conference, 21st annual*. IEEE.
- [21] Focardi, R., & Gorrieri, R. (2003). *Foundations of security analysis and design: Tutorial lectures* (Vol. 2171). Springer.
- [22] Needham, M., & Hodler, A. E. (2019). *Graph algorithms: Practical examples in apache spark and neo4j*. O'Reilly Media.
- [23] Noel, S., Harley, E., Tam, K., Limiero, M., & Share, M. (2016). Cygraph: Graph-based analytics and visualization for cybersecurity. <https://doi.org/10.1016/bs.host.2016.07.001>.
- [24] Crawford, B. (2016). *Granular security in a graph database* (Master's thesis). Naval Postgraduate School Monterey United States. <https://apps.dtic.mil/dtic/tr/fulltext/u2/1027194.pdf>.
- [25] Sasaki, B. M. (2018). Graph databases for beginners: Why graph technology is the future. <https://neo4j.com/blog/why-graph-databases-are-the-future>.

# SGBBA: An Efficient Method for Prediction System in Machine Learning using Imbalance Dataset

Saiful Islam<sup>1</sup>

Computer Science & Engineering  
Chittagong University of Engineering & Technology  
International Islamic University of Chittagong  
Chattogram  
Bangladesh

Umme Sara<sup>2</sup>, Anichur Rahman<sup>4</sup>  
Dipanjali Kundu<sup>5</sup>, Mahedi Hasan<sup>8</sup>

Department of Computer Science and Engineering  
National Institute of Textile Engineering and Research  
(NITER), Dhaka  
Bangladesh

Abu Kawsar<sup>3</sup>

Department of Information and Communication  
Technology, Government Maulana Mohammad Ali College  
Tangail, Bangladesh

Diganta Das Dipta<sup>6</sup>

Department of Computer Science and Engineering,  
Chittagong University of Engineering & Technology  
Chattogram, Bangladesh

A.N.M. Rezaul Karim<sup>7</sup>

Department of Computer Science and Engineering  
International Islamic University of Chittagong  
Chattogram, Bangladesh

**Abstract**—A real world big dataset with disproportionate classification is called imbalance dataset which badly impacts the predictive result of machine learning classification algorithms. Most of the datasets faces the class imbalance problem in machine learning. Most of the algorithms in machine learning work perfectly with about equal samples counts for every class. A variety of solutions have been suggested in the past time by the different researchers and applied to deal with the imbalance dataset. The performance of these methods is lower than the satisfactory level. It is very difficult to design an efficient method using machine learning algorithms without making the imbalance dataset to balance dataset. In this paper we have designed an method named SGBBA: an efficient method for prediction system in machine learning using Imbalance dataset. The method that is addressed in this paper increases the performance to the maximum in terms of accuracy and confusion matrix. The proposed method is consisted of two modules such as designing the method and method based prediction. The experiments with two benchmark datasets and one highly imbalanced credit card datasets are performed and the performances are compared with the performance of SMOTE resampling method. F-score, specificity, precision and recall are used as the evaluation matrices to test the performance of the proposed method in terms of any kind of imbalance dataset. According to the comparison of the result of the proposed method computationally attains the effective and robust performance than the existing methods.

**Keywords**—Imbalanced dataset; sub sample; accuracy; fraud; confusion matrix; bagging

## I. INTRODUCTION

Now-a-days imbalanced classification from the two-class imbalance dataset pose a severe problem of data science and machine learning where every class has supremacy over another class. The dominant class with more data samples is

called the majority class and the other class which has fewer samples is called the minority class. This question makes the machine learning models and algorithms more skewed towards the majority class ignoring the minority class where the minority class is more relevant. In such situation, it is notably important that we should develop a method for both majority and minority class dataset without discrimination to either of the majority and minority class. For most machine learning algorithms, it is very critical to identify rare objects than common objects [27, 28]. Data mining using imbalance dataset can be used in various practical fields such as direct marketing [30], software quality prediction [29], multi object genetic sampling [1] and rare event detection such as human decision making response [2]. This is a critical factor invoked for many practical uses, such as the detection of credit card fraud, disease prediction, market share prediction etc. Without considering imbalance problem in dataset the prediction result of newly developed model and algorithm are overwhelmed through majority classification and left out via minority class. Samples of minority classes are misclassified than samples of the dominant class. Credit card fraud detection is a real-world class imbalanced problem where non frauds 99.83% and frauds 0.17% of the dataset. In this regards, the level of fraud elegance is lower than the level of non-fraud magnificence. It is in this situation that kind 1 error fee is befallen at some stage in the prediction. It means that the non-fraud is graded wrongly over the fraud. It is most important that the machine learning model should be developed properly so that the imbalance problem no more exists in the dataset. If it is failed then the model provides more accuracy that is meaningless in the data science due to result from meaningless matric. Hence this higher accuracy is no longer reliable and realistic for model performance.

## II. BACKGROUND STUDY

A variety of processes have been proposed with the aid of the researchers to resolve the imbalance dataset hassle in the machine learning getting to know. These approaches belong to the following level of solutions such as algorithms level, data level, cost sensitive and ensemble solutions. The data level solution is the most popular and widely used method that is data preprocessing based solution. Data preprocessing is performed by resampling the imbalance dataset such as oversampling or super sampling the class with minorities [3], undersampling of class with majority [4] and combining the oversampling and undersampling through bagging [8] and boosting [7] methods such as SMOTEBoost [9], RUSBoost [10], Overbagging [11], Underbagging [12]. Both oversampling and undersampling methods creates various limitations in the dataset that make the prediction result and performance unreliable.

Japkowics et al. [18] explained the effect of imbalanced dataset very nicely in the machine learning classification algorithms. She experimented and presented three different strategies such as under-sampling, resampling and recognition based scheme. The random resampling refers to the oversampling the minority class that has a bit number of samples than the majority class at random until the wide variety of samples of the minority class is matched with the majority class. Random undersampling refers to the elimination of samples from the majority class which has an enormous number of samples than the minority class until the number of majority class samples equals the number of minority class samples.

Japkowics et al. [19] combined methods of oversampling and undersampling, called hybrid method. They introduced that the test examples are graded by a measure of trust and the lift is used as the assessment criterion. In the first experiment, they oversampled the smaller samples and in the second experiment, they undersampled the greater samples. Their aggregation of oversampling and undersampling did now not offer any significant improvement of performance in the lift of indexing. The oversampling method increases the possibility of data redundancy, depending on how instances are generated. For removing this problem, few approaches have been introduced, such as the Modified Synthetic Minority Oversampling Technique (MSMOTE) [21], and Adaptive Synthetic Sampling (ADASYN0) [22]. Another concern is that the instance replication appears to increase the computational cost of the learning process [23]. By comparison, random undersampling (RUS) is a method that shrinks the majority class though it is easy to use. As a result it may however delete some useful data from the dataset. To solve this percussion, the One Sided-Selection (OSS) technique [24] is used that cuts out the redundancy, noise that close to the boundary instances from the majority class. Border instances are discovered by using Tomek links and instances. In the clustering based under sampling [3] method the dataset is split into two classes as a form of majority and minority. Then clustering based undersampling is applied to eliminate the few samples of majority class data. After that, the reduced majority class data set will then be combined with the minority class dataset to form a balanced dataset. The

classifier is finally trained using the balanced dataset. The problem with this approach is that certain essential data samples are omitted from the original dataset which may make the end result less accurate. In the Repeated random sub sampling [4] methods a number of samples from the original dataset are chosen and then the samples are divided into a number of sub-samples with the same number of instances in each class. After that, every sub-sample is fitted by the classification algorithm. Finally, the results are determined by majority vote on all sub-samples. The problem with this model is that the entire data set is not used in the experiment which may result in the final prediction being less accurate. SMOTE (Synthetic minority oversampling technique) [13] is one of the data science approaches that is most used and famous in the data science and machine learning where a synthetic minority class training instances are generated by spontaneously selected data instances based on interpolation with minority class. The SMOTE identifies each instance's k-nearest (typically k=5) neighbors from the minority class and then creates new instances synthetically as a convex combination that connects the two instances of the feature space to its k-nearest neighbors. Galar et al. [19], SMOTEBoost [20] is one of the most commonly used and popular methods that combines Synthetic Minority Oversampling Technique (SMOTE) and a rule-based standard boosting procedure where all instances that are misclassified are given equal weights. The SMOTEBoost synthetically generates instances of a rare or minority class to indirectly change the weights of a skewed minority class distribution, which reduces the variance. Consequently, removing the data samples from the original dataset can result in inaccurate prediction.

RUS Boosting (Random undersampling): In this RUS some data samples are randomly removed from the majority class of the dataset before the boosting procedure. Seifort et al. [15] proposed a RUSBoosting approach that combines random under sampling method with a boosting procedure providing an effective and efficient method for improving classification performance when the dataset is imbalanced. It presents simple, effective, efficient, faster, easy alternative solution of SMOTEBoost for learning from disproportional dataset in machine learning. Under Bagging: Recently combining multiple classifiers into one classifier as ensembles classifiers has become more popular and considered as more promising approach in machine learning classification. The UnderBagging is essentially a combination of a random sampling technique and a bagging method. In Barandela et al. [16], first uses UnderBagging approach where majority or dominant class instances were sampled and then a balanced training data set was used construct a K nearest (typically K=1) neighbor Ensemble classifier based on bagging. Galar et al. [17] suggested a hybrid approach using a variety of balanced training sets to train classifier ensembles where each balanced training dataset was used for a single classifier. Then, a number of classifiers were then merged into one ensemble classifier by a hybrid bagging approach to achieve higher output while more classifiers made it more complex. The approaches to enhancing the classifier's overall accuracy are called the algorithmic level solution. There are two algorithmic level solutions, including the known recognized and sensitive solution. The SVM one-sided class method [25]

is a known technique that takes into account only one class during the learning process. The support vector model in single-class SVM is trained on data that can only be trained by one normal class. A dynamic sampling method (DyS) for multilayer perceptron (MLP) [26] is a sensitive based approach where the probability of the selected sample is estimated by feeding the every sample to the current MLP.

The limitations are as:

- The oversampling method produces duplicate data sample in the dataset that may affect the overall prediction performance.
- Although under sampling is better than the oversampling, it removes important data sample from the dataset.
- Data redundancy and data hiding.

To remove above mentioned limitations of the existing methods we propose a novel predicting algorithm—The sub group based blanching method solutions of the imbalanced dataset that maximizes the effectiveness of the predictive result.

The contribution of this research can be summarized as follows:

- Firstly, we present a machine learning based prediction algorithm for dealing with the imbalance dataset that separates the data set into two groups i.e. majority class based dataset and minority class dataset. Then a balance dataset is made by taking the equal number of samples of minority class based dataset from the majority class based dataset with the samples of the minority class based dataset.
- Finally, we conduct *experiments* to evaluate the effectiveness of our proposed machine learning based prediction method in terms of imbalance dataset. The experimental results show that our proposed method significantly outperforms than the existing methods according to various test cases.

The remainder of the paper is organized as the following sections. In Section III, the suggested method is presented. Section IV outlines the assessment and experimental findings of the proposed method. Finally, Section V concludes the research study.

### III. PROPOSED METHODOLOGY

The overall dataset is divided into two sub datasets as a dataset of minority class and majority class. The majority class dataset is then split into a number of sub-datasets equal to the total number of minority class data samples. Now the minority class dataset is combined with each sub-dataset of the majority class to create a balanced dataset before the sub-datasets of the majority class are used only with a single minority class sub-dataset. Once the minority class dataset is combined with a majority class sub dataset, the prediction model is tested and applied with the combined balanced dataset and the result is added as a grand total result. After all implementation of all sub-sample balanced data sets has been completed, the grand

total result is averaged by the total number of sub-sample balance dataset. Eliminating all issues with current methods, such as deleting and duplicating essential data samples from the initial dataset, the proposed method does better than other existing methods.

Suppose, the dataset includes N samples. The N samples are divided into  $N_{max}$  and  $N_{min}$ , where  $N_{max}$  is the total number of samples in the majority class and  $N_{min}$  is the total number of samples in the minority class i.e.  $N=N_{max} + N_{min}$ . The  $N_{max}$  is divided into  $N_{max\ i}$  sub samples as equivalent to the  $N_{min}$  where  $i=1, 2, 3...N_{min}$ . Now each group of  $N_{max\ i}$  samples is merged to the  $N_{min}$  samples as a balanced data set. Such as the balanced dataset =  $Merge(N_{max\ i}, N_{min})$  where  $N_{max\ i}$  is a group samples of the majority class data and  $N_{min}$  is the group of samples of the minority class data. Finally, every balanced dataset produced is applied to the classification techniques using the proposed method. After that, average result is calculated from the all balance datasets as final result. The suggested approach is depicted in Fig. 1 as an overall technique.

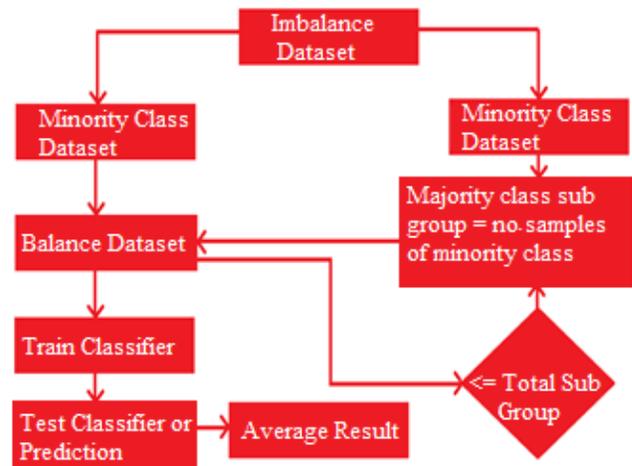


Fig. 1. Flowchart of Sub Group based Blanching Method.

Let's consider an example by considering a dataset of 100 samples where the total number of minority class samples is 20 and total number of majority class samples is 80.

$$totalSamples_{minClass} = 20 \text{ and}$$

$$totalSamples_{majClass} = 80;$$

The minority class samples forms four balanced dataset by randomly selecting twenty or equal number of samples from the majority class.

$$subSampel_{majClass} = 20;$$

Now, these minority class dataset and majority class sub datasets are appended to form a complete balanced dataset.

$$balanceDataset = append(totalSamples_{minClass}, subSampel_{majClass});$$

Now, a complete balanced dataset of forty samples is formed whereas twenty samples of minority class and the rest twenty samples of majority class. This formation of balanced

dataset iterates four times according to the total number of majority class samples is divided by the total number of minority class samples or  $\frac{4}{20} = 20$ ; Finally, the result is calculated and summed for each balanced dataset and average result is considered as the outcome of the proposed method..

**Algorithm 1: SGBBM**

**Data:** Imbalance Dataset: DS=1, 2, 3...N // each sample i contains a number of features and corresponding the majority and minority class.

**Result:** Balance Dataset

Procedure SGBBM(DS, N);

//separate the dataset into the majority and minority class dataset.

$dataset_{majClass} = allSamplesOfTheMajorityClass;$

$dataset_{minClass} = allSamplesOfTheMinorityClass;$

$totalSamples_{minClass} =$

$totalNumberOfMinorityClassSamples;$

$totalSamples_{majClass} =$

$totalNumberOfMajorityClassSamples;$

$balanceDataset_{sub} = '';$

result = 0;

**For**  $count \in [1, totalSamples_{minClass}]$  **do**

a.  $subDataset_{majClass} =$

$RandSelect(dataset_{majClass}, totalSamples_{minClass});$

//equal of  $totalSamples_{majClass}$  samples is selected randomly.

b.  $balanceDataset_{sub} =$

$Append(dataset_{minClass}, subDataset_{majClass});$

// Balance dataset are created

c.  $Result += Prediction(balanceDataset_{sub});$

**End for**

$averageResult = \frac{Result}{dataset_{minClass}};$

$return(averageResult);$

**End Procedure**

IV. RESULT AND DISCUSSION

A. Implementation Methods

1) *Random forest:* Random Forest is a set of tree predictors that is a supervised learning algorithm that can be used for classification as well as regression, generating a number of classifiers and aggregating their results to achieve the best results. In the random forest, every tree depends on the values of a random vector sampled separately and distributed equally to all trees in the forest [31]. This can handle high dimensional data by building decision trees on randomly selected data samples which are predicted for certain data from each tree. Finally, the best solution is selected by means of voting. It works as follows:

- It chooses random instances from the dataset provided.

- It constructs decision tree for each instance and obtains predictive results from each decision tree.
- It applies the voting system to all predicted results.
- Finally, it chooses the best predicted outcome.

Few important characteristics of RF are as follows [14]:

- It can effectively measure the missing data in the dataset.
- Using weighted rand forest (WRF) process, the error in imbalanced dataset can be balanced.
- The value of variables used in the classification can be calculated.

The Random Forest classifier's full operation flow chart is shown in Fig. 2.

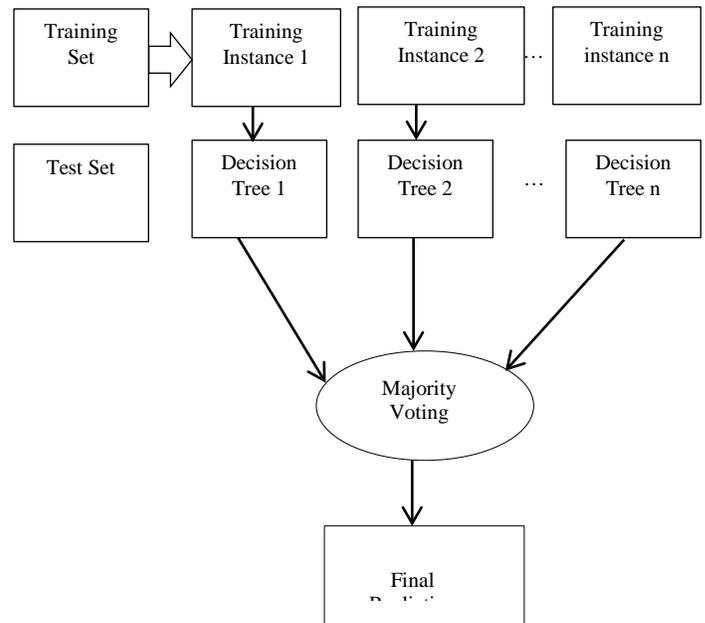


Fig. 2. Random Forest Working Principle.

2) *Naïve Bayes:* In machine learning, naïve Bayes methods are a series of supervised learning algorithms based on the application of Bayes' theorem, a probabilistic model of machine learning. This is a probabilistic model in which each pair of features is independent of each other provided the value of the class variable to be categorized. It works by translating the dataset into a frequency table and requires a number of linear variables for a linear problem. It comes in the form below:

$$P\left(\frac{A}{B}\right) = \frac{P\left(\frac{B}{A}\right) P(A)}{P(B)} \tag{1}$$

Where, the probability of the A event is determined, while the B occurred. Here, the A is hypothesis and B is evidence. It calculates the probability of each input class and helps predict the target class of the unknown data samples. The general theorem of Bayes uses the following formula to measure the posterior probability for each class.

$$P\left(\frac{C}{X}\right) = P\left(\frac{X}{C}\right)P(C) \quad (2)$$

$$P\left(\frac{C}{X}\right) = P\left(\frac{X_1}{C}\right) \times P\left(\frac{X_2}{C}\right) \times \dots \times P\left(\frac{X_n}{C}\right) \times P(C) \quad (3)$$

- $P\left(\frac{C}{X}\right)$  = The corresponding probability of target class in which the predictor attribute is assigned.
- $P(C)$  = The target class's prior probabilities.
- $P\left(\frac{X}{C}\right)$  = The probability of the predictor variable in which the target class is given.
- $P(X)$  = The predictor variable's prior probability.

3) *K-Nearest neighbor*: The K-nearest neighbor method is a non-parametric simple, easy to implement, supervised machine learning technique that classifies the new samples on the basis of similarity measures that can be used for predictive problems of classification and regression. In KNN, three approaches to distance measurements are true only for variables in KNN such as Euclidean, Manhattan, Murkowski. It uses the 'function similarity' to forecast new data point values. If K=1(where k is an integer), the row is then simply allocated to the class of its nearest data point. The KNN does not have a special training process and the entire dataset is used during the classification. Fig. 3 depicts the activity of the KNN.

The KNN algorithm works as follows:

1. Firstly it is needed to take a value of K i.e. the closest data points where K can be any integer.
2. Within the test data set the following steps are performed for each data point:
  - a. Measure the distance between the training data and test data in-row using any distance measurement technique, such as Euclidean or Manhattan or Hamming distance, where Euclidean technique is most used.
  - b. The rows are ordered in ascending order according to the distance calculated.
  - c. Top K rows are picked from the sorted array.
  - d. Now the test point is allocated a class according to the most frequent class in this test point row.
3. End.

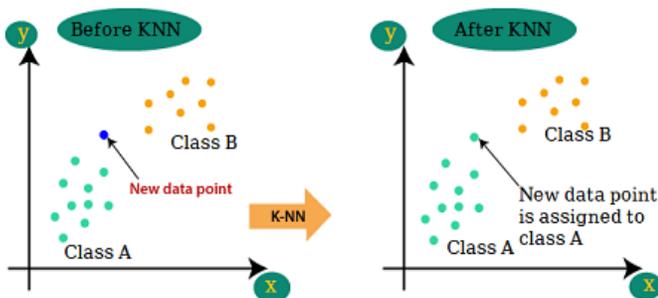


Fig. 3. K-nearest Neighbor Algorithm.

## B. Evaluation and Experimental Result

1) *Dataset description*: The author has been tested this algorithm using three benchmark datasets such as credit card, abalone and wine quality datasets that are presented in the Table I with imbalance ratio (minority: majority) of 1:577, 1:16 and 1:2. The abalone and wine quality datasets were taken from the UCI repository and fetched with imblearch python 3.5 library.

The credit card dataset has been collected during research collaboration from ULB's Worldline and Machine Learning Group (ULB University Libre de Bruxelles) on big data processing and fraud detection. The dataset contains 284,807 transactions made by the holders of credit cards in Europe in September 2013.

All the features of the credit card dataset are shown in the Table II are not identical in terms of the distribution the transaction amount and transaction time. In order to build a machine learning based credit card fraud detection model for imbalance dataset, firstly we have prepared raw dataset with the feature values that are mentioned in the Table II. All transactions took place within two days with 492 fraud transactions out of 284,807 transactions where the proportion of the positive class (fraud) of all transactions was 0.172 percent. The dataset includes only the numerical variables such as  $V_1$  to  $V_n$  ( $n=1, 2, \dots, 28$ ) which are the fundamental components of this dataset.

TABLE I. DATASET DESCRIPTION

	Dataset Name	Description	Minority: Majority	# Samples	# Features
1	Credit Card Dataset	Credit Card fraud detection	492:284315 => (1:577)	284,807	31
2	Abalone Dataset	Prediction of the abalone age	42:689 => (1:16)	731	9
3	Wine Quality Dataset	Prediction the quality of the white wine	175:4898 => (1:27)	5073	13

TABLE II. CREDIT CARD DATASET FEATURES WITH VALUE TYPE

Feature Name	Value Type	Feature Name	Value Type	Feature Name	Value Type
Time	Float	V11	Float	V22	Float
V1	Float	V12	Float	V23	Float
V2	Float	V13	Float	V24	Float
V3	Float	V14	Float	V25	Float
V4	Float	V15	Float	V26	Float
V5	Float	V16	Float	V27	Float
V6	Float	V17	Float	V28	Float
V7	Float	V18	Float	Amount	Float
V8	Float	V19	Float	Class	Integer
V9	Float	V20	Float	V22	Float
V10	Float	V21	Float	V23	Float

Table III describes the all features of the abalone dataset whereas two features are integer types and rest of the features is float types. The abalone dataset is used for foreseeing the period of abalone from actual estimations. Cutting the shell through the cone, staining it, and counting the number of rings through a microscope are used to calculate the age of abalone.

Table IV lists the characteristics of the wine quality dataset, two of which are integer types and the others are float types.

The red varieties of the Portuguese "Vinho Verde" wine are the subject of this dataset.

2) *Experiment setup*: In order to evaluate the effectiveness of our proposed method, we aim to answer the following two questions:

- Question 1: Is the proposed machine learning based prediction method able to detect the credit card fraud and to provide significant effectiveness of result for various test cases?
- Question 2: How effective and efficient is our proposed method compared to the existing machine learning based balancing methods?

In answering the above questions, we have conducted experiments on a credit card dataset consisting of two binary classes discussed in a previous section. We have implemented and tested all the methods in Python programming language, in which we have used Scikit-learn, the most popular machine learning library and executed on a Windows PC for predictive data analysis. In the following subsections, we first define the evaluation metrics that are taken into account to evaluate our proposed prediction method and then discuss the results of the experiment which address the above questions defined for this experimental study.

TABLE III. ABALONE DATASET FEATURES WITH VALUE TYPE

Feature Name	Value Type	Feature Name	Value Type	Feature Name	Value Type
Type	Integer	Length	Float	Diameter	Float
Height	Float	Whole weight	Float	Shucked weight	Float
Viscera weight	Float	Shell weight	Float	Rings	Integer

TABLE IV. WINE QUALITY DATASET FEATURES WITH VALUE TYPE

Feature Name	Value Type	Feature Name	Value Type	Feature Name	Value Type
Sex	Integer	Fixed Acidity	Float	Volatile Acidity	Float
Citric Acid	Float	Residual Sugar	Float	Chlorides	Float
Free Sulfur Dioxide	Float	Total Sulfur Dioxide	Float	Density	Float
pH	Float	Sulphates	Float	Alcohol	Float
Quality	Integer				

3) *Evaluation metric*: The evaluation criteria are an important factor in assessing the classification efficiency. In order to measure the effectiveness and efficiency, we take into account the *accuracy*, *specificity*, *precision*, *recall*, *f-score* to test our proposed efficient prediction methodology that are defined as follows

a) *Accuracy*: The accuracy rate is normally the most common empirical measure in the classification algorithms for machine learning. Accuracy is the ratio of number of accurate predictions to total input samples. Rate of classification or accuracy is determined by the relation:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

In the imbalance data set domain the accuracy rate is not a valid output assessment metric. Since it does not give any result from correctly or incorrectly classified samples of the various classes. This can trigger an incorrect conclusion for this reason. When a classifier achieve a 91 percent accuracy rate is not ideal because it classifies all samples as negative. So the *Confusion metric* is another evaluation metric in the domain of imbalance dataset.

b) *Confusion Matrix*: A confusion matrix is a description of the predictive results on a classification problem for machine learning. It records the samples for each class correctly and incorrectly predicted. Pizzi et al. [28] discuss the confusion matrix in more detail. The confusion matrix demonstrates how the classification model becomes confused when it makes data set predictions where performance can be two or more classes. It is a table with four different expected and actual combinations of values. This is represented by four pieces of data:

- True Positive (TP): An element is expected to be defective and it is defective. Ultimately it applies to the number of successful instances listed correctly.
- False Positive (FP): An element is expected to be defective and is not defective. This applies to how many derogatory classes are misclassified.
- True Negative (TN): An element is expected not to be defective, and is not defective. This refers to the number of correctly identified negative instances.
- False Negative (FN): An element is expected not to be faulty, and is faulty. This applies to the number of positive instances that are misclassified.

The structure of the confusion matrix is shown in Fig. 4.

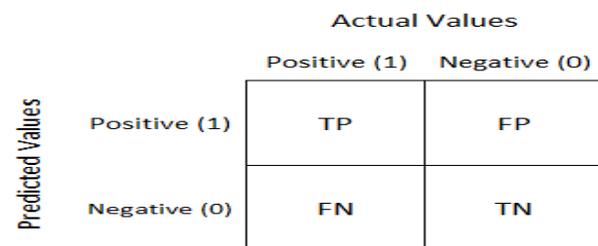


Fig. 4. Structure of the Confusion Matrix.

The specificity, recall, f-score and precision are defined as follows [32]:

$$\text{Specificity: } \frac{TN}{TN+FP} \quad (5)$$

$$\text{Recall: } \frac{TP}{TP+FN} \quad (6)$$

$$\text{F-score: } \frac{2*TP}{2*TP+FP+FN} \quad (7)$$

$$\text{Precision: } \frac{TP}{TP+FP} \quad (8)$$

Where TP denotes true positives, TN denotes true negatives, FP denotes false positives and FN denotes false negatives in these above formal equations of specificity, recall, f-score and precision.

4) *Experimental result:* In order to answer the first question mentioned above, in this experiment show the experimental results of our machine learning based prediction detection method. We have used the three benchmark datasets to verify the performance of the experimental results on different type of data. To calculate the experimental results for various test cases, we first built the method using a subset of 80% data samples from the given highly imbalanced dataset and used the remaining 20% of data samples for testing the proposed method. The experimental results are calculated by generating a confusion matrix that presents the number of true positives, true negatives, false positives and false negatives. According to these values, Table V and Table VI present the prediction results and true & false positive rate of our *proposed* method respectively in terms of specificity, recall, f-score, precision and accuracy for each individual class using the given highly imbalanced dataset in order to show the experimental results. If we observe Table V, we see that for each class, our proposed method gives the significant improved results of the specificity, recall, f-score, precision and accuracy. From Table V, we see that the accuracy, precision, specificity, recall and f-score of Random Forest, Naïve Bayes, K-Nearest Neighbor are (99%,96%,90%),(98%, 98%,97%),(86%,93%,85%),(90%,70%,97%) and (92%, 70%, 97%), respectively. If we observe the Table VI, the true

positive rate of the Random Forest, Naïve Bayes and K-Nearest Neighbor classifiers using our proposed method are 86%, 93%, 85%, respectively that are very close to the maximum value 1 and the false positive rate are 5% , 72%, 5% respectively that are very lower than the existing methods. In this way, from overall experimental results shown in Table V and Table VI, we can say that our proposed machine learning based prediction method in terms of highly imbalanced dataset is able to efficiently detect either fraud or not fraud class according to their occurring patterns in the highly imbalanced credit card fraud dataset and consequently provides a significant effectiveness for a various test cases.

Table VII and Table VIII represent the observe values for Specificity, Recall, F-score, Precision, Accuracy, True Positive rate and False Positive rate using the abalone dataset. Random Forest, Nave Bayes, and K-Nearest Neighbor have almost as high a precision as the most advanced algorithms. The Nave Bayes and KNN recalls are very similar to one, though the Random Forest recall is slightly lower. The F-score of the KNN is very close to 1, while the F-scores of Random Forest and Nave Bayes are a little lower but still appropriate.

For all base line algorithms, the True Positive Rate (TPR) is significantly higher than the False Positive Rate (FPR), which is significantly lower.

The experimental results of the proposed method on a wine quality dataset using various machine learning algorithms are shown in Tables IX and X. Random Forest and Nave Bayes have substantially high accuracy to the highest accuracy, while KNN has a satisfactory and better accuracy of 91%.

The Random Forest algorithm has a very high specificity, but it performs better than other Nave Bayes and KNN algorithms.

The True Positive Rate (TPR) for Random Forest, Nave Bayes, and KNN is significantly higher, while the False Positive Rate (FPR) is significantly lower, even though the FPR of Nave Bayes is 91 percent, suggesting that the Nave Bayes' performance in terms of FPR is not good.

TABLE V. EFFECTIVENESS COMPARISON OF THE DIFFERENT CLASSIFIERS USING PROPOSED ALGORITHM ON CREDIT CARD DATASET

#	Classifier	Specificity	Recall	F-score	Precision	Accuracy
1	Random Forest	98%	86%	90%	92%	99%
2	Naïve Bayes	98%	93%	70%	70%	96%
3	K-Nearest Neighbor	97%	85%	90%	97%	90%

TABLE VI. COMPARISON OF TRUE POSITIVE RATE VERSUS FALSE POSITIVE RATE OF DIFFERENT CLASSIFIERS USING PROPOSED ALGORITHM ON CREDIT CARD DATASET

#	Classifier	True Positive Rate (TPR)	False Positive Rate (FPR)
1	Random Forest	86%	5%
2	Naïve Bayes	93%	72%
3	K-Nearest Neighbor	85%	5%

TABLE VII. EFFECTIVENESS COMPARISON OF THE DIFFERENT CLASSIFIERS USING PROPOSED ALGORITHM ON ABALONE DATASET

#	Classifier	Specificity	Recall	F-score	Precision	Accuracy
1	Random Forest	97%	94%	95%	95%	97%
2	Naïve Bayes	96.2%	98%	94%	92%	98.23%
3	K-Nearest Neighbor	98%	98%	98%	97%	94%

TABLE VIII. COMPARISON OF TRUE POSITIVE RATE VERSUS FALSE POSITIVE RATE OF DIFFERENT CLASSIFIERS USING PROPOSED ALGORITHM ON ABALONE DATASET

#	Classifier	True Positive Rate (TPR)	False Positive Rate (FPR)
1	Random Forest	89%	10%
2	Naïve Bayes	96%	81.4%
3	K-Nearest Neighbor	98.2%	15.6%

TABLE IX. EFFECTIVENESS COMPARISON OF THE DIFFERENT CLASSIFIERS USING PROPOSED ALGORITHM ON WINE DATASET

#	Classifier	Specificity	Recall	F-score	Precision	Accuracy
1	Random Forest	98.6%	91%	95.3%	93.4%	99%
2	Naïve Bayes	93%	83%	90%	89%	98%
3	K-Nearest Neighbor	91%	92%	92.45%	95%	91%

TABLE X. COMPARISON OF TRUE POSITIVE RATE VERSUS FALSE POSITIVE RATE OF DIFFERENT CLASSIFIERS USING PROPOSED ALGORITHM ON WINE DATASET

#	Classifier	True Positive Rate (TPR)	False Positive Rate (FPR)
1	Random Forest	94%	12%
2	Naïve Bayes	97.6%	91%
3	K-Nearest Neighbor	96.5%	10%

5) *Effectiveness comparison*: In order to answer the second question, in this experiment, we calculate and compare the effectiveness of our proposed method with the existing algorithm i.e. *SMOTE*. To show the effectiveness of different machine learning based models, we first select several popular baseline algorithms such as Random Forests (RF), Naïve Bayes (NB) and K-Nearest Neighbor (KNN) for the sake of effectiveness comparisons. For each algorithm, we calculate the experimental results using the same highly imbalanced dataset, in order to compare the model fairly. To compute the effectiveness of different baseline algorithms, we see that Table V and Table XI show the relative comparison of the experimental results of different models using our proposed method and *SMOTE* respectively in terms of accuracy, precision, specificity, recall and f-score on credit card dataset. For each baseline model, we use the same training and testing sets of data, where 80% of data are used to train the model and the rest 20% data are used for testing the model. Our proposed model's specificity for all machine learning algorithms used here are significantly higher than the specificity of the *SMOTE*, indicating superior performance on the credit card dataset. The recalls of proposed method are also better than the *SMOTE*. The proposed method's f-scores are considerably higher, while the f-score of Nave Bayes has plummeted. The proposed method outperforms the traditional *SMOTE* method

in not only specificity, recall, and f-score, but also in all output matrixes.

If we consider Table VII and Table XII, the effectiveness of different baseline models using our proposed methods is better than the effectiveness of different baseline models using *SMOTE* method on abalone dataset. Using the proposed approach on the abalone dataset, the accuracy for all machine learning algorithms used here is substantially higher than the *SMOTE*. On the abalone dataset, the recall of Nave Bayes and KNN using the proposed model is nearly 100 percent higher than that of *SMOTE*, demonstrating the proposed method's superior efficiency whereas the f-score, precision and accuracy are still better than *SMOTE*. Because all samples of the imbalanced dataset are used in the experiment. As a result, the data redundancy and removal of important sample from the dataset are solved successfully.

Table IX and Table X show the significant differences from the result of the proposed method to *SMOTE* method on wine quality dataset that proofs the robustness of the proposed method. The proposed method improves the accuracy of the Random Forest and Nave Bayes to a maximum of 100% compared to the standard *SMTOE* on wine quality dataset. In this regard, the proposed approach not only increases the Random Forest's specificity to the nearest 100 percent, but also greatly improves the recall, f-score, precision, and accuracy output values.

On all three datasets, the proposed method outperforms than the conventional SMOTE method in terms of specificity, recall, f-score, precision, and accuracy, as seen in the above effectiveness comparison. The proposed SGBB has greater generalization capabilities than SMOTE, as shown by the better performance of all evaluation matrices. Since the proposed method eliminates all of the above-mentioned shortcomings of SMOTE, it can be used in all complex cases to predict classes due to its superior performance over conventional SMOTE.

Fig. 5 and 6 show the comparative results of different classifiers that are obtained after experimenting by authors using SMOTE and proposed algorithm respectively. In terms of specificity, recall and accuracy our proposed algorithm is much better than the SMOTE. The F-score of the Naïve Bayes and KNN are drastically down in SMOTE whereas the F-score of these classifiers are efficiently getting higher in our proposed algorithm. The precision of Naïve Bayes and KNN are 1% and 34% using SMOTE whereas these values are 70% and 97% respectively in our proposed algorithm that is very much high.

Fig. 7 and 8 show the true and false positive rates of the SMOTE and our proposed algorithm. The TPR of Random Forest using our proposed algorithm is getting higher than the SMOTE whereas the TNR is 99% that is maximum and unexpected in machine learning. On the other hand, the TPR and TNR of Naïve Bayes are being greater and lower respectively using our proposed algorithm than the SMOTE whereas the TPR of Naïve Bayes is being fallen drastically down to 2% using SMOTE. The TPR and TNR of KNN are greater and lower than the SMOTE respectively that is better performance of the algorithm. The TNR is maximum to 99% using SMOTE and the TPR is much lower than the proposed algorithm that indicates the less performance in machine learning.

For the wine dataset in Fig. 9 and 10, the positive predictive value is considerably greater in terms of Random Forest algorithm using the proposed SGBBA. On the other hand, positive predictive value falls down then the negative predictive value using the SMOTE. In terms of Naïve Bayes, the positive predictive value is still higher than the negative predictive value using the SGBBA whereas the SMOTE drastically falls down at 22.4% although the negative predictive value is too much higher that is another pitfall of the SMOTE. The proposed SGBBA consistently performs well during the prediction of positive value using the KNN whereas the SMOTE performs lower.

In the abalone dataset, the positive predictive value of Random Forest is efficiently higher whereas the negative predictive value is 10% using the SGBBA. On the other hand, the negative predictive value is higher than the positive predictive value using SMOTE. Similarly, the SGBBA performs very well in terms of positive predictive value in Naïve Bayes and KNN classifiers than the SMOTE that are showing in Fig. 11 and Fig. 12.

The proposed method's superior performance in all evaluation matrices demonstrates the robustness of the imbalance dataset handling method, which can be applied to any imbalance dataset for making balance dataset in machine learning. Thus, our proposed method not only remove the data redundancy, removal of important data samples and but also increase the prediction results for various test cases. Therefore, according to the experimental results shown in Table V, Table VI, Table VII, Table VIII, Table IX, Table X, Table XI, Table XII, Table XIII, Fig. 5, and Fig. 7 and above experimental result analysis, we can conclude that our proposed method is more effective and efficient than the existing SMOTE method during the experiment of data analysis and machine learning using the highly imbalanced dataset.

TABLE XI. EFFECTIVENESS COMPARISON OF THE DIFFERENT CLASSIFIERS USING SMOTE ALGORITHM ON CREDIT CARD DATASET

#	Classifier	Specificity	Recall	F-score	Precision	Accuracy
1	Random Forest	91%	83%	84%	85%	91%
2	Naïve Bayes	95%	90%	1%	1%	90%
3	K-Nearest Neighbor	90%	82%	49%	34%	85%

TABLE XII. EFFECTIVENESS COMPARISON OF THE DIFFERENT CLASSIFIERS USING SMOTE ALGORITHM ON ABALONE DATASET

#	Classifier	Specificity	Recall	F-score	Precision	Accuracy
1	Random Forest	95.32%	88.35%	92%	88%	93%
2	Naïve Bayes	91.12%	93.2%	84%	76%	91.5%
3	K-Nearest Neighbor	94.3%	94.3%	92%	87%	90%

TABLE XIII. EFFECTIVENESS COMPARISON OF THE DIFFERENT CLASSIFIERS USING SMOTE ALGORITHM ON WINE QUALITY DATASET

#	Classifier	Specificity	Recall	F-score	Precision	Accuracy
1	Random Forest	93%	83%	90%	89%	98%
2	Naïve Bayes	92%	90%	95.5%	82%	94%
3	K-Nearest Neighbor	91%	92%	49%	95%	91%

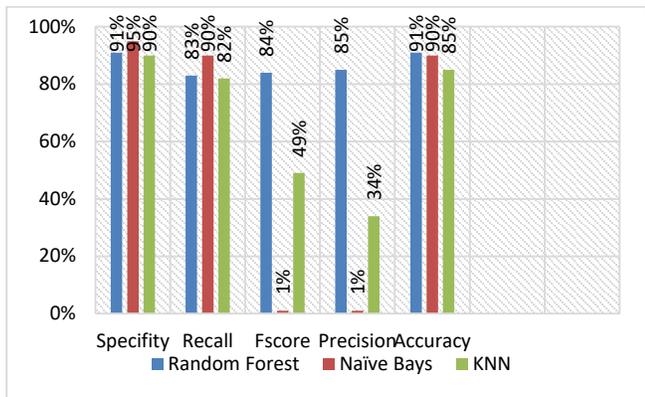


Fig. 5. Accuracy Comparison of the different Classifiers using SMOTE on Credit Card Dataset.

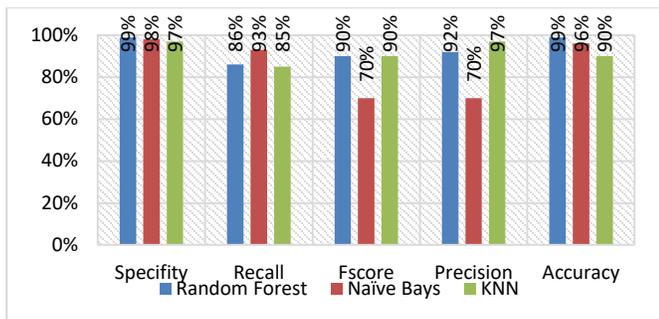


Fig. 6. Accuracy Comparison with Proposed Approach on Credit Card Dataset.

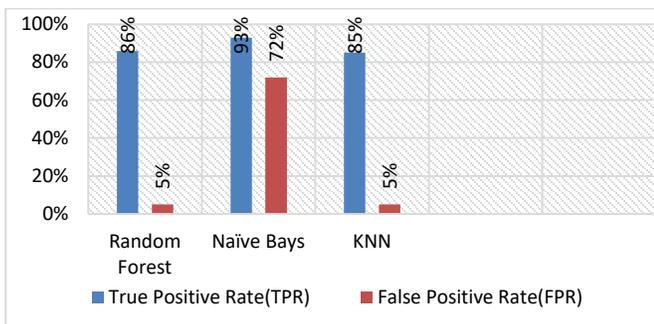


Fig. 7. Comparison of True Positive Rate versus True Negative Rate of different Classifiers using Proposed Algorithm on Credit Card Dataset.

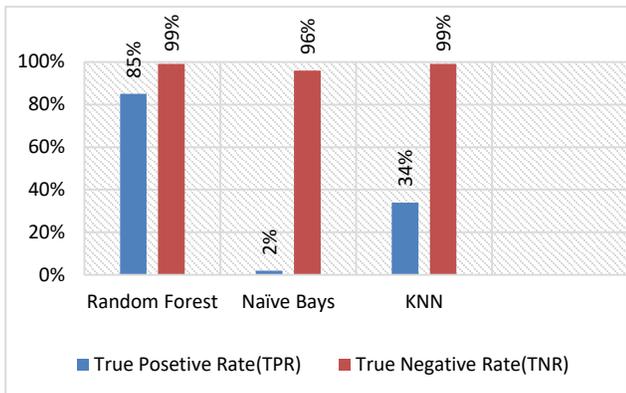


Fig. 8. True Positive Rate versus True Negative Rate of different Classifiers using SMOTE Algorithm on Credit Card Dataset.

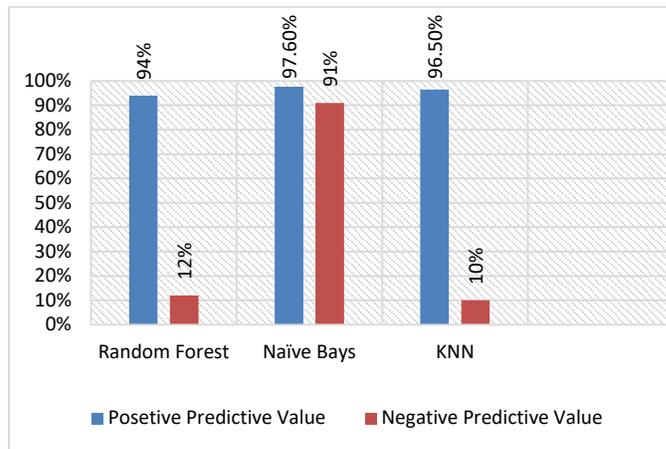


Fig. 9. True Positive Rate versus True Negative Rate of different Classifiers using Proposed Algorithm on Wine Dataset.

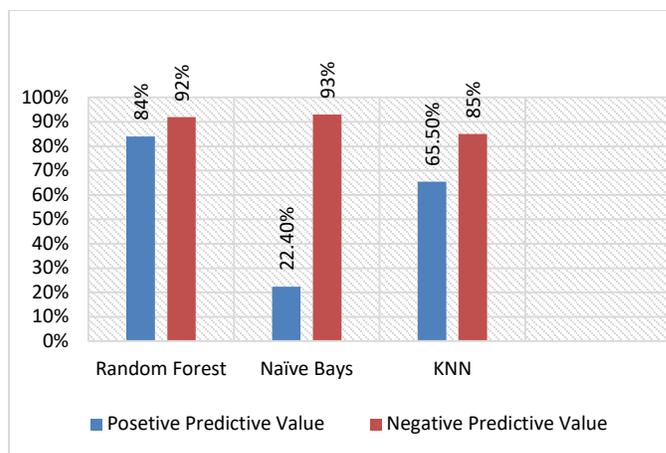


Fig. 10. True Positive Rate versus True Negative Rate of different Classifiers using SMOTE Algorithm on Wine Dataset.

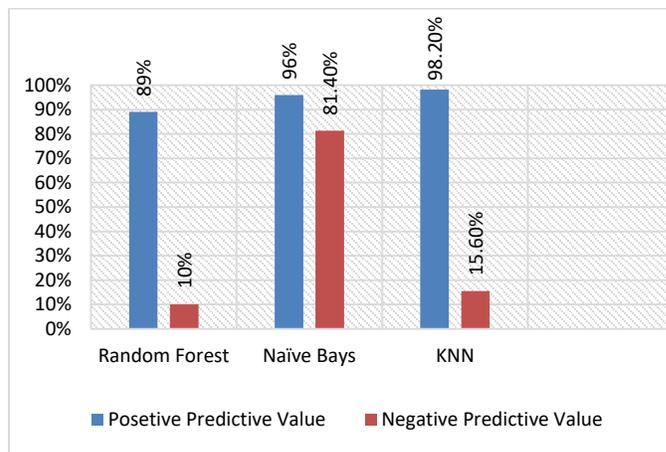


Fig. 11. True Positive Rate versus True Negative Rate of different Classifiers using Proposed Algorithm on Abalone Dataset.

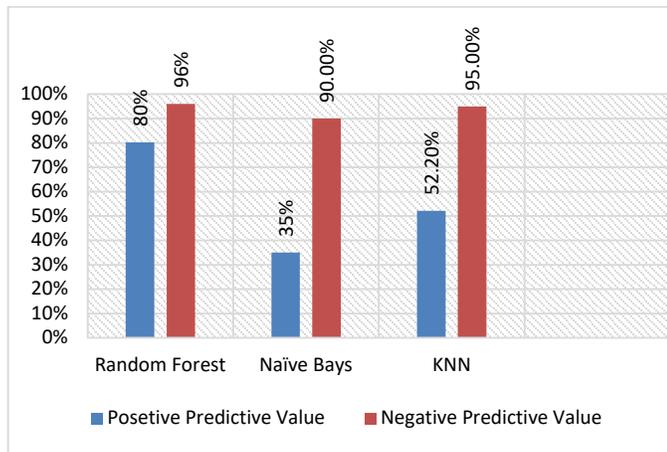


Fig. 12. True Positive Rate versus True Negative Rate of different Classifiers using SMOTE Algorithm on Abalone Dataset.

## V. CONCLUSION AND FUTURE WORK

Trying to train a model using an imbalanced dataset by a researcher is a challenging task due to the biasing of classes in the dataset. The biasing of classes in the dataset decreases the performance of the classifiers to an extent. As a result, perfect prediction is not possible in an imbalanced dataset. The processing of data from an imbalanced dataset is a key challenge and activity in data science and machine learning. Because without having a balanced dataset, the creation of a new classification model produces a skewed prediction result to the majority class, ignoring the minority class. The prediction from the imbalanced dataset is therefore unnecessary and useless for machine learning. A variety of methods are explored in the background analysis section for creating a balanced dataset from the imbalanced dataset. Each methodology has a serious problem with balancing data sets such as data redundancy and removal of essential samples of data. To solve this problem, we have introduced an algorithm named – SGBBA: An efficient algorithm for prediction system in machine learning using an imbalanced dataset where each sub-dataset is a balanced dataset without any data redundancy and removal of important data samples. This new algorithm is implemented with three different classification algorithms, and their results are compared with the predictive result of the SMOTE algorithm. The three datasets have played an important role in terms of determining the efficiency and performance of the proposed algorithm. Our approach has the following advantages:

- It solves the redundancy of data samples from existing methods.
- It solves the elimination of significant samples problem from the original dataset.

Such benefits have advantages for researchers, practitioners, and reviewers so that they can use this theoretical model to predict results in terms of machine learning imbalanced datasets.

Our future goal is to develop an efficient minority class-based algorithm for a prediction system in machine learning with optimal features of the dataset.

## ABBREVIATIONS

$N_{min}$ : Total number of samples of the minority class,  $N_{max}$ : Total number of samples of the majority class, SMOTE: Synthetic Minority Over-sampling Technique, TP: True Positive, TN: True Negative, FN: False Negative, FP: False positive.

## ACKNOWLEDGMENTS

We are extremely grateful to all co-authors for their strong feedbacks and contributions in the field of learning from imbalanced datasets whereas 1. Saiful Islam collected data, studied and implemented the proposed architecture. 2. Umme Sara contributed to designing the idea, writing the proposed methodology partly and compiling the article. 3. Abu Kawsar contributed to the drawing of flow chart and result representation graph. 4. Anichur Rahman reviewed the introduction and organizing the article. 5. Depanjali Kundu. 6. Diganta Das Dipta reviewed background knowledge and wrote the experiment part. 7. A.N.M. Rezaul Karim contributed to the mathematical analysis of the proposed method. 8. Mahedi Hasan contributed in main algorithm for dataset balancing process. We are pleased to work with them and to contribute to this domain.

## REFERENCES

- [1] Everlandio R.Q. Fernandes, Andre C.P.L.F. de Carvalho and Xin Yaho. Ensemble of Classifiers based on Multi Objective Genetic Sampling for Imbalanced Data. Journal of LATEX Class Files, VOL.14, No. 8, August 2015.
- [2] Guo Haixiang, Li Yijing, Jennifer Shang, Gu Mingyun, Huang Yuanyue, Gong Bing. Learning from class-imbalanced data: Review of methods and applications. Expert Systems With Applications 73 (2017) 220-239.
- [3] Wei-Chao Lin, Chinh-Fong Tsai, Ya-Han Hu, Jing-Shang Jhang. Clustering –based undersampling in class-imbalance data. Information Science 409-410 (2017) 17-26.
- [4] Mohammed Khalilia, Sounak Chakraborty and Mihai Popescu. Predicting disease risks from highly imbalanced data using random forest. Khalilia et al. BMC Medical Informatics and Decision Making 2011.
- [5] Nitesh V. Chawla. Data Mining for Imbalanced Datasets: An Overview. Data Mining Knowledge Discovery Handbook, 2<sup>nd</sup> ed. DOI10.1007/978-0-387-09823-4\_45.
- [6] Mohd Farizul Mat Ghani. Intelligent Heart Disease Prediction System Using Data Mining Techniques. IJCSNS International Journal of Computer Science and Network Security, VOL. 8 No. 8, August 2008.
- [7] R.E. Schapire, The strength of weak learnability, Mach. Learn. 5 (2) (1990) 197–227.
- [8] L. Breiman, Bagging predictors, Mach. Learn. 24 (2) (1996) 123–140.
- [9] N.V. Chawla, A. Lazarevic, L.O. Hall, K.W. Bowyer, SMOTEBoost: improving prediction of the minority class in boosting, in: European Conference on Principles and Practice of Knowledge Discovery in Databases, 2003, pp. 107–119.
- [10] Seiffert, T. Khoshgoftaar, J. Van Hulse, A. Napolitano, RUSBoost: a hybrid approach to alleviating class imbalance, IEEE Trans. Syst. Man Cybern. –Part A 40 (1) (2010) 185–197.
- [11] Wang, X. Yao, Diversity analysis on imbalanced data sets by using ensemble models, in: IEEE International Symposium on Computational Intelligence and Data Mining, 2009, pp. 324–331.
- [12] Barandela, R.M. Valdovinos, J.S. Sanchez, New applications of ensembles of classifiers, Pattern Anal. Appl. 6 (2003) 245–256.
- [13] N.V. Chawla, A. Lazarevic, L.O. Hall, K.W. Bowyer, SMOTE Boost: improving prediction of the minority class in boosting, in: European Conference on Principles and Practice of Knowledge Discovery in Databases, 2003, pp. 107–119.

- [14] Breiman L. Random forests. *Machine learning*. 2001, 45 (1): 5-32. 10.1023/A:1010933404324.
- [15] Seiffert , T. Khoshgoftaar , J. Van Hulse , A. Napolitano , RUSBoost: a hybrid approach to alleviating class imbalance, *IEEE Trans. Syst. Man Cybern. –Part A* 40 (1) (2010) 185–197.
- [16] Barandela , R.M. Valdovinos , J.S. Sanchez , New applications of ensembles of classifiers, *Pattern Anal. Appl.* 6 (2003) 245–256.
- [17] Galar , A. Fernandez , E. Barrenechea , H. Bustince , F. Herrera , A review on ensembles for the class imbalance problem: bagging-, boosting-, and hybrid-based approaches, *IEEE Trans. Syst. Man Cybern. –Part C* 42 (4) (2012) 463–484.
- [18] Japkowicz, N. (2000a). The Class Imbalance Problem: Significance and Strategies. In *Proceedings of the 2000 International Conference on Artificial Intelligence (IC-AI'2000): Special Track on Inductive Learning*, Las Vegas, Nevada.
- [19] M. Galar , A. Fernandez , E. Barrenechea , H. Bustince , F. Herrera , A review on ensembles for the class imbalance problem: bagging-, boosting-, and hybrid-based approaches, *IEEE Trans. Syst. Man Cybern. –Part C* 42 (4) (2012) 463–484.
- [20] N.V. Chawla , A. Lazarevic , L.O. Hall , K.W. Bowyer , SMOTEBoost: improving prediction of the minority class in boosting, in: *European Conference on Principles and Practice of Knowledge Discovery in Databases*, 2003, pp. 107–119.
- [21] S. Hu, Y. Liang, L. Ma, and Y. He, "Msmote: Improving classification performance when training data is imbalanced," in *Computer Science and Engineering, 2009. WCSE '09. Second International Workshop on*, vol. 2, Oct 2009, pp. 13-17.
- [22] H. He, Y. Bai, E. Garcia, S. Li et al., "Adasyn: Adaptive synthetic sampling approach for imbalanced learning" in *Neural Networks, 2008. IJCNN 2008. (IEEE World Congress on Computational Intelligence)*. IEEE International Joint Conference on. IEEE, 2008, pp. 1322-1328.
- [23] Y. Sun, A. K. C. Wong and M. S. Kamal, "Classification of imbalanced data: a review," *IJPRAI*, vol. 23, no. 4, pp. 687-719, 2009.
- [24] M. Kubat and S. Matwin, "Addressing the curse of imbalanced training sets: One-Sided selection," in *In Proceedings of the Fourteenth International Conference on Machine Learning*. Morgan Kaufmann, 1997, pp. 179-186.
- [25] B. Scholkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution ." *Neural Computation*, vol. 13, no. 7, pp. 1443-1471, 2001.
- [26] M. Lin, K. Tang, and X. Yao, "Dynamic sampling approach to training neural networks for multiclass imbalance classification." *IEEE Trans. Neural Netw. Learning Systems*, vol 24, no. 4, pp. 647-660, 2013.
- [27] G.E.A .P.A . Batista , R.C. Prati , M.C. Monard , A survey of the behavior of several methods for balancing machine learning training data, *SIGKDD Explor.* 6 (1) (2004) 20–29.
- [28] Y. Sun , A.K.C. Wong , M.S. Kamel , Classification of imbalanced data: a review, *Int. J. Pattern Recognit. Artif. Intell.* 23 (4) (2009) 687–719.
- [29] N. Pizzi, A. Summers, and W. Pedrycz. Software quality prediction using median-adjusted class labels. In *Neural Networks, 2002. IJCNN '02. Proceedings of the 2002 International Joint Conference on*, volume 3, pages 2405 {2409, 2002.
- [30] Charles X. Ling and Chenghui Li. *Data Mining for Direct Marketing: Problems and Solutions*.
- [31] Leo Breiman, *Random Forests*. *Machine Learning*, 45, 5–32, 2001.
- [32] Han, J.; Pei, J.; Kamber, M. *Data mining: Concepts and Techniques*; Elsevier: Amsterdam, The Netherlands, 2011.

# An Improved Multi-label Classifier Chain Method for Automated Text Classification

Adeleke Abdullahi<sup>1</sup>

Noor Azah Samsudin<sup>2</sup>

Software Engineering Department  
Universiti Tun Hussein Onn  
Malaysia (UTHM)  
Batu Pahat, Malaysia

Shamsul Kamal Ahmad Khalid<sup>3</sup>

Information Security Department  
Universiti Tun Hussein Onn  
Malaysia (UTHM)  
Batu Pahat, Malaysia

Zuhaila Ali Othman<sup>4</sup>

Center for Artificial Intelligence  
Technology  
National University of Malaysia  
(UKM)  
Selangor, Malaysia

**Abstract**—Automated text classification is the task of grouping documents (text) automatically into categories from a predefined set. The conventional approach to classification involves mapping a single class label each to a data point (instance). In multi-label classification (MLC), the task is to develop models that could predict multiple class labels to a data instance. There exist several MLC methods such as classifier chain (CC) and binary relevance (BR). However, there are drawbacks with these methods such as random label sequence ordering issue. This study attempts to address this issue peculiar with the classifier chain method. In this paper, a hybrid heuristic evolutionary-based technique is proposed. The proposed PSOGCC is a combination of particle swarm optimization (PSO) and genetic algorithm (GA). Genetic operators of GA are integrated with the basic PSO algorithm for finding the global best solution representing an optimized label sequence order in the chain classifier. In the experiment, three MLC methods: BR, CC, and PSOGCC are implemented using five benchmark multi-label datasets and five standard evaluation metrics. The proposed PSOGCC method improved the predictive performance of the chain classifier by obtaining the best results of 98.66%, 99.5%, 99.16%, 99.33%, 0.0011 accuracy, precision, recall, *f1 Score*, and Hammingloss values, respectively.

**Keywords**—Text classification; multi-label classification; classifier chain; particle swarm optimization; genetic algorithm

## I. INTRODUCTION

Automated text classification (ATC) is the task of developing predictive models capable of categorizing text documents into distinct class labels from a predefined set. In other words, ATC is a technique that involves the process of managing and processing a vast number of documents in a continually increasing form. Conventionally, classification technique [1]–[3] focuses on the development of predictive model, a function that learnt to map an input  $x$  to an output  $y$ , *i. e.*,  $f: x \rightarrow y$ . This traditional approach to classification is otherwise termed single-label classification (SLC). Unlike the classical SLC technique, where an instance of a data sample is associated with a single class label, multi-label classification (MLC) [4]–[6] involves the problem of assigning to a data point (instance) multiple class labels simultaneously.

Given an input vector  $x = [x_1, x_2, \dots, x_n]^T$  and a vector of labels  $y = [y_1, y_2, \dots, y_k]^T$ , the goal of MLC is to build a model applicable in predicting one or more class labels

simultaneously provided the labels are not mutually exclusive. The multi-label classification concept primarily originated from text [5]. In a real-world scenario, a document (such as news article) could have multiple themes (topics) like entertainment, business, security, health, science, etc. To automate the categorization of such related textual data, MLC methods and techniques have been proposed. The existing MLC techniques could be broadly categorized into two approaches [6]: problem transformation and algorithm adaptation.

In problem transformation (PT) approach, the strategy involves transforming a multi-label problem into multiple single-label problems and learn one of the SLC algorithms (or classifiers) such as decision trees, for modeling the membership class (label). Subsequently, a new observation (test instance) is then predicted by combining the output of the positive predictions from the baseline classifiers. The PT strategy [7] is a very straightforward, easy, and flexible multi-label classification approach. Most of the conventional MLC algorithms such as binary relevance (BR), label powerset (LP), calibrated label ranking (CLR), and classifier chain (CC) adopt the PT strategy for MLC tasks.

Algorithm adaptation (AA) approach is based on inducing a conventional machine learning classification algorithm (single-label classifier) for multi-label problem. In other words, in AA strategy, a learning algorithm (classifier) such as support vector machine (SVM) is modeled and directly applied on MLC problems. This approach to MLC has been less applied by researchers due to its limitations such as lack of flexibility, complexity [8]. Notable algorithms that have adopted AA approach include ML- $k$ NN, BP-MLL, and BR- $k$ NN.

Classifier chain (CC) [9] [10] is one of the conventional MLC methods based on the problem transformation approach. The method is a direct extension of binary relevance (BR), developed to address the issue of label correlations. In BR, labels are taken as independent classifiers; hence the algorithm ignores labels inter-correlations. However, CC models consider labels as a chain-like structure, allowing communication (*i. e.*, sharing of predictions) among the underlying classifiers. The multi-label classification method has shown to be very competitive, achieving better classification results compared to other classical MLC methods such as BR [9].

Although, CC algorithm has been widely applied to several applications [11], [12]–[17], the method suffers from a major setback, which is the labels ordering issue [11], [12]. The conventional CC method adopts a random approach for labels sequence ordering, but studies have shown that the random labels sequence ordering may affect the performance of the classification method [11]. Attempts have been made to improve the original CC method, particularly to address the random labels sequence ordering issue, with several CC extensions proposed. This work attempts to further improve the standard CC method using a new alternative approach. In this paper, a hybrid heuristic evolutionary-based technique is proposed. The proposed PSOGCC optimization technique is a combination of particle swarm optimization (PSO) and genetic algorithm (GA).

The contributions of this work are grouped into three folds. First, we proposed an improved multi-label classifier chain method based on hybrid heuristic evolutionary techniques. Second, the proposed PSOGCC method is successfully demonstrated with standard benchmark multi-label datasets. Third, several conventional metrics are exhaustively employed to validate the performance of the proposed method against standard BR and CC methods in terms of Accuracy, Precision, Recall,  $f$ -Measure, and Hammingloss.

The rest of this paper is organized as follows. Section 2 reviewed related works, with focus on multi-label classifier chain method. Section 3 documented the experiment and method, and Section 4 presented the classification results. Section 5 concluded with direction to future works.

## II. RELATED WORKS

MLC is an emerging, growing field in the area of machine learning and data mining. MLC methods and techniques have been applied to various application domains including [4], [6], [18]–[20].

Specifically, there have been a growing number of works [11], [17], [21], [22] based on implementing and improving the multi-label classifier chain method. As aforementioned, CC is an extension of the classical BR method. The classifier chain method improved on BR by taking into consideration label correlations. The method works by modeling a set of binary classifiers (learning phase) based on the random label sequence ordering defined in the chain. The learning algorithm is then used to predict (a target label) taking into consideration the predictions of preceding labels in the chain. Given a new observation (prediction phase), the classifier makes prediction (following same procedure in the learning phase), by combining all positive predictions (outputs) of the classifiers. The performance of CC is sensitive to the label sequence order, which may be likely prone to “error propagation” in the chain. Several attempts have been made to overcome the limitations of CC.

In [23] an efficient label ordering approach was proposed for improving multi-label classifier chain accuracy. The proposed approach is based on exploiting semantic relationships among labels. The method achieved better

accuracy compared to the original CC method. Also, a decision function based on Bayesian network was proposed in [24] for multi-label classifier chain. Similarly, [22] employed the use of Bayesian network based on conditional entropy for discovering label correlation and order of labels in the chain classifier. The author in [25] proposed an improved classifier chain method based on conditional likelihood maximization. A  $k$  dependence classifier chains with label-specific function was developed. The method is shown to be effective. A cost-sensitive CC method was proposed in [12] for selecting low-cost features in multi-label classification. The method combined classifier chain with logistic regression dimensionality reduction technique.

In this paper, a hybrid heuristic evolutionary-based technique is proposed for improving the performance of multi-label classifier chain method. Heuristic techniques [26]–[30] are a set of intelligent self-learning algorithms developed to search for the optimum (best) solution to an optimization problem. Evolutionary-based heuristic methods are optimization algorithms that mimic the natural biological process (nature) in finding solutions to optimization problems. Most common and widely applied of the evolutionary-based optimization algorithms include: genetic algorithm, PSO, differential evolution, ant colony optimization algorithm, bee optimization algorithm, artificial immune system, cuckoo search, firefly algorithm, and tabu search algorithm.

The proposed technique applied in this work combined PSO and GA for finding the global solution that best represents an optimized label sequence order in the chain. Genetic operators: selection, crossover, and mutation, were integrated into the basic PSO algorithm for improving the search process, updating and maintaining diversity of the population (solutions). Details of the research methodology are presented in the next section.

### A. PSO Algorithm

Particle swarm optimization (PSO) is a population-based heuristic algorithm developed by Eberhart and Kennedy for solving optimization problems. The heuristic algorithm was influenced by the social behavior of species of animals such as birds flocking, fish schooling etc. In PSO algorithm (shown in Algorithm 1), a population entity called particle is assigned with position and velocity. A particle is a potential solution to a given problem. Each of the particles, represented as  $D$ -dimensional vector, moves around in the solution space, adjusting its position and velocity at every iteration using Eqn (1) and (2) respectively. Each particle has memory and remembers its previous best position  $pbest$  based on its experience. The global best represented as  $gbest$  is the collective best position in the swarm. Each particle knows the global best and move towards it. The performance of each particle (at every successive iteration) is measured using a fitness function.

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (1)$$

$$v_i(t+1) = wv_i(t) + c_1r_1[p_i(t) - x_i(t)] + c_2r_2[p_g(t) - x_i(t)] \quad (2)$$

where  $i = 1, 2, \dots, N$ ;  $t = 1, 2, \dots, T$ ;  $N$  represents swarm size and  $T$  is the maximum iteration limit;  $p_i$  and  $p_g$  are the local and global best solutions respectively;  $c_1$  and  $c_2$  are two acceleration constants in the value  $[0,1]$ ;  $r_1$  and  $r_2$  are two random numbers in the value  $[0,1]$ ;  $w$  is the inertia weight (which balances between local and global search);  $x_i(t)$  is the position of the particle and  $v_i(t)$  is the velocity of the particle at  $t$ -th iteration; particle ( $i^{th}$ ) position is denoted as  $x_i(t) = (x_{i1}, x_{i2}, \dots, x_{iD})$ , and velocity ( $i^{th}$ ) is denoted as  $v_i(t) = (v_{i1}, v_{i2}, \dots, v_{iD})$ .

```

Algorithm 1: Standard PSO Pseudocode

Step 1: Initialize population of particles with random
positions  $x$  and velocities  $v$ , swarm size  $s$ 
Step 2: For each particle, let  $pbest = x$ 
Step 3: calculate particles fitness  $f(x)$ ; update  $gbest$ 
Step 4: while (termination criterion is not met)
Step 5: For  $i = 1$  to  $S$ 
Step 6: calculate the new velocity using Eq (3.1)
Step 7: calculate the new position using Eq (3.2)
Step 8: calculate  $f(x)$  of each particle
Step 9: if ( $f(x) < f(pbest)$ )  $pbest = x$ 
Step 10: if ( $f(pbest) < f(gbest)$ )  $gbest = pbest$ 
Step 11: end For
Step 12: end For
Step 13: show the best solution found ( $gbest$ )
    
```

**B. GA Algorithm**

Genetic Algorithm (GA) is a global search optimization algorithm developed by Holland and based on the concept of natural selection adopted from the principle of Charles’ Darwin theory of evolution. GA is one of the most important and successful evolutionary-based heuristic method. The algorithm has been widely applied to several application problems [31]–[33]. The algorithm uses genetic operators: selection (or reproduction), crossover (or recombination), and mutation, to find (or produce) the global best solution to a given problem.

The evolutionary-based algorithm works (refer to Fig. 1) by first generate random initial population. At each generation, the quality of individuals (candidate solutions) is validated using a defined fitness function. Selection operator is applied to identify (select) individuals from the current generation based on the best fitness values. The process is improved through crossover and mutation operators until a new (better) population is created. The search ends with a termination criterion when the maximum iteration limit is reached or the best solution is found.

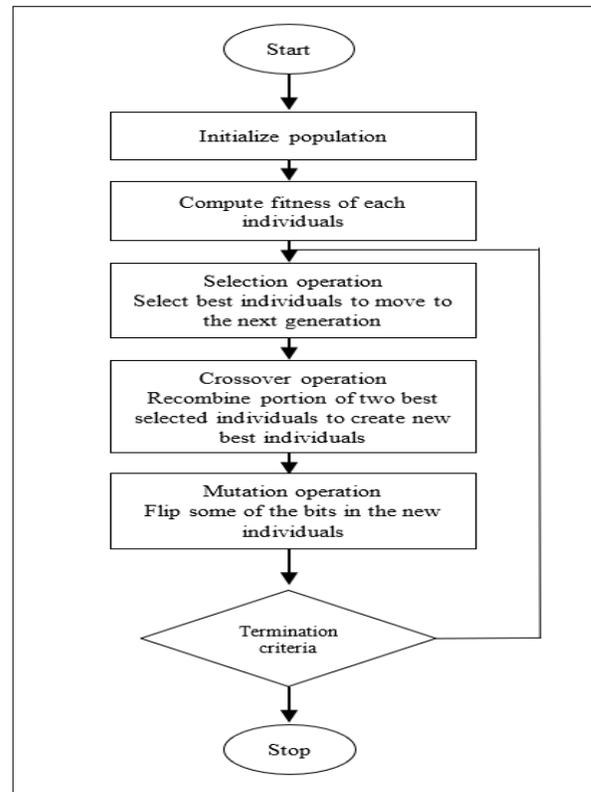


Fig. 1. Standard Genetic Algorithm.

**III. METHODOLOGIES**

In this paper, the experimental work comprises of four phases. These include input (data), preprocessing, classification, and output (results).

The experimental work is carried out using 5 benchmark multi-label datasets from Mulan (an open source library for multi-label classification problem). The standard datasets (in Table I) are from the most commonly experimented MLC datasets. The input data is preprocessed using StringToWordVector filtering tool and Term frequency inverse-document frequency (TFIDF). These are from the standard preprocessing techniques often applied in machine learning problems. The preprocessed data is stored in ARFF (Attribute-Relation File Format), the standard file format for machine learning using Mulan and Weka.

TABLE I. BENCHMARK ML DATASETS (WITH  $D$  = NO OF FEATURES;  $Q$  = NO OF CLASS LABELS;  $lc$  = LABEL CARDINALITY)

Dataset	Doman	#Instances	$D$	$Q$	$lc$
enron	Text	1702	1001	53	3.378
birds	Multimedia	645	260	19	1.014
flags	Image	194	19	7	3.392
genbase	Text	662	1186	27	1.252
yeast	Text	2417	103	14	4.237

### A. Proposed PSOGCC Multi-label Classification Method

The proposed MLC method is based on the concept of heuristic optimization technique, where the goal is finding the optimum solution to the search problem. The PSOGCC method (as shown in Fig. 2) is a hybrid of PSO and GA. The combined heuristic techniques are used to find the global best solution that best represents an optimized label sequence order in the chain classifier. PSO is an efficient, simple optimization algorithm and GA is a powerful, robust global search algorithm. Genetic operators: selection, crossover, and mutation, are applied for the population updates and reproduction of new generations (individuals).

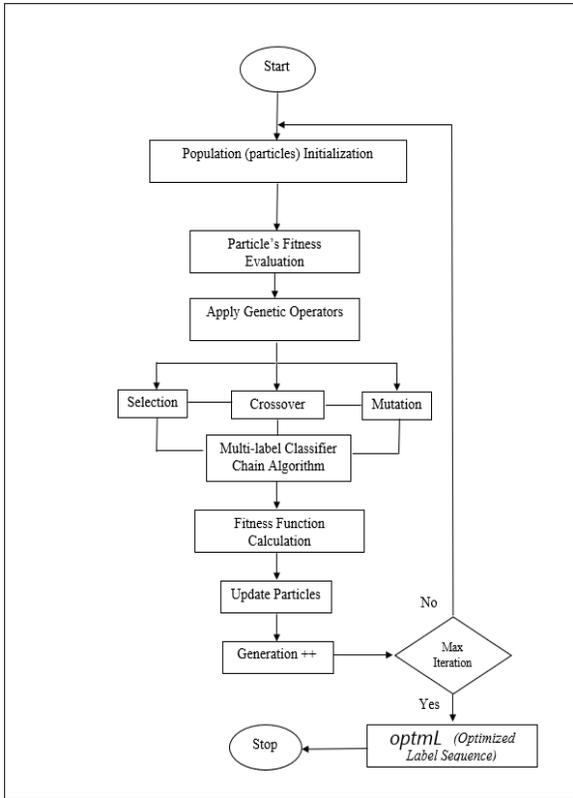


Fig. 2. Proposed PSOGCC Multi-label Classification Approach.

In PSOGCC (as shown in Algorithm 2), the optimization algorithm takes as input a training set  $T$  and produces as output an optimized label sequence  $optmL$ , representing the global optimum solution found in the chain. The entire algorithmic process could be broadly categorized into two: PSO loop (1 – 7) and GA loop (9 – 20).

In the first phase (*PSO loop*), population of particles (also called individuals) is initialized randomly with position  $x$ , velocity  $v$ , and swarm size  $s$ . Individual particles are represented as  $k$ - dimensional vectors (where  $k$  is equivalent to the number of predefined labels). The particles are encoded as integers representing label sequence indexes in the range value  $[1, q]$ . Individual particle's previous best position  $pbest$  is initialized with a copy of its current position  $x$ . The quality of particles is assessed using a defined fitness function  $f(x)$  in

Eq (3). Subsequently, the global best  $gbest$  is initialized with the index of the best fitted particle.

#### Algorithm 2: Pseudocode of the Proposed PSOGCC model

Input:  $T$  (training set)

Output:  $optmL$  (an optimized label sequence)

Step 1: Initialize population of particles (potential candidate solutions representing the label sequences) with random positions  $x$ , velocities  $v$ , and swarm size  $s$ . Set the particle's previous best position to the current position ( $pbest = x$ )

Step 2: Given a training set  $T$

Step 3: **For** all particles (label sequences) in the population **do**

Step 4: Build the classifier chain (CC) model (using standard **10 – fold** cross validation)

Step 5: Compute the particle's fitness  $f(x)$  using Eq (3)

Step 6: Update the population  $pbest$  and set the best particle  $gbest$  to the current population

Step 7: **end For**

Step 8: **repeat**

Step 9: Partition the training set  $T$  into **buildSet** and **validationSet**

Step 10: **For** all particles (candidate label sequence  $i$ ) in the current population **do**

Step 11: Construct the CC model using **buildSet** and label sequence  $i$

Step 12: Evaluate the fitness (quality) of the CC model using the **validationSet** and the fitness function  $g(x)$  defined in Eq (4)

Step 13: Apply Genetic operators:

Step 14: Using Tournament selection approach **SELECT** parents (particle with best fitness value)

Step 15: Generate new particles (child) from the old ones (parents) with **CROSSOVER** operator

Step 16: Apply **MUTATION** procedure (to the offspring)

Step 17: Update particles and population using **elitism age – based replacement** approach

Step 18: **end For**

Step 19: **Until (Max iterations (generations) reached)**

Step 20: return  $optmL$  (optimum solution rep labeled-ordered sequence)

In the second phase (*GA loop*), standard genetic operators: selection, crossover, and mutation, are applied. Classifier chain (CC) models are built and further evaluated using the fitness function  $g(x)$  defined in Eq (4). Genetic tournament selection strategy [34] is applied to select the best individuals to be recombined for producing a new generation (offspring). Order crossover operation [35] is performed using the selected individuals, resulting in the generation of new individuals. Thereafter, mutation operator is applied on the new individuals in order to avoid being trapped in the local minima. Age-based elitism replacement approach [36] is employed to replace the old generation with new ones while preserving a small group (elite individuals) in the population. This helps to improve and maintain diversity in the population. The PSOGCC implementation ends with the termination criteria and the global best solution  $optmL$  representing an optimized label sequence order in the chain classifier is returned.

$$Fitness f(x) = (\alpha * Acc) + (\beta * (\frac{N-T}{N})) \quad (3)$$

$$Fitness g(x) = \frac{(1 - (\frac{HL}{gMean})) + Acc + EM + F1}{N} \quad (4)$$

( $\alpha$  &  $\beta$ ) are control parameters (for balancing the trade-offs of particle's  $gbest$ ,  $gworst$ ,  $pbest$ , and  $pworst$ );  $Acc$  represents the accuracy of the baseline classifier; ( $N$  &  $T$ ) represent population size and neighborhood size, respectively.  $HL$ ,  $gMean$ ,  $Acc$ ,  $EM$ , and  $F1$  score are standard performance metrics.

#### IV. EXPERIMENTS AND RESULTS

This section details the experiments performed and the simulation results obtained. Five benchmark multi-label datasets with five conventional performance metrics were employed to validate the performance of the proposed PSOGCC method against the standard binary relevance (BR) and classifier chain (CC) multi-label classification algorithms. The classification results were compared in terms of: Accuracy ( $ACC$ ), Hammingloss ( $HL$ ), Precision ( $P$ ), Recall ( $R$ ), and  $f$ -Measure ( $F1$  score).

Accuracy ( $ACC$ ) [Eq 5] is a standard performance metric used to measure the correctly classified instances across data points. The higher the accuracy value, the better the classification algorithm. Precision [Eq 6], Recall [Eq 7], and  $f$ -Measure [Eq 8] are performance metrics often applied in classification problems to measure the degree of correctness of the positively classified instances. An effective classifier should have high precision, recall, and  $F1$  score. Lastly, Hammingloss [Eq 9] evaluation metric helps to measure the degree of incorrectness (misclassification) wrongly predicted by the classification algorithm. In general, a good classifier is one with high accuracy, precision, recall,  $F1$  score, and low Hammingloss values.

$$ACC = \frac{1}{N} \sum_{i=1}^N \frac{|Y_i \cap Z_i|}{|Y_i \cup Z_i|} \quad (5)$$

$$P = \frac{1}{N} \sum_{i=1}^N \frac{|Y_i \cap Z_i|}{|Z_i|} \quad (6)$$

$$R = \frac{1}{N} \sum_{i=1}^N \frac{|Y_i \cap Z_i|}{|Y_i|} \quad (7)$$

$$F1\ score = \frac{1}{N} \sum_{i=1}^N \frac{2|Y_i \cap Z_i|}{(Y_i) + (Z_i)} \quad (8)$$

$$HL = \frac{1}{N} \sum_{i=1}^N \frac{|Y_i \Delta Z_i|}{k}, |Y_i \Delta Z_i| \text{ denotes symmetric diff btw } Y_i \& Z_i \quad (9)$$

The three multi-label classification methods: PSOGCC, BR, and CC, produced competitive results. In Table II, the proposed PSOGCC achieved the highest accuracy result of 98.66% with the genbase multi-label dataset. Closely followed by the CC method with 98.15% accuracy while BR obtained 98.06%. From the accuracy results, it could be observed why the classifier chain (CC) outperformed the traditional BR algorithm. This is due to the limitation (associated with BR) of ignoring label correlations. Also, the proposed PSOGCC heuristic method outperformed the other two methods due to its combined advantages of considering label correlations and finding an optimized label sequence order, thereby addressing the limitation of the original CC method (i.e., random label sequence order in the chain).

Tables III to V presented the experimental results in terms of precision, recall, and  $f$ -Measure, respectively. Consistently, the proposed PSOGCC optimization algorithm outperformed both BR and CC multi-label methods. PSOGCC obtained the highest scores of 99.5%, 99.16%, and 99.33% precision, recall, and  $f1$  score respectively. These results further proved the effectiveness and superiority of the proposed method compared to the other two classical methods: binary relevance and classifier chain.

Finally, Table VI showed the Hammingloss values of the three classification methods obtained across the benchmark multi-label datasets. As aforementioned, Hammingloss metric helps to check the frequency of misclassification by the classifier. A good classifier should have less labels misclassified (i.e., low Hammingloss value). From the result, it could be seen that the proposed PSOGCC performed best compared to BR and CC. The method obtained the lowest Hammingloss value of 0.0011 with genbase dataset. The original CC method came second with 0.0102 Hammingloss value while BR performed the least (0.0121).

To further show a clearer and easier understanding of the classification results, the performance of the three MLC methods are presented in graphical forms as plotted in Fig. 3 to 7. The results comparisons showed the proposed PSOGCC had better performance across the multi-label datasets. This reflects the significance influence of finding an optimized label sequence order in the chain classifier.

TABLE II. CLASSIFICATION ( $ACC$ ) RESULTS OF PSOGCC, BR, AND CC

Datasets	Accuracy ( $ACC$ ) $\uparrow$		
	PSOGCC	BR	CC
enron	0.4046	0.3671	0.3671
birds	0.5515	0.5723	0.5725
flags	0.5586	0.5763	0.5700
genbase	0.9866	0.9806	0.9815
yeast	0.4537	0.4226	0.4219

TABLE III. CLASSIFICATION (P) RESULTS OF PSOGCC, BR, AND CC

Datasets	Precision (P) ↑		
	PSOGCC	BR	CC
enron	0.5959	0.6574	0.6576
birds	0.8153	0.8061	0.8064
flags	0.6741	0.6956	0.6943
genbase	0.9950	0.9947	0.9950
yeast	0.5796	0.5929	0.5950

TABLE IV. CLASSIFICATION (R) RESULTS OF PSOGCC, BR, AND CC

Datasets	Recall (R) ↑		
	PSOGCC	BR	CC
enron	0.4858	0.4481	0.4483
birds	0.6050	0.6403	0.6406
flags	0.6856	0.7741	0.7577
genbase	0.9916	0.9903	0.9908
yeast	0.6008	0.5613	0.5616

TABLE V. CLASSIFICATION (f1 Score) RESULTS OF PSOGCC, BR, AND CC

Datasets	f-Measure (f1 Score) ↑		
	PSOGCC	BR	CC
enron	0.5352	0.5329	0.5331
birds	0.6946	0.7137	0.7140
flags	0.6798	0.7328	0.7246
genbase	0.9933	0.9925	0.9928
yeast	0.5900	0.5767	0.5778

TABLE VI. CLASSIFICATION (HL) RESULTS OF PSOGCC, BR, AND CC

Datasets	Hammingloss (HL) ↓		
	PSOGCC	BR	CC
enron	0.0535	0.0540	0.0542
birds	0.0521	0.0515	0.0515
flags	0.2857	0.2747	0.2654
genbase	0.0011	0.0121	0.0102
yeast	0.2642	0.2588	0.2579

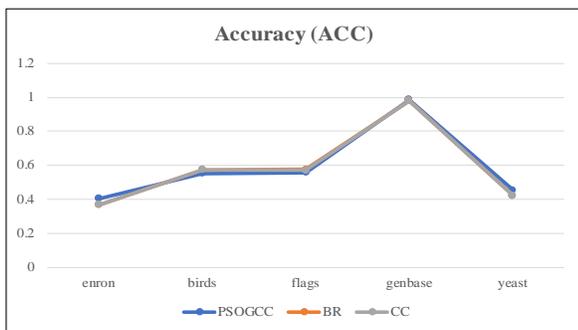


Fig. 3. Comparison of PSOGCC, BR, and CC in Terms of Accuracy.

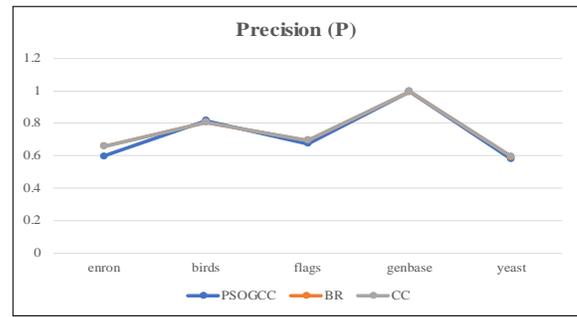


Fig. 4. Comparison of PSOGCC, BR, and CC in Terms of Precision.

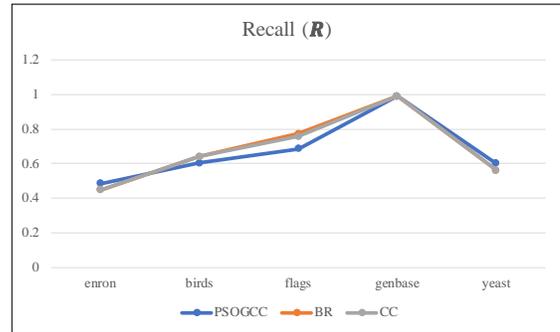


Fig. 5. Comparison of PSOGCC, BR, and CC in Terms of Recall.

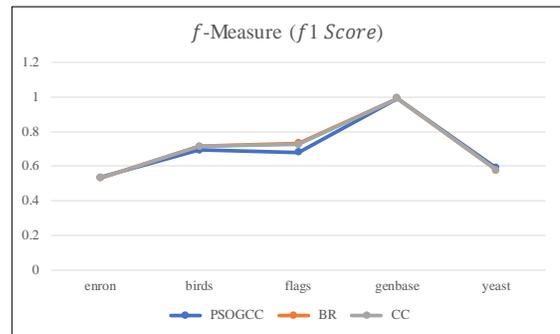


Fig. 6. Comparison of PSOGCC, BR, and CC in Terms of f1 Score.

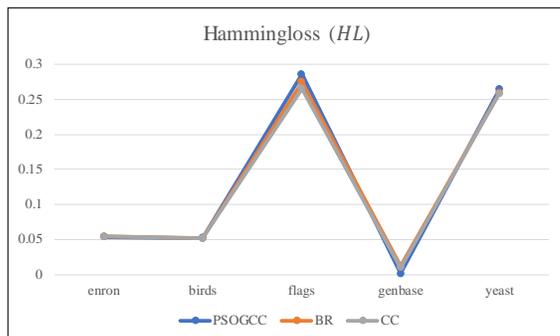


Fig. 7. Comparison of PSOGCC, BR, and CC in Terms of Hammingloss.

## V. CONCLUSION

Single-label classification (SLC) involves predicting a single class (output) for a particular data instance (input) whereas in multi-label classification (MLC), the task is to develop predictive models capable of assigning multiple class

labels simultaneously (to a single instance). In MLC, there are standard methods such as binary relevance (BR), classifier chain (CC), and label powerset (LP). There exist limitations with these methods such as ignoring label correlations (associated with BR), complexity (associated with LP), and random label ordering (associated with CC). This study attempted to improve the predictive performance of the multi-label CC method. In this work, the randomized label sequence order issue of CC is addressed. To achieve this, the study proposed a hybrid heuristic evolutionary-based technique.

Heuristic techniques involve developing a set of intelligent self-learning algorithms designed for finding the optimal best solution to an optimization problem. In this paper, PSOGCC multi-label classification method is proposed to extend the original CC method. The evolutionary-based algorithm is a combination of particle swarm optimization (PSO) and genetic algorithm (GA). The proposed PSOGCC method is used to find the global best solution representing an optimized label sequence order in the chain classifier. Genetic operators: selection, crossover, and mutation were integrated with the basic PSO for optimizing the search problem.

The experiment was conducted using five benchmark multi-label datasets. Furthermore, five evaluation metrics were applied to validate the performance (predictions) of the proposed PSOGCC against standard BR and CC methods. Results were presented in Tables II to VI in terms of accuracy, precision, recall,  $f$ -measure, and Hammingloss respectively. The proposed PSOGCC achieved the overall best classification results of 98.66%, 99.5%, 99.16%, 99.33%, 0.0011 accuracy, precision, recall,  $f$ -measure, and hammingloss values respectively.

In the future work, the proposed technique will be further validated using more multi-label datasets. Also, it is recommended to compare the performance of PSOGCC against other standard MLC algorithms. Finally, the research study will be further extended to employ other recent heuristic evolutionary-based techniques such as bat algorithm, whale optimization algorithm, and firefly algorithm etc.

#### ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education, Malaysia for supporting this research under Fundamental Research Grant Scheme Vot K213 (FRGS/1/2019/ICT02/UTHM/02/2) and Universiti Tun Hussein Onn Malaysia for Multidisciplinary Research, Vot H511.

#### REFERENCES

- [1] M. Iqbal, S. Ali, M. Abid, F. Majeed, and A. Ali, "Artificial Neural Network based Emotion Classification and Recognition from Speech," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 12, pp. 434–444, 2020.
- [2] A. K. Dehariya and P. Shukla, "Medical Data Classification using Fuzzy Main Max Neural Network Preceded by Feature Selection through Moth Flame Optimization," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 12, pp. 655–662, 2020.
- [3] A. Abdullahi, N. A. Samsudin, M. R. Ibrahim, M. S. Aripin, S. K. A. Khalid, and Z. A. Othman, "Towards IR4.0 implementation in e-manufacturing: Artificial intelligence application in steel plate fault detection," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 430–436, 2020.
- [4] M. Jethanandani, A. Sharma, T. Perumal, and J.-R. Chang, "Multi-label classification based ensemble learning for human activity recognition in smart home," *Internet of Things*, vol. 12, 2020.
- [5] A. Blanco, A. Casillas, A. Pérez, and A. Diaz de Ilarraza, "Multi-label clinical document classification: Impact of label-density," *Expert Syst. Appl.*, vol. 138, 2019.
- [6] Y. Xia, K. Chen, and Y. Yang, "Multi-label classification with weighted classifier selection and stacked ensemble," *Inf. Sci. (Ny)*, 2020.
- [7] M. Pushpa and S. Karpagavalli, "Multi-label Classification: Problem Transformation methods in Tamil Phoneme classification," *Procedia Comput. Sci.*, vol. 115, pp. 572–579, 2017.
- [8] B. Al-Salemi, M. Ayob, G. Kendall, and S. A. M. Noah, "Multi-label Arabic text categorization: A benchmark and baseline comparison of multi-label learning algorithms," *Inf. Process. Manag.*, vol. 56, no. 1, pp. 212–227, 2019.
- [9] J. Read and L. Martino, "Probabilistic regressor chains with Monte Carlo methods," *Neurocomputing*, vol. 413, pp. 471–486, 2020.
- [10] P. Teisseyre, "Classifier chains for positive unlabelled multi-label learning," *Knowledge-Based Syst.*, vol. 213, 2021.
- [11] X. Jun, Y. Lu, Z. Lei, and D. Guolun, "Conditional entropy based classifier chains for multi-label classification," *Neurocomputing*, vol. 335, pp. 185–194, 2019.
- [12] P. Teisseyre, D. Zufferey, and M. Słomka, "Cost-sensitive classifier chains: Selecting low-cost features in multi-label classification," *Pattern Recognit.*, vol. 86, pp. 290–319, 2019.
- [13] F. Bellmann, L. Bunzel, C. Demus *et al.*, "Multi-Label Classification of Blurbs with SVM Classifier Chains," *Proc. 15th Conf. Nat. Lang. Process. (KONVENS 2019)*, pp. 293–299, 2019.
- [14] Z. Wang, T. Wang, B. Wan, and M. Han, "Partial classifier chains with feature selection by exploiting label correlation in multi-label classification," *Entropy*, vol. 22, no. 10, pp. 1–22, 2020.
- [15] W. Weng, D. H. Wang, C. L. Chen, J. Wen, and S. X. Wu, "Label Specific Features-Based Classifier Chains for Multi-Label Classification," *IEEE Access*, vol. 8, pp. 51265–51275, 2020.
- [16] Z. Yu, H. Hao, W. Zhang, and H. Dai, "A Classifier Chain Algorithm with K-means for Multi-label Classification on Clouds," *J. Signal Process. Syst.*, vol. 86, no. 2–3, pp. 337–346, 2017.
- [17] L. Sun and M. Kudo, "Optimization of classifier chains via conditional likelihood maximization," *Pattern Recognit.*, vol. 74, pp. 503–517, 2018.
- [18] R. Wang, S. Ye, K. Li, and S. Kwong, "Bayesian network based label correlation analysis for multi-label classifier chain," *arXiv*, vol. 554, pp. 256–275, 2019.
- [19] E. K. Y. Yapp, X. Li, W. F. Lu, and P. S. Tan, "Comparison of base classifiers for multi-label learning," *Neurocomputing*, vol. 394, pp. 51–60, 2020.
- [20] S. Nazmi, X. Yan, A. Homaifar, and E. Doucette, "Evolving multi-label classification rules by exploiting high-order label correlations," *Neurocomputing*, vol. 417, pp. 176–186, 2020.
- [21] T. T. Nguyen, M. T. Dang, A. V. Luong, A. W. C. Liew, T. Liang, and J. McCall, "Multi-label classification via incremental clustering on an evolving data stream," *Pattern Recognit.*, vol. 95, pp. 96–113, 2019.
- [22] R. Wang, R. Ridley, X. Su, W. Qu, and X. Dai, "A novel reasoning mechanism for multi-label text classification," *Inf. Process. Manag.*, vol. 58, no. 2, 2021.
- [23] B. Liu and G. Tsoumakas, "Dealing with class imbalance in classifier chains via random undersampling," *Knowledge-Based Syst.*, vol. 192, 2020.
- [24] T. Ali and S. Asghar, "Efficient Label Ordering for Improving Multi-label Classifier Chain Accuracy," *J. Natn. Sci. Foundation Sri Lanka*, vol. 47, no. 2, pp. 175–184, 2019.
- [25] G. Varando, C. Bielza, and P. Larrañaga, "Decision functions for chain classifiers based on Bayesian networks for multi-label classification," *Int. J. Approx. Reason.*, vol. 68, pp. 164–178, 2016.
- [26] X. Chu *et al.*, "An artificial bee colony algorithm with adaptive heterogeneous competition for global optimization problems," *Appl. Soft Comput. J.*, vol. 93, 2020.

- [27] H. S. Alhadawi, D. Lambić, M. F. Zolkipli, and M. Ahmad, "Globalized firefly algorithm and chaos for designing substitution box," *J. Inf. Secur. Appl.*, vol. 55, 2020.
- [28] H. Wang, X. Lang, and W. Mao, "Voyage optimization combining genetic algorithm and dynamic programming for fuel/emissions reduction," *Transp. Res. Part D Transp. Environ.*, vol. 90, 2020.
- [29] N. Taheranpour and S. Talebi, "Development of a new efficient method using genetic algorithm for increasing of fuel rod life time," *Prog. Nucl. Energy*, vol. 131, 2020.
- [30] J. Liu, X. Ma, X. Li, M. Liu, T. Shi, and P. Li, "Random convergence analysis of particle swarm optimization algorithm with time - varying attractor," *Swarm Evol. Comput.*, vol. 61, 2020.
- [31] E. T. Bacalhau, L. Casacio, and A. T. de Azevedo, "New hybrid genetic algorithms to solve dynamic berth allocation problem," *Expert Syst. Appl.*, 2020.
- [32] A. Santiago, B. Dorronsoro, H. J. Fraire, and P. Ruiz, "Micro-Genetic algorithm with fuzzy selection of operators for multi-Objective optimization:  $\mu$ FAME," *Swarm Evol. Comput.*, vol. 61, 2019.
- [33] A. Singh and A. Khamparia, "A hybrid whale optimization-differential evolution and genetic algorithm based approach to solve unit commitment scheduling problem: WODEGA," *Sustain. Comput. Informatics Syst.*, vol. 28, 2020.
- [34] Z. Li, J. Huang, and M. Ding, "Comparison and analysis of different selection strategies of genetic algorithms for fuel reloading optimization of Thorium-based HTGRs," *Nucl. Eng. Des.*, vol. 373, 2020.
- [35] B. Koohestani, "A crossover operator for improving the efficiency of permutation-based genetic algorithms," *Expert Syst. Appl.*, vol. 15, 2020.
- [36] S. Rani, B. Suri, and R. Goyal, "On the effectiveness of using elitist genetic algorithm in mutation testing," *Symmetry (Basel)*, vol. 11, no. 9, 2019.

# Efficient Task Scheduling in Cloud Computing using Multi-objective Hybrid Ant Colony Optimization Algorithm for Energy Efficiency

Fatima Umar Zambuk<sup>1</sup>, Abdulsalam Ya'u Gital<sup>2</sup>, Mohammed Jiya<sup>3</sup>  
Nahuru Ado Sabon Gari<sup>4</sup>, Badamasi Ja'afaru<sup>5</sup>, Aliyu Muhammad<sup>6</sup>

Department of Mathematical Sciences, Abubakar Tafawa Balewa University, ATBU, Bauchi, Nigeria<sup>1, 2, 3, 4, 5</sup>  
Department of Computer Science, Federal Polytechnic Bauchi, FedPoly, Bauchi, Nigeria<sup>6</sup>

**Abstract**—The efficiency of Internet services is determined by the Cloud computing process. Various challenges in computing are being faced, such as security, the efficient allocation of resources, which in turn results in the waste of resources. Researchers have explored a number of approaches over the past decade to overcome these challenges. The main objective of this research is to explore the task scheduling of cloud computing using multi-objective hybrid Ant Colony Optimization (ACO) with Bacterial Foraging (ACOFB) behavior. ACOFB technique maximized resource utilization (Service Provider Profit) and also reduced Makespan and user wait times Job request. ACOFB classifies the user job request in three classes based on the sensitivity of the protocol associated with each request, Schedule Job request in each class based on job request deadline and create a Virtual Machine (VM) cluster to minimize energy consumption. Based on comprehensive experimentation, the simulated results show that the performance of ACOFB outperforms the benchmarked techniques in terms of convergence, diversity of solutions and stability.

**Keywords**—Ant colony; scheduling; hybrid; foraging; cloud computing

## I. INTRODUCTION

Cloud computing proliferation has become a major issue with the omnipresent evolution of big data in its range, speed, and volume through the Internet. Autonomous computing, grid computing, distributed computing, and utility computing consist of cloud computing [1]. Cloud computing offers high performance storage facilities and highly flexible on-demand computing. With the massive increase in energy usage is the major issue faced in cloud data centers.

In order to enhance the overall efficiency of cloud computing, task planning is an essential step. The conventional centralized framework for managing and tracking cloud resources has been widely used in enterprise environments. As such, due to the heterogeneous and large-scale data, supervision and checking systems in multiple data centers have faced serious challenges [2]. The first paper to address the planning problem of the heterogeneous system for energy consumption by means of multi-objective hybrid ACO and bacteria foraging algorithm in the IaaS cloud is this study.

Researchers have recently concentrated more on addressing the issue of task scheduling in a distributed environment. Task scheduling is considered a critical problem

in the world of cloud computing by considering different variables such as power consumption, fault tolerance, the overall cost of performing the tasks of all users, completion time and use of resources. Task scheduling has been shown to be a full NP problem [3], which make it impossible to achieve solutions easily. The issue of finding the best balance between the tenacity time and the energy required by a precedence-constrained corresponding application is a bi-objective optimization problem. This issue can be solved by a set of Pareto points [4]. Pareto strategies are those for which only one goal can be strengthened with the deterioration of at least one other goal. Thus, the solution to a bi-objective problem is a (possibly infinite) set of Pareto points instead of a particular solution to the problem.

Internet forms a connection of large group of servers in cloud data centers. Thus, task schedulers are needed in the cloud data centers for the organization of task executions. A good task scheduler must efficiently utilize cloud data center resources for task execution. A scheduler should be able to use less resources and time to execute tasks. The scheduling algorithm's efficiency problems include makespan and energy consumption. In fact, using fewer resources ensures that it uses less energy. The minimization of makespan and energy consumption is one of the major problems for building large-scale clouds.

Different studies have been carried out in [5] to exploit the diversity of makespan and energy usage in cloud computing. These studies are that in [4] scheduling techniques and algorithms for particular tasks have been developed and implemented, fault-tolerant tasks with real-time deadlines and energy-efficient tasks with dependence. At the design time, the optimization goals set statically constructed monolithic virtual machines (VMs) cluster for task scheduling that lacks flexibility and adaptability in changing resource provisioning, classification of workloads and environmental cloud execution. As the study failed to address convergence, diversity and stability, resulting in too much wasting of resources, there is certainty about the inherent issue of resource availability and task scheduling. The majority of the techniques and algorithms for task planning and resource provisioning often apply to some widespread functional method that uses a comparable deterministic task execution system for various optimization goals.

However, incorporating new scheduling skills needs to be performed one at a time for the algorithm of scheduling, which is not only monotonous but also stochastic. As such, the aim of this study was to explore task scheduling using multi-objective hybrid Ant Colony Optimization (ACO) with Bacteria Foraging (BF) behavior in cloud computing. The ACOBF technique maximized the usage of services (profit from service providers) and also reduced Makespan and Job Request user waiting time. Based on the sensitivity of the protocol associated with each application, ACOBF will categorize user job requests into three classes, schedule job requests in each class based on the deadline for job requests, and create a VM cluster to minimize the amount of energy consumption.

The rest of this paper is structured as follows; Section 2 addresses the relevant reviews of other authors' literature on resource management and task scheduling, while Section 3 discusses the methodological processes. Then Section 4 considers implementation, results and discussions while section exposes conclusion and future works for upcoming researchers.

## II. REVIEW OF RELATED LITERATURE

The most fruitful ACO research in cloud computing nowadays is improving the quality of solution and convergence speed for energy efficiency. Researchers have attempted to explore these problems by metaheuristic hybridization or preprocessing of the input population, transfer operator adjustment, etc. [6]. In [2], combining two population-based meta-heuristics with identical characteristics will possibly strengthen the solution as one's strength would easily overpower the other's weakness. The authors have argued that by hybridizing ACO with another population-based metaheuristic for efficient exploration and exploitation by the search strategy, there is a greater chance of obtaining better solution outcomes. This section addresses many similar work analyses performed on various ACO approaches to resource provisioning by other researchers.

The ACO was adopted in [6] for resources allocation in cloud. The authors' objective function is to minimize makespan. The research looked into the relative weakness and strength of the search process by experimentation where assignment of VM's is based on a simple, short-term memory using constraint satisfaction rule for incoming batch jobs. VM migration from one PM to another was modeled using the Graph theorem such that PMs are represented with vertex (node) and edge defines the transition [7, 8]. The rule did not resolve the convergence problem arising from the existence of transition loops, plurality of solutions, and as such stability; too much energy was consumed in the datacenter. The authors in [9, 10] also researched Makespan minimization, where the authors attempted to balance cloud load for IaaS. The Heuristic Dependent Load Balancing Algorithm (HBLBA) proposed by the authors strategized tasks to configure servers for assigning VMs to process tasks in datacenters based on the incoming number of tasks and their sizes. Other minimization of makespan by ACO technique studied can be seen in [10-12].

A updated ACO algorithm [13] was proposed to obtain a Pareto solution package. An approximate non-deterministic tree-search method based on the ACO was inculcated by the researchers. This leads to simplifying the calculation of probability and also updating the pheromone law, which allows the learning capacity of ants to increase. In [14], a multi-objective ACO (MO-ACO) algorithm was proposed with the objective function considered to be load balancing, cost and minimization of makepan. The law did not discuss the dependence between convergence tasks, but instead used a limited number of tasks in their experiment, resulting in resource and energy wastage. In the primary step, current setbacks in ACO that include poor convergence accuracy, easy falling into optimal local solution and slow solving speed were found. The authors resolved the initial pheromone deficiency through the rapid search capability of the ACO with a spanning tree to increase the ACO's convergence speed. Solution diversity and consistency in convergence have not been discussed as a result of the lack of energy. Other metaheuristic population focused on an attempt to fix energy waste was seen in [15] where the authors used the general concept of ACO and the Clonal Selection Algorithm for task scheduling. The technique used for pattern recognition was based on the independence of the populations of memory cells and antigens. Two population-based techniques that failed to address convergence in their exploration and exploitation may lead to a search phase that ended in a local optima solution. Too much electricity was also lost.

[16] investigated the scheduling problem on the set of batch processing machines, which were arranged in a parallel with different processing capabilities. The jobs were aligned with different sizes, processing and releasing time. A bio-objective ACO is used to reduced makespan and total energy consumption. Also, [17] designed to examine the effect of the association of ACO in solving the problems of job scheduling. This book focused to introduce hybrid ACO as a solution to that effect, which was evaluated based on parameters; makespan time, delay (tardiness) and workload. In the same vein, [18] proposed a multi-objective hybrid ACO for real world two stage blocking permutation, flow shop scheduling problem in order to tackle the total energy cost as well as makespan based on the current market situation. The author in [19] proposed Ant Mating Optimization (AMO) to reduce total energy consumption and makespan for Fog Computing platform. The algorithm determines trade-off between system makespan and the consumed energy required established by the end user. This techniques out performs Particle Swarm Optimization (PSO), Bee Life Algorithm (BLA) and Genetic Algorithm (GA) in term of the parameters under examination. In another development [20] preemptive scheduling in a single machine is proposed to minimize total completion time, energy cost under the electricity period. ACO – DR, dominant ranking procedure.

## III. METHODOLOGY

By means of methods for searching, handling and ingesting food, natural selection aims to eradicate animals with poor foraging strategies. It favors the spread of the genes of those organisms with successful foraging strategies, because reproductive success is more likely to occur [16]. Bad

foraging techniques are either re-structured to succeed or eliminated after many years. Since the foraging activity of the animal/organism seeks to maximize energy intake per unit of time spent on foraging. Constraints considered to be cognitive and sensing capacities combined with environmental parameters (e.g. predator threats, prey density, search area physical characteristics) are optimized due to natural evolution. This basic concept has been extended to complex optimization problems. The problem quest room for optimization could be based on the social foraging system in which parameter groups work to solve difficult engineering issues [21].

In order to achieve the optimum local and worldwide solutions, the ACO's discovery and operating methods to forage algorithms for bacteria are used. The effectiveness of the proposed ACOBF multi-objective solution will be verified explicitly in terms of the function of multiplicity and excellence of solutions, convergence and constancy. The cloud service provider tracks the entry of customer demands for task processing and the use of PMs in the data center details (CSP). To have this user request scenario, the Direct Acyclic Graph (DAG) is followed. In this scenario, the relation between the task unit, the functionality and the work unit are captured.

The CPU-limited job which spends most of its time in calculating multiple RAM size processing parts will be the basic characteristics of the tasks is considered. Although I/O-bound tasks depend on only peripheral devices linked to computers. As such, it might be important to have a computer with a wide buffer capacity and enough network bandwidth. The adding of inputs and outputs to reserve the available resource in a pm is an essential feature of the task unit. Dependence can exist between the units of the mission. Fig. 1 depicts DAG, where each node is a task unit with its task form, the addressed line demonstrates the relationship of dependency between the tasks and add weight that links the edges to the flow size of two tasks. By using the following five times, the diagram can be seen:

$$G = (TD, TS, D, Mi, Mout) \quad (1)$$

TD is the user request collection consisting of task units (1/n).

TS are the assignment type for each only task unit (1/m);  $T_1, T_2, \dots, T_m$ ;  $T_m$  is the determined amount of assignment in a task unit.

D is task dependency that represents the dependencies between the task units in TD.

$M_i$  is the Input data representing the size of task unit.

$M_{out}$  is the Output data representing the size of task unit.

#### A. Assumptions

A remote location server or PC or a physical machine that forms the data center can be a heterogeneous resource pool

and services. There may be different configurations of the same tools with the similar mission but yet the results differ. The total heterogeneity features can be generalized by changing PM capacity and network bandwidth. By building a direct relationship between the available memory size and the Processor power, the capacity of the PM gives the minimum time taken to execute the data present in a task. The rate and price of data transmission between two physical devices are facilitated by network bandwidth. Instead of distinguishing between the types of activities, it deals only with data flow. M represents the resource information, consisting of six-tuples.

$$M = (PM, CP, R, CE, Nbw, Ecom) \quad (2)$$

PM is the set of physical machines inside a data center.

CP is the computing power of the PM. Here,  $(ES_{ij})$  denotes the implementation time of job of unit type i on a PM  $PM_j$ .  $ES_{avg;j}$  denotes the average power of  $PM_j$  as  $ES_{avg;j}$ ,

Computing the nasty of essentials in column of matrix  $ES_j$  produces  $ES_{avg;j}$  value

$$ES_{ij} = PM_1 \dots PM_j TD_1 \dots TS_{11} \dots TS_{1j} TD_i TS_{i1} \dots TS_{ij}$$

R is the available RAM (memory) size of each PM.

CE is the processing energy that gives the rate of a task unit's execution consumption. Here it is possible to denote the energy consumed by a  $PM_j$  to run I task unit form per unit time per unit data as  $CE_{ij}$ .

Nbw denotes the bandwidth between PMs and is known as  $Nbw_{;ij}$ , the data transmission rate between  $PM_i$  and  $PM_j$ .

Ecom denotes the energy consumption rate for the communication. Therefore,  $Ecom_{;ij}$  is the energy consumed during transmission of data from  $PM_i$  to  $PM_j$  per unit time per unit data.

#### B. Problem Formulation and Solution Domain

By highlighting the different models for the solution domain, the formulated problem is presented in this section. For optimizing resource scheduling in cloud computing, the two most important objectives considered are the minimization of makepan and energy consumption. The contradictory essence of these two priorities is created by heterogeneity and parallelism. The former states that reducing makespan at the cost of robust inter-PM data transmission directly affects the energy use of the data center and later explains that the quickest resource in existence is not necessarily the cheapest.

#### C. Modeling the Makespan

Makespan is the length taken from the moment when a user submits his request to the last task unit's completion time. The processing time of both waiting periods is necessary. By decomposing user requests into task units, the processing time is measured based on user request and then apply topological sorting to ensure that each task unit can only rely on those with lower priority indexes.

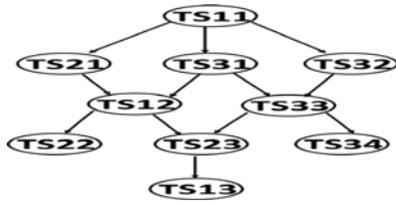


Fig. 1. DAG of Tasks and Task.

Task unit TDi's completion time is nearly the same as the overall processing time. For each TDi task unit, the CT(i) completion time is determined by adding the execution time of the current task unit and the time it takes to bring all the necessary data to the current PMP. Consider, for example, the DAG depicted in Fig. 1; The completion time of the TD8 task unit can be determined as the time when all input data for the TD8 task unit arrives (by adding the completion time of task unit TD8 and the processing time of TD5, TD6, and TD7).

$$CT(i)=T_c+T_{ex} \quad (3)$$

Where  $T_c$  is the time taken for all task arrival to current task given as

$$T(c) = Max + \sum_{j=1}^{i-1} \left( D_{i,j} * CT(j) + \frac{D_{ij} * MAXout}{NBw,p,q} \right) \quad (4)$$

P and q are execution start time and execution end time respectively.

$T_{ex}$  is the current task execution time;

$$T_{ex}=ES_{(g,h)}M_{i,j} \quad (5)$$

g and h are current task time and starting time respectively.

The waiting period is the sum of all processing times, because the degree of multi-threading is not too high when more task units are allocated or some PMs are overloaded. The significant attribute for task scheduling after deep analysis of the operation is the balance of load among the PMs in the data center. As such, proper information about the load distribution between the data center PMs is very important to obtain. Even if this information were measurable, the resource provider or cloud broker would not make it publicly accessible. Therefore, finding a solution to this issue is very vital. To this end, it assumed that the ratio on the load distribution at each PM average computing power and load distribution as follows:

#### Load Balancing

$$(LB) = \sum_{i=1}^n (A(i) - B(i))^2 \quad (6)$$

N here is the number of PMs in the data center

$$A(i) = \frac{\sum_{j=1}^m M_{i,j}|x(j)=1}{\sum_{j=1}^m M_{i,j}} \quad (7)$$

$$B(i) = \frac{R_i/EC_{average,i}}{\sum_{i=1}^n R_i/EC_{average,i}} \quad (8)$$

Some PMs that remain busy for a long time are made to push other tasks into the waiting queue, which adversely increases the system's makeup as it poses a risk with a deviation from the ideal ratio. Therefore, it is assumed that the

optimal ratio was taken into account for the initial load distribution. To this end, the prioritized load balancing for the task distribution, as the risk parameter has an indirect effect on the system's makespan. The new mathematical model for makespan will be given as:

$$CT_f = CT(n) * e^\theta \quad (9)$$

$\theta$  is the load balancing aspect increases as data traffic increases. The influence of various load distributions is also increased by Makespan. It is doubtful that the load balancing effect on the makespan reflecting the idleness of data traffic.

#### D. Modeling the Energy Consumption

The overall energy consumed in the data center is the amount of energy consumed by the individual PMs participating in the customer's service requests. CPU uses more energy than other components involved in the task scheduling process (Singh and Chana, 2016). The usage of energy is measured by the CPU using resources (voltages and frequencies). This means that as long as the working state of the CPU remains stable, energy consumption remains unchanged. The total energy consumed during computing and communication is measured as follows:

$$Tc=E_c+E_{ce} \quad (10)$$

$$E_c = \sum_{i=1}^{i=n} CE_{g,h}E_{com(g,h)}M_{i,j} \quad (11)$$

$$g=TD_i \text{ and } h=x(i) \quad (12)$$

$$E_{ce} = \sum_{i=1}^{i=n} \sum_{j=1}^{i-1} \frac{D_{j,i}M_{0,j}}{N_{bw(p,q)}} * E_{com(p,q)} \quad (13)$$

$$P=x(j), q=x(i) \quad (14)$$

It has been observed from this analysis the trade-off in minimizing makespan and energy. So, the multi-objective optimization problem for minimizing these conflicting parameters at topological sorting can be given in eq. 15, 16 and 17.

#### Minimization of Makespan

$$(CT_f) = Min (CT(n)*e^{\theta*LB}) \quad (15)$$

$$\text{Minimization of Energy } (T_c) = Min (T_c) \quad (16)$$

$$\text{Fitness function } \Omega = \alpha(CT(n)*e^{\theta*LB}) + \beta(T_c) \quad (17)$$

Where  $\alpha$  and  $\beta$  are weights to prioritize components of the fitness function such that  $0 \leq \alpha \leq 1$  and  $0 \leq \beta \leq 1$ .

#### IV. MULTI OBJECTIVE APPROACH

The ACO algorithm has excellent global search capability and, as such, a mediocre local search capability suffers from the curse of dimensionality [4]. BF has very high local search capabilities and low global search capability (Lin et al, 2013). It is assumed that a combination of the two algorithms will result in an outstanding solution with the best local and global search capabilities through a selective combination of some desirable functions, resulting in faster convergence time. ACOBF would have all the combined ACO and BF algorithm properties. Theoretically, BF that was hybridized with other algorithms other than ACO was tested to be successful, based

on the extensive literature reviewed. In all these literatures, also observed that the combinations retained general validity and optimized characteristics that can be used in many other contexts. The hybridized BF inherits both BF exclusion and swarming characteristics.

The aim here is to adjust BF features that do not help ACO's global search capabilities and implement BF's local search features. Swarming and elimination are the essential features of the method for searching for globalization that have to be substituted in the procedure while maintaining the functions of chemo taxis and reproduction in the local search. The parameter to be optimized is the bacteria's position (coordinate). In conclusion, the solution to task planning dilemma is a bacterium. Several bacteria for the algorithm input are created. To obtain minimum makespan and energy, the bacteria are also assessed against the objective function.

In a desirable range, the parameters are discretized, where and distinct set value represents a point in the space coordinates. Also, the separate values are defined by a point on the space coordinate. All bacteria are tested in the proposed ACOBF according to a solution consistency measure at the end of the iteration.

The primary objective is to minimize the use of makespan and energy consumption:

S: population number of bacteria,

C(i): random path taken during tumble,

N<sub>c</sub>: steps of chemotaxis,

N<sub>s</sub>: swimming length,

N<sub>re</sub>: steps of reproduction, N<sub>ed</sub>: events of elimination and dispersal;

P<sub>ed</sub>: likelihood of elimination and dispersal,

p: search space dimension.

---

Algorithm 1. Algorithm *positioning bacterium*

---

1.  $P = \{ \}, N_c = \{ \}, S = \{ \}$
2. For  $I = 1 : N$  do
3.  $P = \text{Protocol of Req}$ ;
4. For  $j = I : X$  do
5. Scan  $P_{ed}$  in Order;
6. If  $N_{re} = P$
7. Insert  $N_c$  Into Set  $N_s$ ;
8.  $\text{Count}_j = \text{Count}_j + 1$ ;
9. Break;
10. End if;
11. End For;
12. If  $N_{re} \neq \text{NULL}$ ;
13. Continue;
14. End if;
15. For  $k = 1 : Y$  do
16. Scan  $N_c$  in Order;
17. If  $N_c(k) = P$
18. Insert  $N_{ed}$  Into Set  $N_{re}$ ;
19.  $\text{Count}_k = \text{Count}_k + 1$ ;

20. Break
21. End if;
22. End For;
23. If  $C(e) \neq \text{NULL}$ ;
24. Continue;
25. End if;
26. Insert  $P_{ed}$  into C;
27. End For;

---

Algorithm 2. *ACOBFBased Task Scheduling Algorithm*

---

**Begin**

**Reproduction**

**Select:** Sort the bacteria on the basis of  $N_c$  accumulated during the chemeostasis steps

**Crossover:** perform crossover with leastfit bacteria in the colony

**Mutation:** Perform mutation in the position of the bacteria based on the ACO fraging behavior

**Dispersal and Elimination**

With probability  $P_{ed}$  disperse and eliminate each bacterium

**Termination**

End the program and output best performing bacterium position

**End**

---

## V. IMPLEMENTATION

### A. Experimental Setup

The simulation environment used for the experiment comprises of an Intel(R) Core i5 CPU (2.53 GHz Processor), Hard Drive of 500GB, Memory of 8.0GB Windows 8 OS, JDK8.1, Eclipse IDE and CloudSim version 3.0. The implementation process adopts and extends classes in CloudSim; DataCenterBroker, VM, Cloudlet (includes new parameters that defines the protocols associated with job request) and Host.

### B. Results and Discussion

1000 User Work Requests have been split into five groups of 200 Simulation Process Request tasks. For processing, each class is submitted to the system. To obtain the Makespan and the energy consumed, the average values of the five experimental results are computed. BF and Genetic Algorithms [22] were used in benchmarking to demonstrate the performance of ACOBF. In the same parameter configuration as ACOBF, both BF [23] and GA were also simulated. To measure the makespan and energy consumption of the Cloud task units, the environment with non-uniform and uniform parameters as a low PM heterogeneity was set. The efficacy of the algorithms is determined by the responds of different heterogeneous tasks and resources utilized:

Makespan time, as shown in Fig. 2 to 6, was recorded in seconds (due to cloudsim relative time unit) from the y-axis with the total number of tasks on the x-axis. This illustrates the difference with low system heterogeneity for non-uniform and uniform parameters. From the statistics, it is noted that ACOBF has the least makespan for non-uniform and uniform parameters as it is able to execute user job requests more

quickly. This has been done because of the ability of the algorithm to prioritize tasks that do not need to be postponed.

A task range of 10-200 has been used for the simulation of low PM heterogeneity. Fig. 7 to 11 demonstrates the impact on the energy consumption of the four heuristics in the case of low PM heterogeneity with non-uniform and uniform parameters. Unlike GA and BF, the statistics show that ACOBF achieves minimum energy consumption, resulting in the highest energy consumption in all task range situations.

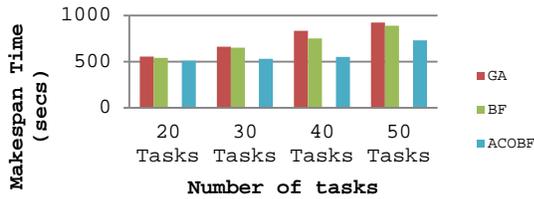


Fig. 2. Makespan Time for 20-50 Tasks.

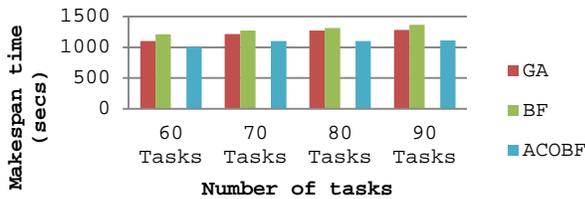


Fig. 3. Makespan Time for 60-90 Tasks.

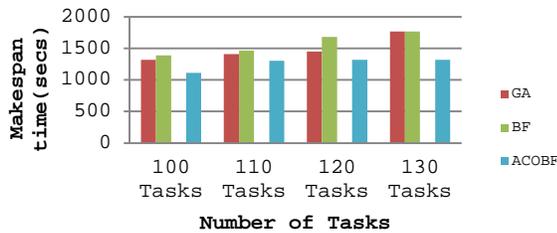


Fig. 4. Makespan Time for 100-130 Tasks.

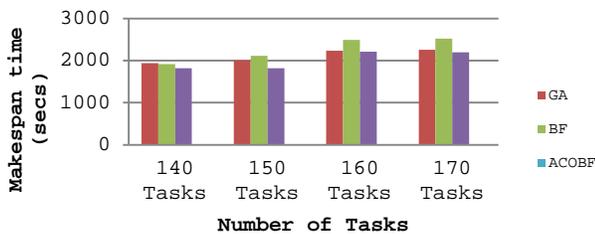


Fig. 5. Makespan Time for 140-170 Tasks.

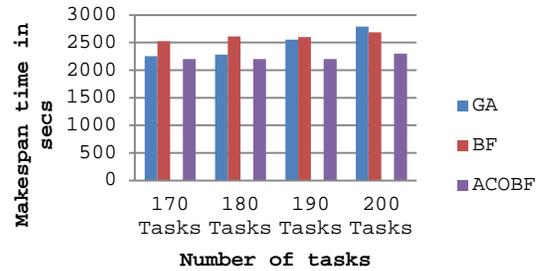


Fig. 6. Makespan Time for 170-200 Tasks.

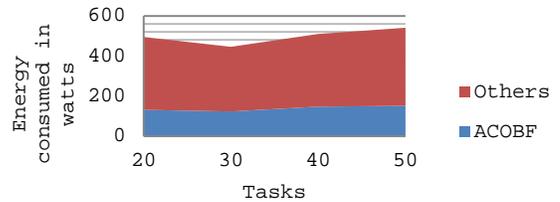


Fig. 7. Energy Consumed by Processing 20-50 Tasks.

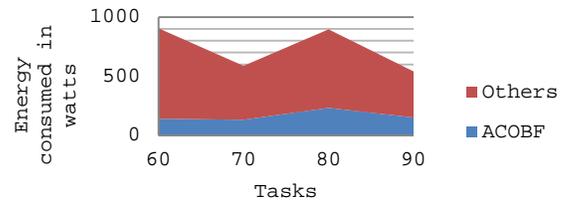


Fig. 8. Energy Consumed by Processing 60-90 Tasks.

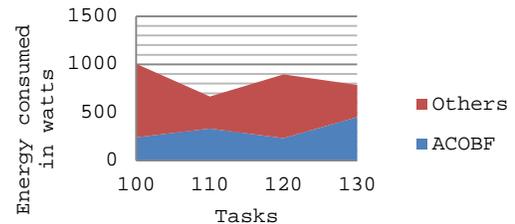


Fig. 9. Energy Consumed by Processing 100-130.



Fig. 10. Energy Consumed by Processing 140-170 Tasks.

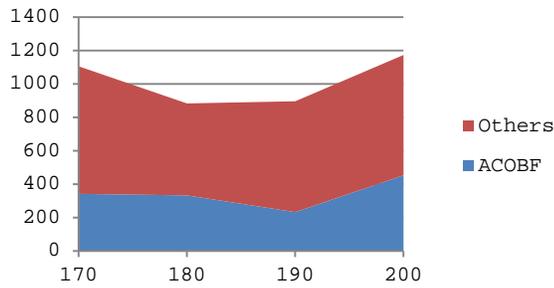


Fig. 11. Energy Consumed by Processing 170-200 Tasks.

This is a straightforward feasibility of the ACOBF exhibition in addressing the user's time prerequisites. Tasks that are sent to the Cloud are supposed to be independent of each other, as mentioned before. The findings explain the algorithms for GA and BF. When the Cloud receives a comparable number of task units/tasks, makespan and energy increases dramatically, whereas in the case of ACOBF, makespan and energy either decreases or fluctuates. This is due to the ability of the algorithm to preserve convergence that was done by having the starting point close to the minimum.

## VI. CONCLUSION AND FUTURE WORK

In the cloud computing environment, this article proposes a generic task scheduling algorithm based on BF and ACO algorithms. Task scheduling is modeled as a multi objective optimization problem in order to deal with the trade-off between makespan and energy consumption cost functions. A simple and most effective optimization technique, referred to as a hybrid ACOBF-based approach, was applied to obtain Pareto optimal solutions for the task scheduling problem. On the basis of the comprehensive simulations conducted, the scalability and effectiveness of the proposed solution was seen as it was benchmarked on two current and state-of-the-art algorithms. Simulation results also show that the creation and energy usage have been significantly optimized with the proposed convergence strategy and task priority for the cost function.

The weakness of ACOBF would be examined in future studies and areas such as; accelerating the convergence rate resulting in extra time for crossover and mutation, chemotaxis and reproduction would be addressed. The research also looked at the relationship of dependency between tasks and task sizes for input and output.

## ACKNOWLEDGMENT

This study was supported by the Tertiary Education Trust Fund (TETFund) Institutional Based Research (IBR) Fund, through the Directorate of Research and Innovation of Abubakar Tafawa Balewa University, Bauchi (2018).

## REFERENCES

[1] Mezmaz, M., et al., A parallel bi-objective hybrid metaheuristic for energy-aware scheduling for cloud computing systems. *Journal of Parallel and Distributed Computing*, 2011. 71(11): p. 1497-1508.  
[2] Aliyu, M., et al., An Efficient Ant Colony Optimization Algorithm for Resource Provisioning in Cloud.

[3] Stocker, A.M. and A. Chenn, The role of adherens junctions in the developing neocortex. *Cell adhesion & migration*, 2015. 9(3): p. 167-174.  
[4] Aliyu, M., et al., Efficient Metaheuristic Population-Based and Deterministic Algorithm for Resource Provisioning Using Ant Colony Optimization and Spanning Tree. *International Journal of Cloud Applications and Computing (IJCAC)*, 2020. 10(2): p. 1-21.  
[5] Shuja, J., et al., Energy-efficient data centers. *Computing*, 2012. 94(12): p. 973-994.  
[6] Tawfeek, M.A., et al. Cloud task scheduling based on ant colony optimization. in *2013 8th international conference on computer engineering & systems (ICCES)*. 2013. IEEE.  
[7] Kumar, A.S. and M. Venkatesan, An Efficient Multiple Object Resource Allocation Using Hybrid GA-ACO Algorithm. *Australian Journal of Basic and Applied Sciences Journal*, 2015. 9(31): p. 53-59.  
[8] Lee, C.-Y., Z.-J. Lee, and S.-F. Su. A new approach for solving 0/1 knapsack problem. in *2006 IEEE International Conference on Systems, Man and Cybernetics*. 2006. IEEE.  
[9] Adhikari, M. and T. Amgoth, Heuristic-based load-balancing algorithm for IaaS cloud. *Future Generation Computer Systems*, 2018. 81: p. 156-165.  
[10] Tiwari, A., P. Richhariya, and S. Patra, Ant Colony based Cloud VM Allocation and Placement Approach for Resource Management in Cloud. *International Journal of Computer Applications*, 2017. 158(4): p. 8-12.  
[11] Guo, X. Ant Colony Optimization Computing Resource Allocation Algorithm Based on Cloud Computing Environment. in *International Conference on Education, Management, Computer and Society*. 2016. Atlantis Press.  
[12] Shabeera, T., et al., Optimizing VM allocation and data placement for data-intensive applications in cloud using ACO metaheuristic algorithm. *Engineering Science and Technology, an International Journal*, 2017. 20(2): p. 616-628.  
[13] Chaharsooghi, S.K. and A.H.M. Kermani, An effective ant colony optimization algorithm (ACO) for multi-objective resource allocation problem (MORAP). *Applied mathematics and computation*, 2008. 200(1): p. 167-177.  
[14] Guo, Q. Task scheduling based on ant colony optimization in cloud environment. in *AIP Conference Proceedings*. 2017. AIP Publishing LLC.  
[15] Lin, J., et al., Hybrid ant colony algorithm clonal selection in the application of the cloud's resource scheduling. *arXiv preprint arXiv:1411.2528*, 2014.  
[16] Jia, Z., et al., Ant colony optimization algorithm for scheduling jobs with fuzzy processing time on parallel batch machines with different capacities. *Applied Soft Computing*, 2019. 75: p. 548-561.  
[17] Deepalakshmi, P. and K. Shankar, Role and Impacts of Ant Colony Optimization in Job Shop Scheduling Problems: A Detailed Analysis. *Evolutionary Computation in Scheduling*, 2020: p. 11-35.  
[18] Zheng, X., et al., Energy-efficient scheduling for multi-objective two-stage flow shop using a hybrid ant colony optimisation algorithm. *International Journal of Production Research*, 2020. 58(13): p. 4103-4120.  
[19] Ghanavati, S., J.H. Abawajy, and D. Izadi, An Energy Aware Task Scheduling Model Using Ant-Mating Optimization in Fog Computing Environment. *IEEE Transactions on Services Computing*, 2020.  
[20] Rubaiee, S. and M.B. Yildirim, An energy-aware multiobjective ant colony algorithm to minimize total completion time and energy cost on a single-machine preemptive scheduling. *Computers & Industrial Engineering*, 2019. 127: p. 240-252.  
[21] Kim, D.H. and J.H. Cho. Intelligent control of AVR system using GA-BF. in *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*. 2005. Springer.  
[22] Salido, M.A., et al., A genetic algorithm for energy-efficiency in job-shop scheduling. *The International Journal of Advanced Manufacturing Technology*, 2016. 85(5-8): p. 1303-1314.  
[23] Ullah, I., et al., An efficient energy management in office using bio-inspired energy optimization algorithms. *Processes*, 2019. 7(3): p. 142.

# Motor Insurance Claim Status Prediction using Machine Learning Techniques

Endalew Alimir<sup>1</sup>, Teklu Urgessa<sup>2</sup>, Ashebir Hunegnaw<sup>3</sup>, Tiruveedula Gopikrishna<sup>4</sup>

Department of Management Information Systems, Mettu University, Mettu, Ethiopia<sup>1,3</sup>

Department of Computer Science and Engineering, Adama Science and Technology University, Adama, Ethiopia<sup>2,4</sup>

**Abstract**—The insurance claim is a basic problem in insurance companies. Insurance insurers always have a challenge to the growing of insurance claim loss. Because there is the occurrence of claim fraud and the volume of claim data increases in the insurance companies. As a result, it is difficult to classify the insured claim status during the claim review process. Therefore, the aims of the study was to build a machine learning model that classifies and make motor insurance claim status prediction in machine learning approach. To achieve this study Missing value ratio, Z- Score, encoding techniques and entropy were used as data set preparation techniques. The final preprocessed data sets split using K- Fold cross validation techniques into training and testing sets. Finally the prediction model was built using Random Forest (RF) and Multi Class – Support Vector Machine (SVM).The performance of the models, RF and Multi –Class SVM classifiers were evaluated using Accuracy, Precision, Recall, and F- measure. The prediction accuracy of the model is capable of predicting the motor insurance claim status with 98.36% and 98.17% by RF and SVM classifiers respectively. As a result, RF classifier is slightly better than Multi-Class Support vector machines. Developing and implementing hybrid model to benefit from the advantages of different algorithms having graphical user interface to apply the solution to real world problem of the insurance company is a pressing future work.

**Keywords**—Motor insurance claim; machine learning; classification; Random Forest (RF); Support Vector Machine (SVM); supervised learning

## I. INTRODUCTION

Insurance company is fast growing, industry [1] [2]. It has great role in assuring economic wellbeing of a country, and Insurance claims in insurance companies are costly problems [3]. Insurance providers always make a great effort, with the growing of insurance claim cost or claim loss because of insurance claim fraud [4]. Insurance companies have business problems, such as risk assessment, classification of policy holders and resource allocation, insurance claim classification and prediction in the insurance claim handling process [3]. This insurance business problems were not solved using traditional analytical approaches, including regression, linear programming [5].

Nowadays an insurance corporation has been struggled (stressed) to get best methods that handle transactional data and, risk management data for years [6]. But there is a recent emphasis to use different sources, of data which extends beyond traditional data sources, often known as big data. This big data has created to change data management across the

insurance industry [7] [8]. Data variety and data volume push the traditional data management (Relational Database Management System (RDBMS) technologies and software tools because of their restrictions [7] [9].

As the computing technology has been technologically advanced enormously [5], machine learning approach is used to solve insurance business problems like insurance risk, claim loss, to understand and analysis huge amount of data [10] [11]. Companies have huge amounts of data, in the insurance database, which could not be understandable and interpretable by humans like Ethiopian Insurance companies specifically Awash motor insurance claim data.

Therefore, handling and processing large amount of insurance claim data requires computational tools. Machine learning approaches are essential to process the data and, extract the vital insurance claim information for decision making process [5] [12].

For these problems, supervised machine learning techniques, particularly classification algorithms are used as the computational processes for the data set that stored in the insurance database. Machine learning classifiers are used to classify different types or classes of data from a dataset to predict what will happen in the future from the past data set [5] [11].

Machine learning approach in big data is helping to connect machine with huge databases making them to learn new things by its own. Analysis of big data using machine learning approach helps the insurance industry to predict future trends in the competitive market. Big data initially emerged as a term in order to describe data sets whose amount or size is beyond the capability of traditional databases, to capture, store, analyze, manage, and too complex to analyze by traditional data processing techniques and database management tools [9] [13]. Big data is not only about the size, finding insights from complex, heterogeneous, and complex, noisy and voluminous data [11]. Big data categorized as structured data, unstructured data and semi structured data. Structured data is accessed, stored and processed in the fixed format. The type of data in this study is structured data. Because the motor insurance claims data have stored in fixed format, which is store in fixed relational database format. The main objective of the study was to build machine learning model that classifies and make motor insurance claim status prediction in machine learning techniques.

Finally the proposed motor insurance claim status prediction model was addressed the following research questions.

- Can we build more accurate machine learning model that classify motor insurance claim data and make claim status prediction for the insurance company?
- Which techniques needed to prepare the data sets to be able to apply model building techniques?

- What are the better classification techniques that would use for claim classification and how we evaluate the performance of the built machine learning model?

## II. RELATED WORKS

This section described the existing related work that has been done before by other researchers .This section includes methods and techniques, implementation tools, aims of study and findings of the research as follows in the following Table I.

TABLE I. RELATED WORKS OF THE STUDY

Objective of Study	Methods and Techniques	Data and place	Findings
Build Predictive Model for Auto Insurance Claims prediction [18]	CART, Entropy Gini index Decision Tree	1,528 Ghana insurance data Vehicle age and customers age are most predictor variable	Policy holders whose age is 18 to 48 have max claim Vehicle age 0 to 8 years have max claim
Support vector machines to classify policy holders satisfactory in automobile insurance[11][17]	Machine learning algorithm, SVM kernel trick, RBF Parameter 0.05	13,635 Indonesia automobile insurance policies,40% data to train,60% data to test	Classification of Customer satisfaction had claim or not. Reliable SVM model to predict, claim ,84.08% of accuracy
An Ensemble Random Forest Algorithm for Insurance Big Data Analysis[6] [11]	Apache Hadoop, Map reduce Apache spark Ensemble RF SVM,LR Precision , G-mean F-measure ,Information gain	500,000, customers data from China insurance	Ensemble RF Algorithm is better than SVM, and logistic regression for insurance product and policy holder analysis Application of ensemble RF with spark for insurance big data analysis
Data mining classification model to Predict the customer's claims in auto insurance company[2]	Logistics regression, Artificial Neural network, Decision Tree C4.5,Accuracy ,precision, recall	80% sample data as training and 20% sample data as testing	The insurance claims classified as low, high, fair. Neural network Has best prediction accuracy of 61.7% to classify claims
Predict the customer's choice of car insurance policies using random forest[12]	Data mining classifications algorithms include Decision Tree, K-Nearest Neighbors Naïve Bayes, Neural Networks and, and Support vector machine algorithms, weka	665,250 records of insurance policies from Allstate insurance company. 665,250 as train set and 198,857as test set.	split the data in to seven categories in order to predict the customer's car insurance policy The performance of the Random Forest model was 97.9%.

## III. MATERIALS AND METHODS

### A. Development Tools

Anaconda Navigator and python programing language was used for this research. Anaconda Navigator tool, Jupiter notebook, scikit – learn (sklearn) frame work, and python programing language was used to implement the proposed model. Descriptive statistics summary and graphics data analysis techniques were used. Descriptive statistics used for motor insurance claim data analysis using count, mean, standard deviation, quartiles (25%, 50%, and 75%), min and max. Graphics techniques were used for visualization of the data distribution, using graphical representation like density plot, histograms, table and bar graph.

### B. Data Collection

The sources of data for this research were secondary and primary data sources. Secondary data was collected from the existing centralized insurance database of Awash insurance company main office, which is found at Addis Ababa. The relevant secondary motor insurance claim data were collected from the standard experts of Awash insurance company. In

addition to, this the researcher used interview methods in order to understand the insurance domain knowledge and motor insurance claim data with insurance experts of the company.

### C. Dataset Description

The amount of the dataset used for this research consists of a sample of 65,535 records or instances of AIC motor insurance claim data. The data set contains a total of eleven attributes of motor insurance claim data. This data has excel data format. The column shows the attributes and the row shows the records (instances). The motor insurance dataset have five target classes of insurance policy holders claim status which are close, notification, pending, re-open and settled. The other ten features (attributes) are policy number, name of insured, claim numbers, claim date, estimated loss, claim paid(gross), net of recoveries, total claims expense paid, change in outstanding and claim incurred. The period of the sample motor insurance claim dataset was covered from 2014 up to 2017. This range takes as a base line of the study, because the AIC started to use system for register insurance claim data at the end of 2013. After a year the system starts to store well organized data in the insurance database.

#### D. Data Preparation Techniques

Data processing techniques were used for data set preparation. Data preprocessing techniques include: data cleaning, data integration, data normalization or data transformations, and encode as shown in Fig. 2. Data cleaning was used to remove noisy data, irrelevant data, which are 47 non-relevant columns from the data set, and reduce the dimension of the dataset from 58 columns to 11 columns by using dimensional reduction techniques specifically missing value ratio. z - Score was used for data normalization, because it normalizes each feature to have mean of zero and variance of one. It also tells as how many standard deviations each feature far away from the mean and it can normalize the data when the actual min and max value is not known. The formula of z - score described below as equation 1.

$$\sum_{n=1}^n \left(\frac{x}{n}\right)$$

$$\sigma^2 = \sum_{n=1}^n \left(\frac{(x - x')^2}{n-1}\right)$$

$$z = \frac{(xi - x')}{\sigma} \quad (1)$$

Where X' is mean, sigma is standard deviations, and Z is Z - Score.

To encode categorical data one - hot encoding (OHE) technique was used to convert claim status categorical data to numeric or binary, because there is no natural ordinal relationship between claim status (closed, notification, pending, re-open, and settled).

Policy Number, Name of Insured ,and Claim Number contains string values as an instances or records, this three features have quantized to numeric data values to make the data understandably by RF, and SVM machine learning algorithm. The other features have numeric and float values, namely Claim paid (gross paid=A), Net of Recoveries=B, Net of Recoveries (A-B), Change in Outstanding. These values have a large difference between the max and min values for each feature. Because of this Z - score data normalization technique was applied to transform or scale down the data set. The last features, which is claim status is encoded by using a label encoder because it is a nominal categorical data. Where the claim status 0, 1, 2, 3, and 4 refers to Closed, Notification, Pending, Re-open, and settled, respectively.

Attribute evaluation techniques or variable importance measure was used to identify the most relevant attribute or features from the whole attributes during classification process for model construction. For variable importance measure information gain or entropy and domain experts was used.

$$\text{Gain}(D, A) = \text{Entropy}(D) - \sum_{j=1}^V \frac{|D_j|}{|D|} \text{entropy}(D_j) \quad (2)$$

Where D is the data partition, A is attribute, V is partition the instances to D1, D2..... Dj but the entropy can be calculated as follows below, and attribute Aj that have maximum information gain is used as important features .

$$H = - \sum_{i=1}^n p(xi) \log_2 p(xi) \quad (3)$$

Where (pxi) is the probability of selected class and n is number of the data set class and H is entropy. The following Fig. 1 shows the relative importance of the feature using Information gain.

Fig. 1 shows the relative importance of the features based on their information gain. The orders of the features are shown as follows in decreasing order, this is a Claim Incurred, Claim Number, Change In out Standing, Estimated Loss, Policy Number, Name of Insured, Net of Recoveries(A-B), Claim paid Gross(A), Net of Recoveries (B) and their corresponding information gain values are 0.176, 0.175, 0.148, 0.115, 0.113, 0.093, 0.075, 0.065, 0.037 respectively. Claim Incurred has highest information gain value. On the contrary, Net of Recoveries (B) has lowest information gain values.

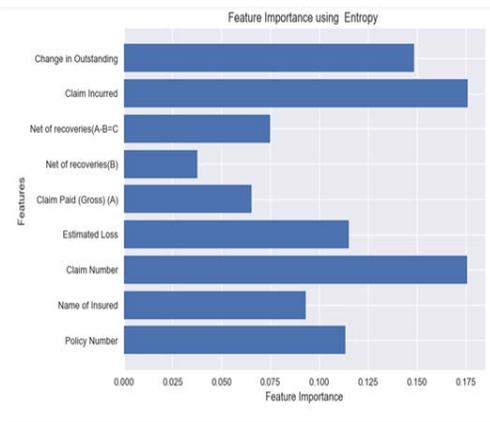


Fig. 1. Relative Feature Importance using Information Gain.

#### E. Cross Validation Techniques

Machine learning approaches are evaluated using cross validation techniques, it also called rotation estimation. Because the result of cross validation believed that more reliable and less variance to other single train, test split techniques [14] [15]. For this study tenfold cross validation technique was used. 90 % of motor insurance claim data set (58,982 motor insurance claim incurred instances of data sets) used to train the model and 10% of the motor insurance claim data set (6,554 motor insurance claim incurred instances of data sets) used to test the model through iteration.

#### F. Machine Learning Algorithms

Supervised machine learning algorithms were used to build motor insurance claim status prediction model. For this study, Random Forest (RF) and Support vector machine (SVM) machine learning classifiers were used to build machine learning model. RF classifier consists of many numbers of decision trees as base learners, and each tree train by using random samples of the motor insurance dataset with a replacement which is called bootstrapping. Train all trees by using different samples and take the majority vote for insurance claim status prediction. This process, called Bagging.

Multi class SVM classifier with kernel trick Radial basis function (RBF) and parameter C (cost of penalize misclassification error) with value 1 was used to build motor insurance claim status prediction model. One against all (1AA) approach was used for multi class claim status classification

and prediction. In the data set there are five target classes. Therefore, multiple binary class classification was applied using One vs. Rest (OVR) or 1AA approach, because it is efficient to compute and easy to interpret. Five SVM binary classes were built, means that one class vs. the rest classes.

### G. Model Performance Evaluation Methods

Machine learning model performance evaluated using different parametric measures, because individual learner gives biased result solutions. Due to this reasons it is useful to measure or evaluate the performance of the algorithm how it is learned from the experience [15]. To evaluate the performance of the model, evaluation metrics were used. For this study, confusion matrices, accuracy, precision, recall and, F-score were used.

Confusion matrix representing as a two dimensional table having predicted values as rows or instances and actual classification values as column. It is not performance measure by its own rather than using other performance metrics with it. These are TP (True positive), TN (True negative), FP (False positive) and FN (False negative) [16]. Accuracy shows the classification problems correct prediction value and calculated as the total number of the model correct prediction divide by all number of data set used for classification. Precision measure the predicted value true and it show how many times the model predicts true.

In the case of Recall the built model identifies the whole relevant examples or instances. F-Measure calculated as by combining the above two methods which is precision and recall as harmonic mean. It is also called F-score, F1- measure. The equation of the above metrics shows as follows.

$$\text{Accuracy(ACC)} = \frac{\text{TN} + \text{TP}}{\text{For All Total Instances}}$$

$$\text{Precision(p)} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recall(R)} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{F - score} = 2 * \frac{(\text{Recall} * \text{Precision})}{(\text{Recall} + \text{Precision})}$$

## IV. PROPOSED MOTOR INSURANCE CLAIM STATUS PREDICTION MODEL

Fig. 2 shows the proposed model architecture for motor insurance claim status prediction. This architecture has the following components. These are Explanatory data analysis (EDA), Data preprocessing (data cleaning and integration, dimensional reduction, data normalization and encoding), Training and Testing, Evaluate and Model performance comparisons. Fig. 2, shows the detail architecture of the proposed model design.

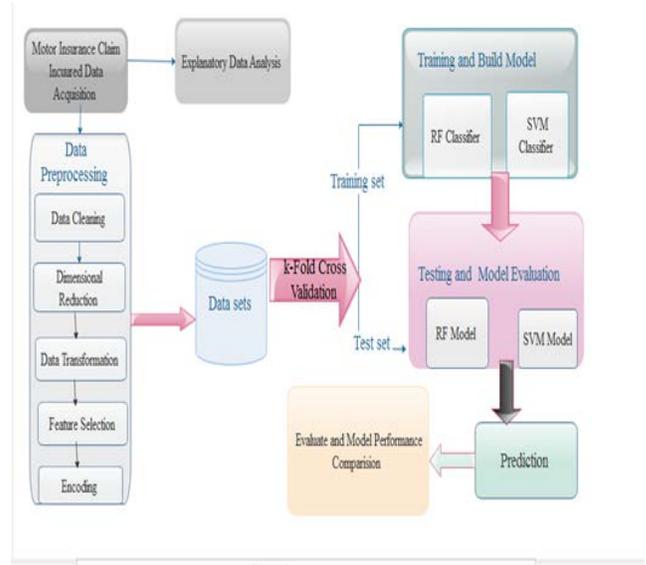


Fig. 2. Architecture of the Proposed Motor Insurance Claim Status Prediction Model.

## V. RESULTS AND DISCUSSION

### A. Evaluation of Result

In machine learning, classification is the most common type of problems [15], because of this there are evaluation metrics, which we used to evaluate the performance of the built machine learning models. For this study, four performance evaluation metrics were used to evaluate the classification performance of the RF, and SVM models using ten – fold cross validation techniques as stated in Section 3F. The data set is split in two parts as training, and testing as it discussed in Section 3D. The two models namely RF and SVM were used, as classifiers. Each classifier is trained and tested. The models obtained, from the training phase were tested by using new motor insurance claim data in addition to, training sets. Accuracy of ten –fold cross validation results were computed by taking the average result of each training set and test sets as demonstrated or illustrated in Table II.

Table II shows the Prediction accuracy of RF and SVM. The RF prediction accuracy in each fold was as follows, 97.45%, 98.94%, 96.99%, 97.03%, 98.39%, 97.07%, 96.73%, 89.42%, 93.17%, and 96.59% on the corresponding experiment 1, experiment 2, experiment 3, experiment 4, experiment 5, experiment 6, experiment 7, experiment 8, experiment 9, and experiment 10 respectively. The lowest percentage result was recorded on experiment 8 (89.42%,) and the highest percentage result was recorded on experiment 2 (98.94%). The average prediction accuracy of RF from those ten experiments is 96.43%. The prediction accuracy of SVM on each fold was 98.96%, 99.19%, 99.11%, 99.40%, 99.63%, 97.22%, 98.10%, 79.18%, 96.45%, and 98.80% on the corresponding experiment 1, experiment 2, experiment 3, experiment 4, experiment 5, experiment 6, experiment 7, experiment 8, experiment 9, and experiment 10 respectively. The lowest percentage score was recorded on experiment 8 (79.18%), similar to RF. The highest percentage score was recorded on experiment 5 (99.63%). The average prediction accuracy of SVM from those ten experiments was 96.60%. Except experiment 8, the accuracy

result of the SVM on each experiment was slightly greater than the accuracy result of RF. The performance of the RF, and SVM models clearly illustrated using a bar graph in Fig. 3.

The bar chart in Fig. 3 shows the graphical or visual representation of the above Table I results. The green color represents RF's classification accuracy and the blue color represents the classification accuracy of the SVM's. This bar chart shows the comparison of RF and SVM, how it performs on each fold through iteration.

**B. Classification Result of Models**

The classification performance of the two classifiers (RF and SVM) validated or measured using the test data sets. The results of these classifiers for the test data sets were shown in the Table III and IV, respectively. The column show the actual value and the row show predicted value. The diagonal value of the confusion matrix indicates the correctly classified instances among the test data sets as illustrated below.

Where class, Close, Pending, Notification, Re-open, Settled represent 0, 1,2,3,4, respectively.

The result of each class, TP, FP, FN, TN, accuracy, precision, and F- measure based on RF and SVM models from the confusion matrix report is presented in the Table IV and Table V respectively as shown below.

Table V shows the summary result of RF model. 98.36 % was correctly classified and 1.64 % was misclassified by RF. On the other way, The Precision, Recall and F- measure result of the RF model was 95.15%, 94.71%, and 94.90% respectively. The highest prediction accuracy found for class, re-open, that has 99.83%, and the lowest prediction accuracy for class settled, was 97.34%.

Similarly, Table VI shows the summary of SVM model result of, Accuracy, Precision, RECALL AND F-MEASURE IS 98.17%,

97.22%, 93.80%, and 95.36% respectively and 1.83% was misclassified. The highest prediction accuracy found for class re-open (99.89%) and lowest prediction accuracy was found for class closed (95.94%).

From the above two experimental results, both of the two models have nearly similar prediction accuracy performance. But, RF Model slightly greater than Support vector machine model in terms of accuracy. Both RF and SVM model had the best prediction accuracy of re-open claim status among all other classes of MOTOR INSURANCE CLAIMS.

Generally, Random Forest model is slightly better than support vector machine model in both accuracy, and Recall. On the other hand, SVM model better than RF model in both precision and F-measure as summarized in Fig. 4, which shows the comparison of RF and SVM models using the four performance metrics evaluation (Accuracy, Precision, Recall and F- measure).

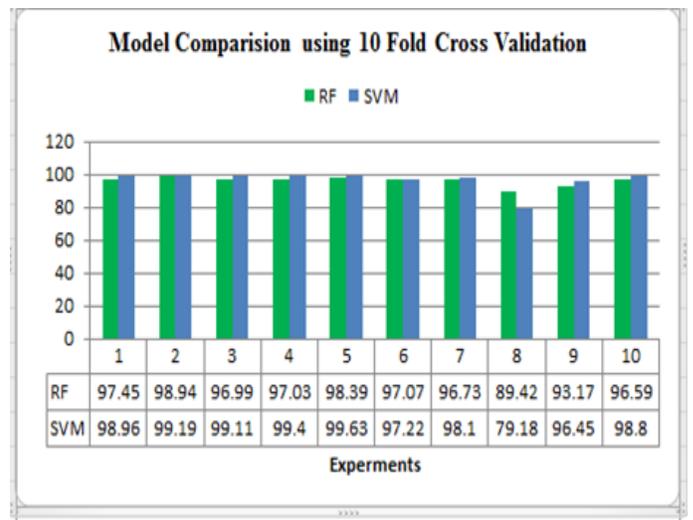


Fig. 3. RF and SVM classification Accuracy Result in Bar Chart.

TABLE II. TEST RESULT FOR RF AND SVM USING EACH FOLD

Experiment	1	2	3	4	5	6	7	8	9	10	Average
Total No. of data sets	65,535										
Accuracy of RF in %	97.45	98.94	96.99	97.03	98.39	97.07	96.73	89.42	93.17	96.59	96.43
Accuracy of SVM in %	98.96	99.19	99.11	99.40	99.63	97.22	98.10	79.18	96.45	98.80	96.60

TABLE III. CONFUSION MATRIX RESULT FOR RF MODEL

Actual	Predicted					Total
	Close	Notification	Pending	Reopen	Settled	
Close	2452	5	34	2	25	2518
Notification	4	685	1	1	1	692
Pending	33	2	798	0	43	876
Re-open	7	0	0	76	1	84
Settled	24	30	50	0	2280	2384
Total	2520	722	883	79	2350	6554

TABLE IV. CONFUSION MATRIX RESULT FOR SVM MODEL

Actual	Predicted					Total
	Close	Notification	Pending	Re-open	Settled	
Close	2393	1	2	1	6	2403
Notification	64	693	4	0	11	772
Pending	84	2	889	0	7	982
Re-open	4	0	0	94	2	100
Settled	104	4	3	0	2186	2297
Total	2649	700	898	95	2212	6554

TABLE V. TP, FP, FN, TN ACCURACY, PRECISION, RECALL, AND F-MEASURE (SCORE) FOR RF MODEL

Class	TP	FP	FN	TN	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
Closed	0	2452	68	3968	97.7955447	97.301587	97.378872	97.3349771
Notification	1	685	37	5825	99.328654	94.875346	98.9888439	96.8880576
Pending	2	798	85	5593	97.512969	90.373726	91.09589	90.733371
Re-open	3	76	3	6467	99.832164	96.202532	90.47619	93.2515336
Settled	4	2280	70	4100	97.345133	97.021277	95.637584	96.3247046
<b>Average (%)</b>					<b>98.3628928</b>	<b>95.1548936</b>	<b>94.715476</b>	<b>94.9065288</b>

TABLE VI. TP, FP, FN, TN ACCURACY, PRECISION, RECALL, AND F-MEASURE (F- SCORE) FOR SVM MODEL

Class	TP	FP	FN	TN	Accuracy (%)	Precision (%)	Recall (%)	F-score (%)
Closed	0	2393	256	3895	95.94141	90.335976	99.583854	94.7349474
Notification	1	693	7	5775	98.687824	99	89.766839	94.1576084
Pending	2	889	9	5563	98.443699	98.997773	90.529532	94.5744684
Re-open	3	94	1	6453	99.893195	98.947368	94	96.4102562
Settled	4	2186	26	4231	97.909673	98.824593	95.16761	96.9616222
<b>Average (%)</b>					<b>98.17516</b>	<b>97.221142</b>	<b>93.809567</b>	<b>95.3677806</b>

According to the above Fig. 4, the result of high value precision in RF and SVM models indicates that, the built model can correctly classify motor insurance claim status and predict the sample data to their corresponding real class.

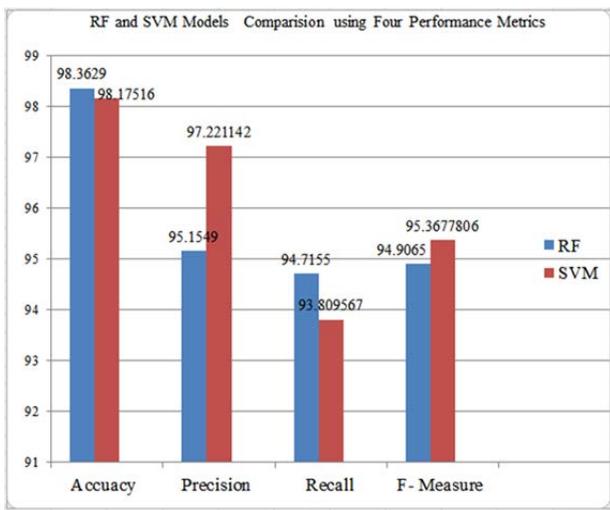


Fig. 4. Models Comparison by using Various Performance Evaluation Metrics.

High recall indicates that many of the data were predicted and high relevant data were selected. Other high value of F-measure shows that best result values are obtained at the precision and recall performance measures. On the contrary, low values of F-measure indicate less value of precision and recall. Generally, the two models give ideal precision-recall results, means that it scores high precision and high recall results.

## VI. CONCLUSION

In this study, the potential applicability of machine learning has been implemented and evaluated in the insurance company, specifically for motor insurance claim prediction. This experimental study, which has employed the most powerful, used methodological techniques in machine learning research. So to address the problem, Random forest model and Support vector machine, were used as a predictive model.

In this study, an attempt has been done to design, and implements the model that has a capability of predicting motor insurance claim status. The procedures included data Understanding and explanatory data analysis, data preprocessing), model training, model testing, classification and prediction, and finally comparison of the two built models have done.

The two models built on using 65, 535 instances of motor insurance claim data as input. This input data first needs data understanding and data preparation before to build the two models. The final preprocessed data sets were used for model training and testing. This preprocessed data sets split into two, training set and testing set using K –Fold cross validation with k= 10. Hence, dataset divided in to 10 folds or experiments through iteration. Each fold used as training and testing iteratively, at least each fold used once as testing set. Finally the average score for each fold was taken. The performances of the two classifiers were evaluated by using four metrics (Accuracy, Precision, Recall and F-measure). Therefore, the experimental result shows that the two classifiers score an overall accuracy of 98.36929% and 98.17516%, correctly classified by the two models respectively.

Generally, the performance of the model was evaluated with four metrics (Accuracy, Precision, Recall, and F-measure). The developed motor insurance claim status prediction models have best prediction accuracy, and the two models have promising prediction accuracy. RF model prediction accuracy is slightly better than SVM model in the insurance domain specifically in motor insurance.

#### VII. FUTURE WORK

In this study, a good result was achieved in predicting motor insurance claim status. But, it was not possible to implement all machine learning classification algorithms, because of this the researchers propose extending this study with other machine learning algorithms, and build hybrid machine learning model using graphical user interface design to apply in the real world insurance companies.

#### REFERENCES

- [1] Hailu Zeleke ., "Insurance in Ethiopia: Historical Development, Present Status and Future Challenges .," vol. 1, no. 1, p. 308, 2009.
- [2] K. P. M. L. P. W. and M. C. W. Depa, "A Comparative Study of Data Mining Algorithms in the Prediction of Auto Insurance Claims," *Eur. Int. J. Sci. Technol.*, vol. 5, no. 1, pp. 47–54, 2016.
- [3] A. C. Yeo, K. A. Smith, R. J. Willis, and M. Brooks, "Clustering Technique for Risk Classification and Prediction of Claim Costs in the Automobile Insurance Industry," *Int. J. Intell. Syst. Accounting, Financ. Manag.*, no. November 1999, pp. 39–50, 2001.
- [4] M. C. Wijegunasekara and Weerasingheand M.C. Wijegunasekara , "A Comparative Study of Data Mining Algorithms in the Prediction of Auto Insurance Claims," vol. 5, no. 1, pp. 47–54, 2016.
- [5] K. A. Smith, R. J. Willis, M. Brooks, K. A. Smith, R. J. Willis, and M. Brooks, "An analysis of customer retention and insurance claim patterns using data mining : a case study," *J. Oper. Res. Soc. ISSN*, no. 5682, pp. 1476–9360, 2017.
- [6] W. Lin, Z. Wu, L. Lin, A. Wen, and J. I. N. Li, "An Ensemble Random Forest Algorithm for Insurance Big Data Analysis," *IEEE Access*, vol. 5, 2017.
- [7] P. Bharal and A. Halfon, "Making Sense of Big Data in Insurance," *ACORD and MarkLogic*, 2013.
- [8] L. Wang and C. A. Alexander, "Big Data : Infrastructure , technology progress and challenges," *J. Data Manaagement Comput. Sci. Vol.*, vol. 2, no. 1, pp. 1–6, 2015.
- [9] A. L. Heureux and M. Grolinger, Katarina and Caprtz, "Machine Learning With Big Data : Challenges and Approaches," *IEEE Access*, vol. 5, pp. 7776–7797, 2017.
- [10] A. S. Alshamsi and A. Ain, "Predicting Car Insurance Policies Using Random Forest," *IEE*, pp. 128–132, 2014.
- [11] Endalew Alamir, Teklu Urgessa, T. GopiKrishna and Ellappan V, "Application of Machine Learning with Big Data Analytics in the Insurance," vol. 11, no. 12, pp. 1064–1073, 2020.
- [12] A. S. Alshamsi and A. Ain, "Predicting Car Insurance Policies Using Random Forest," pp. 128–132, 2014.
- [13] T. Kavipriya and N. Kumar, "A Study on Machine Learning Algorithms for Big Data Analytics," *IOSR J. Eng.*, no. Iccids, pp. 40–46, 2018.
- [14] A. C. Tan and D. Gilbert, "An empirical comparison of supervised machine learning techniques in bioinformatics," *First Asia Pacific Bioinforma. Conf. (APBC 2003)*, vol. 19, no. Apbc, 2003.
- [15] J. Brownlee, *Machine Learning Mastery with python*, V1.4. 2016.
- [16] R. J. Kate and A. M. Swartz, "Assessment of various supervised learning algorithms using different performance metrics Assessment of various supervised learning algorithms using different performance metrics," *IOP Conf. Ser. Mater. Sci. Eng.*, 2017.
- [17] C. Using, S. Vector, F. K. C-means, Z. Rustam, and F. Yaurita, "Support Vector Machines for Classifying Policyholders Satisfactorily in Automobile Insurance .," *J. Phys. Conf. Ser. Pap.*, 2018.
- [18] N. K. Frempong, N. Nicholas, and M. A. Boateng, "Decision Tree as a Predictive Modeling Tool for Auto Insurance Claims," *Int. J. Stat. Appl.*, vol. 7, pp. 111–120, 2017.

# Detecting Malware based on Analyzing Abnormal behaviors of PE File

Lai Van Duong<sup>1</sup>, Cho Do Xuan<sup>2</sup>  
Information Assurance Department  
FPT University, Hanoi  
Vietnam

**Abstract**—Attack by spreading malware is a dangerous attack form that is very difficult to detect and prevent. Attack techniques that spread malware through users and then escalate privileges in the system are increasingly used by attackers. The three main methods and techniques for tracking and detecting malware that is being currently studied and applied include signature-based, behavior-based, and hybrid techniques. In particular, the behavior-based technique with the support of machine learning algorithms has given high efficiency. On the other hand, in reality, attackers often find various ways and techniques to hide behaviors of the malware based on the Portable Executable File Format (PE File) of the malware. This makes it difficult for surveillance systems to detect malware. From the above reasons, in this paper, we propose a malware detection method based on the PE File analysis technique using machine learning and deep learning algorithms. Our main contribution in this paper is proposing some features that represent abnormal behaviors of malware based on PE File and the efficiency of some machine learning algorithms in the classification process.

**Keywords**—Malware; portable executable file format; detection malware; abnormal behaviors; machine learning; deep learning

## I. INTRODUCTION

Malware is software that is purposefully designed to cause damage to a personal computer, server, or computer network system [1, 2]. The purpose of malware is to execute illegal acts such as unauthorized access, stealing user information, spreading spam email, and even performing blackmail, attack and damage to computer system, etc. for personal gain, economic gain, political or simply they can be created as just some malicious joke. The study [3, 4] listed some common types of malware including Virus, Worm, Trojan Horse, Malicious Mobile Code, Tracking Cookie, Attacker Tool, Phishing, Virus Hoax. According to the statistics [5], the malware distribution situation in 2020 increased by 75% compared to 2019. This is completely reasonable because hackers used to focus on attacking information systems but today they usually primarily chose to attack the user. Therefore, malware increases rapidly not only in the number of attacks but also in their danger level. Studies [6, 7, 8] listed a number of approaches to malware detection including signature-based detection and behavior-based detection. The signature-based detection method is the static analysis which analyzes the source code without executing the file [9]. Some techniques used in the static analysis include:

- Checking file format: the metadata of files can provide useful information. For example, Windows PE files can provide information such as execution time, import and export functions.
- String extraction: involves checking the output of the software (status message or error message) and inferring about the behavior of the malware.
- Trace: Before performing analysis, it is necessary to calculate the hash value of the file in order to verify whether the file has been modified or not. Commonly used hashing algorithms are Message-Digest algorithm 5, Secure Hash Algorithm 256-bit. Also can search for information in source code such as username, file name, registry string.
- Scan with anti-virus software: if the file being analyzed is a known malware, most anti-virus software will be able to detect it. This is often used to verify the results of the analysis.
- Disassembly: involves reversing the machine code into assembly language and thus knowing the logic and the purpose of the software. This is the most commonly used and reliable method in static analysis.

This detection method is only suitable for common types of malware with permanent signatures stored in the database. Modern malware usually attacks and exists for a short period of time.

The behavior-based detection method is based on dynamic analysis. This method will evaluate an object based on its behavior. When an object attempts to perform abnormal or unauthorized behavior, it denotes that the object is malicious or suspicious. A number of behaviors are considered dangerous such as disabling security controls, installing rootkits, autostart, modifying host files, establishing suspicious connections, etc. Each behavior may not be dangerous but when combined together can increase the suspicions of the subject. There is a predefined threshold. If any files exceed this threshold, it will be warned as malware [10, 11, 12, 13]. This method is used to detect malware that has capable of changing signature (polymorphism) or new types of malware (zero-day). However, some types of malware have the ability to detect the virtual environment, it will not execute malicious behavior in the sandbox environment [13]. Moreover, in fact, with the increasing amount of malware, this method is not really effective against new types of malware.

To fix the above disadvantages, in this paper, we propose a malware detection method based on the PE file analysis technique using machine learning and deep learning algorithms.

In particular, in this paper, we will analyze and extract abnormal behaviors in PE files to seek signs of malware and then use machine learning and deep learning algorithms to analyze and conclude about the existence of malware. The difference between our proposed approach and other traditional studies is we do not seek to extract malware behavior based on data that is collected in a virtualized environment. Instead, we analyze each different component in the PE file in detail in order to build behavior profiles of malware. With this approach, we could instantly collect behaviors and functions of malware designed and installed before by attackers.

Details of abnormal behaviors are defined in Section 3A of the paper. The classification algorithms selected for use are presented in Section 3C.

## II. RELATED WORKS

Dragos Gavrilut [10] proposed a malware detection system based on the improved Perceptron algorithm. With different algorithms, accuracy fluctuates in the range of 69.90% to 96.18%. However, the algorithm with the highest accuracy also has the most false positive results. The most balanced algorithm has a low false positives and accuracy as 93.01%.

Singhal and Raul discussed a detection method based on an improved Random Forest (RF) algorithm combined with Information Gain for presenting more optimal feature [11]. The dataset used by the author includes only the executable file so the feature selection is simpler. The detection rate is 97% and the false positives rate is 0.03%.

Baldangombo et al introduced a feature selection method based on the PE header, DLL libraries, and Application Programming Interface (API) functions [12]. Algorithms used include Naïve Bayes, Decision Tree J48, and Support Vector Machines (SVM). The algorithm with the best results is J48 with an accuracy rate of up to 99%.

Alazab [13] proposed a method to use the API to represent malware features. The SVM algorithm gave the best results with the accuracy as 97.6% and the rate of false positives as 0.025%.

The results given by the above studies are not the same, because there has not been a unified method for feature detection and representation. The accuracy of each case also depends on the types of malware used to sample and the actual running process.

## III. MALWARE DETECTION METHOD BASED ON PE FILE ANALYSIS

### A. Proposed Model

From Fig. 1, in order to detect malware based on analyzing abnormal behaviors of PE files, we will conduct 2 main tasks:

- Extracting behaviors of PE files. In this process, the system finds ways to analyze the PE files to calculate and extract the values of behaviors in PE files. To accomplish this goal, we will pre-define the behaviors

that need to be assessed as the basis for the system to check and extract. Details of these behaviors are presented in section 3.2 of the paper.

- Evaluating behavior profiles of PE files. This process evaluates and concludes about malware behaviors based on the behavior profiles of PE files that have been collected. To accomplish this goal, we propose to use machine learning and deep learning algorithms.

### B. Selecting and Extracting Features

PE File [14] is a Win32-specific file format. All executable files on Win32 such as \*.EXE, \*.DLL (Dynamic Link Library) (32 bits), \*.COM, \*.NET, \*.CPL, etc. are PE format, except for VxDs and \*.DLL (16 bits) files. Even NT's kernel mode driver uses the PE file format. PE file is divided into two sections: Header and Section. In which, the Header is used to store file format values including information required for the process of loading files to memory. This structure consists of 3 parts defined in windows.inc: Signature is one DWORD starting in PE Header and containing PE signatures: 50h, 45h, 00h, 00; FILE\_HEADER includes the next 20 bytes of the PE Header, this section contains information about the physical layout diagram and file features; OPTIONAL\_HEADER include the next 224 bytes after FILE\_HEADER. The Section Table is a component after the PE Header. It includes an array of IMAGE\_SECTION\_HEADER structures, each element contains information about a section in the PE file. In which, there are some important fields: VirtualSize is the actual size of the data on the section in bytes, this value may be smaller than the size on the disk (SizeOfRawData); VirtualAddress is the RVA of the section which is the value to map when the section is loaded into memory; SizeOfRawData is the size of the data section on the disk; PointerToRawData is the offset from the beginning of the file to the data section; Characteristic is the section properties including execution or data initialization.

From the brief overview of the PE file format, we can see that the PE header is quite complex with many variables and fields. Malware designers often use the PE header to conceal the malware version from the malware detection software. In this paper, we will examine and extract some features that represent malware behaviors in the PE header using the LEIF library. Table I below lists malware behaviors that are extracted based on different components in the PE header.

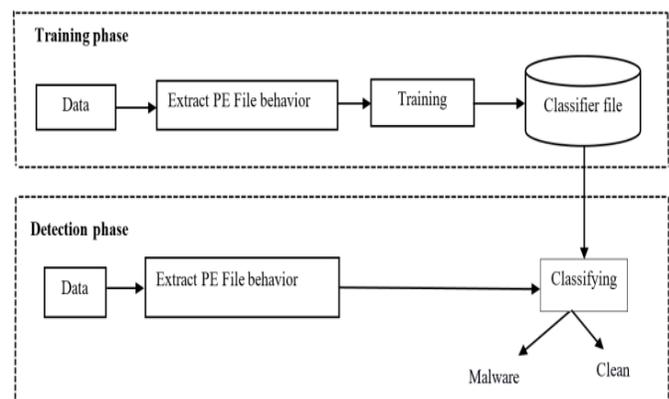


Fig. 1. Malware Detection Model based on Analyzing Abnormal behaviors in PE Files.

TABLE I. LIST OF MALWARE BEHAVIOR FEATURES IN PE HEADER

No.	Group	Name	Description	Data type
1	Properties*	pe.has_configuration	Contains the address and size of the load configuration	Integer
2		pe.has_debug	The address and size of the debug start point	Integer
3		pe.has_exceptions	Exception handling functions	Integer
4		pe.has_exports	Export special characters	Integer
5		pe.has_imports	Import special characters	Integer
6		pe.has_nx	The area of memory to use by storing processor instructions	Integer
7		pe.has_relocations	The address and size of the base relocation table	Integer
8		pe.has_resources	Indexed resources	Integer
9		pe.has_rich_header	Structure after MZ DOS header	Integer
10		pe.has_signature	Digital signatures	Integer
11		pe.has_tls	A special storage layer that Windows supports	Integer
12	PE entry point *	First 64 bits of Entry point	This function is in IMAGE_OPTIONAL_HEADER and contains the address of the base image	Real
.				
.				
75				
76	ASCII	256 characters in ASCII code table	Character set and character encoding based on the Latin alphabet	Real
.				
.				
331				
332	Liblabries	150 most commonly used libraries (Group B)	Dynamic Link Libraries	Real
.				
.				
481				
482		Pe.virtual_size	Ratio of the size of the PE file on the disk and on the RAM	Real
483	PE Section	CNT_CODE	Total SECTION_CHARACTERISTICS.CNT_CODE divided by the total sections	Real
484		MEM_EXECUTE	Total SECTION_CHARACTERISTICS.MEM_EXECUTE divided by the total sections	Real
485		Entropy	Total entropy in sections	Real
486		Virtual_size	The ratio of the actual size of each section to the size on disk and total sections	Real

### C. Malware Classification Algorithm

In this paper, we will use a number of deep learning and machine learning algorithms to classify files into normal or malicious. Accordingly, we choose to use the RF and SVM algorithms. Regarding deep learning algorithms, we use 3 main algorithms: Multi Layers Perceptron (MLP), Convolutional Neural Network (CNN), Long Short Term Memory (LSTM). The documents [15, 16, 17, 18] described in detail the mathematical basis and operating principle of these algorithms. Regarding MLP, CNN, LSTM algorithms, the documents [19, 20, 21, 22] presented about how they work and their applicability. In this paper, we will proceed to apply algorithms in the task of detecting malware. Based on the experimental results, we will have a basis to evaluate the effectiveness of each algorithm in the task of detecting malware.

## IV. EXPERIMENTS AND EVALUATION

### A. Experimental Dataset

In this paper, we use the datasets about malware and normal files provided at [19]. Specifically, the dataset includes 49,128 records consisting of 24,528 malware files and 24,602 normal files. The malware and normal files are selected and extracted into the fields and components listed in Table I.

### B. Experimental Scenarios

1) *For the experimental dataset:* Based on the experimental dataset that was collected and described as in Section 4A, we will mix and randomly divide in which 80% of the number of records in the dataset will be used in the training process and the remaining 20% of the data set will be used in the test process.

2) For the classification algorithm: We will use five different algorithms to conduct experiments on the dataset presented above. To evaluate the effectiveness of each algorithm, we will conduct experiments on each algorithm with the change in their parameters. Our purpose is to evaluate and find the most efficient algorithm as well as the most optimal parameters in that algorithm. Specifically, we proceed to refine the parameters of the algorithm as follows:

- For the Random Forest algorithm, we will conduct experiments and evaluate algorithms based on the change number of decision trees respectively as 20, 30, 50, 70, 100.
- For the SVM algorithm, we select the Kernel parameter as RBF, linear, sigmoid, polynomial.
- For the MLP algorithm, we will change Activation function = ("identity", "relu", "logistic", "tanh") and Solver = ("lbfgs", "adam").
- For the CNN algorithm, firstly, we convert the entire dataset to images with a certain size. With CNN model, we have the following model: Input image -> Convolution2D -> Pooling Layer -> Fully Connected layer -> Output. The input is 49128 images with a size of 27 \* 18 (3 dimensions). Then we use alternately 3 Convolution2D layers to extract the features of the image, and 3 Pooling Layers (MaxPooling) to reduce the size of the input and still retain image characteristics. After going through many Convolution and Pooling Layers, the model has also learned the characteristics of the image and the Fully Connected Layer will combine the features of the image into the output of the model.
- For the LSTM algorithm, we will change Activation function = ("tanh", "relu", "softsign", "selu").

### C. Methods of Evaluating a System

- Accuracy: is the ratio between the number of correctly predicted points and the total number of points in the test dataset. It is calculated by the following formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

- Recall: is the ratio of the number of true positive points among actually positive points. It is calculated by the formula:

$$Recall = \frac{TP}{TP + FN}$$

- Precision: is the ratio of the number of true positive points among those classified as positive. It is calculated by the formula:

$$Precision = \frac{TP}{TP + FP}$$

- F1 Score: is harmonic mean of precision and recall (assuming that these two quantities are nonzero).

Where:

- True Positive (TP): Both the actual and predicted values are positive.
- True Negative (TN): Both the actual and predicted values are negative.
- False Positive (FP): The actual value is negative but the prediction is positive.
- False Negative (FN): The actual value is positive but the prediction is negative.

### D. Experimental Results

1) *Experimental results with random forest:* From the experimental results in Table II, we found that the accuracy of the Random Forest algorithm increases gradually when the number of decision trees increases. The algorithm gives the best classification results with all metrics when the number of decision trees is 100. The best results in classification are Accuracy, Precision, Recall, F1-score as 97.62; 99.10; 96.123; 97.59 at the number of decision trees as 100. Besides, the result classification of the algorithm for normal files is relatively high from 98.82% to 99.10% while the result classification for malware reaches only from 95.19% to 96.123%. This result is relatively good because the experimental dataset is balanced in the number of malware and normal files. Fig. 2 shows the results when testing the malware detection model using the Random Forest algorithm with the number of decision trees as 100.

From Fig. 2, can see that the algorithm incorrectly predicted 211 malwares and 42 normal files. This result is acceptable when the dataset has a large number of malwares and normal files.

2) *Experimental results with SVM:* Table III shows the results of malware detection using SVM algorithm.

The experimental results in Table III show that with the 486 features of PE file and using the SVM algorithm, we obtained the results with accuracy as 95.77%. Obviously, the default kernel of the algorithm as RBF (C = 100.0) gave the highest accuracy compared to the remaining kernels. For the Sigmoid kernel, the result is quite low (only approximately 50%). With this result, the SVM algorithm is not really suitable for this PF file-based malware detection dataset. Fig. 3 below shows the evaluation results of the process of testing the model with the SVM algorithm with parameter as RBF (C = 100.0).

TABLE II. EXPERIMENTAL RESULTS WITH RANDOM FOREST ALGORITHM

N_estimator	Accuracy	Precision	Recall	F1_score
20	97.02	98.82	95.19	96.97
30	97.07	98.78	95.33	97.02
50	97.16	98.95	95.35	97.12
70	97.25	98.89	95.59	97.21
100	<b>97.62</b>	<b>99.10</b>	<b>96.123</b>	<b>97.59</b>

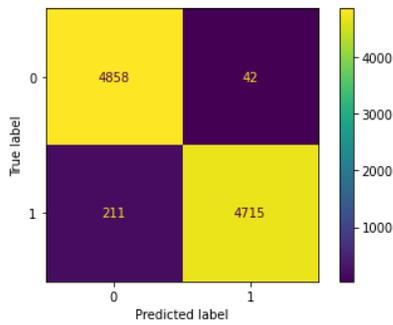


Fig. 2. Confusion Matrix when using Random Forest.

TABLE III. EXPERIMENTAL RESULTS OF DETECTING MALWARE USING SVM ALGORITHM

Kernel	C	Accuracy	F1_Score	Recall	Precision
RBF	1	93.40	93.40	93.40	93.46
	10	95.47	95.47	95.48	95.51
	100	95.77	95.78	95.78	95.78
Linear	1	87.06	87.06	87.07	87.14
Polynomial	1	92.45	92.45	92.45	92.45
	10	95.13	95.12	95.13	95.15
Sigmoid	1	49.56	49.56	49.56	49.56
	10	49.31	49.31	49.31	49.31

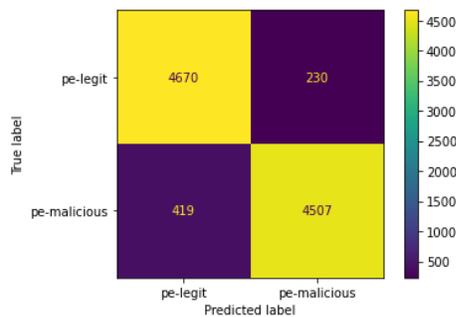


Fig. 3. Confusion Matrix when using SVM with kernel RBF/C=100.0.

From Fig. 3, we can see that the results with the test dataset are as follows: the algorithm correctly predicted 4,507 malware, incorrectly predicted 230 normal files into malware and predicted missing 419 malware.

Based on the experimental results in Table III, we noticed that the Random Forest algorithm is more efficient than the SVM algorithm.

3) *Experimental results with MLP*: Table IV shows experimental results of detecting malware using the MLP algorithm in some cases with custom activation and solver.

From the experimental results in Table IV, we noticed that the more layers and complex the architecture, the higher the classification result of MLP model is. However, the case given the best classification result of MLP model had the number of Hidden Layer as 256, activation as "tanh" and solver as "adam".

With this result, the MLP model has improved the efficiency in the malware classification process compared to the SVM and Random Forest algorithms. However, this model is not as efficient as the Random Forest algorithm in normal file classification.

TABLE IV. LIST OF MALWARE BEHAVIOR FEATURES IN PE HEADER EXPERIMENTAL RESULTS OF DETECTING MALWARE USING MLP ALGORITHM

Activa-tion	Layer	Accuracy	F1 Score	Recall	Precision
relu	256	97.13	97.13	97.52	96.73
	128-256	97.03	97.03	97.04	96.98
	128-128-256	96.97	96.97	97.71	96.24
	128-256-512-512	97.09	97.08	97.7	96.46
tanh	256	97.16	97.14	97.99	96.11
	128-256	96.79	96.78	97.33	96.24
	128-128-256	96.99	96.98	97,75	96.22
	128-256-512-512	97.05	97.03	97.77	96.31
logistic	256	96.96	96.95	97.41	96.44
	128-256	96.41	96.42	96.65	96.18
	128-128-256	96.4	96.4	96.43	96.39
	128-256-512-512	96.58	96.59	96.57	96.61
identity	256	89.11	88.94	90.57	87.37
	128-256	89.23	89.07	90.65	87.55
	128-128-256	89.07	88.44	90.23	87.7
	128-256-512-512	89.61	89.51	90.62	88.43

4) *Experimental results with LSTM*: Table V shows some experimental results of detecting malware using LSTM model with different activation functions including "tanh", "relu", "logistic", and "identity". Corresponding to the activation functions, we have the different number of hidden layers.

From Table V, it can be seen that when using the model trained with the activation function as "relu" (default) and the number of hidden layers as 1 (1024), we had the best results with accuracy as 98.73%, precision as 98.81%, recall as 99.55% and f1 score as 99.18%. These results are quite high. However, with the malware detection problem, if precision is 98.81%, with 49128 files (dataset used in the experiments), the model will detect incorrectly 584 files. Leaking 584 files is considered quite bad because there may be malware files in these files which leads to affecting the work as well as personal data of users and businesses. Considering recall, with recall as 99.55%, the rate of mistakenly detecting malware files to normal files is at an acceptable level (0.45%). Assuming have 1000 malware files, the model can only detect 995 files, the remaining 5 files are classified as normal files. When the number of files need to be detected increases, the rate is pretty bad. As is well known, f1 score is the harmonic mean of recall and precision. However, the loss ratio of the f1 score is still approximately 0.82%. This is acceptable in terms of training

ratio but it would be bad when the data need to be detected is very large. Overall, hidden layers with the “relu” activation function give better results (accuracy, f1 score, recall, and precision) than ones with the other activation function. Therefore, for the problem of detecting malware using the LSTM algorithm, to optimize it, we will use the "relu" activation function and the corresponding hidden layers.

TABLE V. EXPERIMENTAL RESULTS OF DETECTING MALWARE USING LSTM

Activa-tion	Layer	Accuracy	F1 Score	Recall	Precision
tanh	1024	98.17	98.53	98.38	98.68
	32-32-32-32	97.39	97.39	97.41	97.38
	32-64-64-128	97.46	97.46	97.47	97.46
	128-128-256-512	97.76	97.76	97.78	97.76
	128-512-512-512	97.56	97.57	97.61	97.57
relu	1024	98.73	99.18	98.81	99.55
	32-32-32-32	97.7	97.71	97.03	97
	32-64-64-128	96.94	96.93	96.97	96.93
	128-128-256-512	97.79	97.79	97.8	97.89
	128-512-512-512	97.89	97.88	97.9	97.89
softsign	1024	98.37	98.74	98.72	98.77
	32-32-32-32	97.49	97.48	97.5	97.48
	32-64-64-128	97.3	97.29	97.36	97.29
	128-128-256-512	97.91	97.91	97.93	97.9
	128-512-512-512	97.96	97.57	97.96	97.96
selu	1024	98.23	98.63	98.39	98.86
	32-32-32-32	97.19	97.17	97.22	97.17
	32-64-64-128	97.36	97.59	97.31	97.88
	128-128-256-512	97.52	97.77	97.28	98.28
	128-512-512-512	97.69	97.69	97.7	97.69

5) *Experimental results with CNN:* Table VI shows some experimental results of detecting malware using CNN model with different activation functions including "Image", "No image", "1D".

We noticed that when the input data is converted to images, we had the best results and the difference between the layers is very small (approximately 0.0001 - the results are rounded). The accuracy and f1 score are very good (99.97%). We think this is a very good classification model. With approximately 4% lower, 1D gave the second best results. This model is better because its f1 score is higher than the other two models. As shown in the previous sections, the f1 score helps to choose the best model since it is the harmonic mean of recall and precision. To test the accuracy of CNN after training, we put in a test set including 30,000 images consisting of malware

and normal files, the results are similar to the trained model. The algorithm detects completely correct input data. Of course, when the data set is larger, there will be errors in detection. Fig. 4 below shows the evaluation results of the process of testing the model with the CNN algorithm.

Based on the confusion matrix, it can be seen that the model detected very well with the test dataset because there is no file that the model detected incorrectly. The following is a graph that shows the accuracy, loss, f1 score, recall, precision of train and test data during 20 epochs. It can be seen that the train and test ratio increased sharply in the 3rd epoch and stayed the same until the end. Fig. 5 describes in detail the results of this experiment.

E. General Evaluation

After conduct experiments with 5 different algorithms that are SVM, Random Forest, CNN, MLP, LSTM, we have the best results of each algorithm.

Comment: Based on the comparison table (Table VII) of algorithms when analyzing the same file data, we can see that CNN gave the results with the highest accuracy of 99.99%. The algorithm detects completely correct input data.

TABLE VI. EXPERIMENTAL RESULTS OF DETECTING MALWARE USING CNN

Train method	Model train	Accuracy	F1 Score	Recall	Precision
Image	256	99.97	99.97	99.94	1
	16-32-32	99.97	99.97	99.94	1
	32-32-64-64	99.97	99.97	99.94	1
	64-64-128-128-256	99.97	99.97	99.94	1
No image	32	91.4	91.42	91.4	91.4
	32-64	93.81	93.83	93.81	93.81
	64-128	93.86	93.88	93.86	93.86
1D	32-64	94.08	94.06	94.08	94.08
	32-64-128	95.41	95.42	95.41	95.41
	64-128-256	95.29	95.64	93.28	98.11

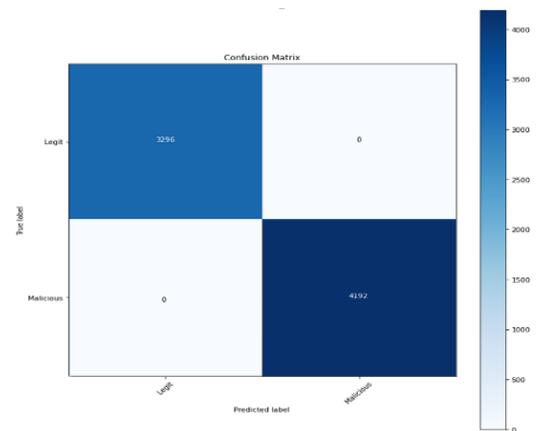


Fig. 4. Confusion Matrix when using CNN.

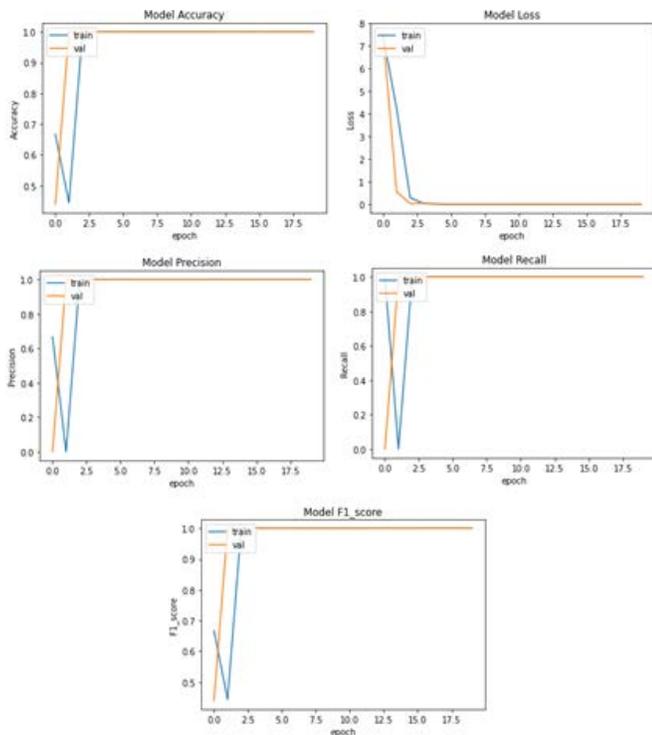


Fig. 5. Accuracy and Loss after 20 Epoch.

TABLE VII. COMPARING ALGORITHMS WHEN ANALYZING THE SAME PE FILE DATA

Algorithm	Accuracy	F1 Score	Recall	Precision
CNN	<b>99.97</b>	<b>99.97</b>	<b>99.94</b>	<b>1</b>
LSTM (activation="relu", layer=256)	98.46	98.94	98.72	99.15
RF(N_estimator = 100)	97.62	99.1	97.59	96.12
MLP (Layer=256, activation="tanh", solver="adam")	97.16	97.14	97.99	96.11
MVC (kernel = RBF, C=100)	95.78	95.78	95.78	95.78

## V. CONCLUSION

In this paper, based on the PE File analysis technique, we proposed some features that represent abnormal behaviors of malware. The experimental results in section 4.3 have demonstrated that the features that are extracted from the PE File and selected and proposed by us gave good results, it correctly classified not only for normal files but also for malware. Besides, based on the experimental results of algorithms with different parameters, we have proven that the CNN algorithm gave better efficiency than the remaining algorithms in all aspects. Especially, in this dataset with a relatively high number of features (485 features), the CNN algorithm brought the best results. In the future, in order to improve the efficiency of the malware detection process based on PE File analysis, we need to improve two main issues: i) extracting additional features of malware based on PE File. We found that the PE File consists of many different

components and has many important components that are exploited by malware developers to conceal information about malware behavior. Therefore, analyzing detailed and generalizing these features will significantly improve the efficiency of the malware detection process in the context of increasing malware in both quantity and form of distribution; ii) use other advanced machine learning algorithms. Obviously, classical machine learning algorithms have brought good efficiency to the classification process. However, due to the real situation about the rapid increase in the number of malware behaviors as well as the amount of experimental data, other advanced classification algorithms are required to ensure the effectiveness of the detection and monitoring process.

## REFERENCES

- [1] Daniel Gibert, Carles Mateu, Jordi Planes, "The rise of machine learning for detection and classification of malware: Research developments, trends and challenges," *Journal of Network and Computer Applications*, vol. 153, pp. 1-22, 2020.
- [2] Ucci, Daniele & Aniello, Leonardo, "Survey on the Usage of Machine Learning Techniques for Malware Analysis," *Computers & Security*, 2017, 81. 10.1016/j.cose.2018.11.001.
- [3] Sanjay Sharma, C. Rama Krishna, Sanjay K. Sahay, "Detection of Advanced Malware by Machine Learning Techniques," 2019, arXiv:1903.02966.
- [4] Alireza Souri, Rahil Hosseini, "A state-of-the-art survey of malware detection approaches using data mining techniques," *Human-centric Computing and Information Sciences*, vol. 8(1), pp. 1-22.
- [5] Kaspersky-Lab, "Machine Learning Methods for Malware Detection," 2020.
- [6] R. Islam, R. Tian, L. M. Batten, S. Versteeg, "Classification of malware based on integrated static and dynamic features," *Journal of Network and Computer Applications*, vol. 36 (2), pp. 646–656, 2013.
- [7] C.-T. Lin, N.-J. Wang, H. Xiao, C. Eckert, "Feature selection and extraction for malware classification," *Journal of Information Science and Engineering*, vol. 31 (3), pp. 965–992, 2015.
- [8] A. Mohaisen, O. Alrawi, M. Mohaisen, "Amal: High-fidelity, behaviorbased automated malware analysis and classification," *Computers & Security*, vol. 52, pp. 251–266, 2015.
- [9] S. Palahan, D. Babi'c, S. Chaudhuri, D. Kifer, "Extraction of statistically significant malware behaviors," *Computer Security Applications Conference*, ACM, pp. 69–78, 2013.
- [10] Gavrilut, Dragos, Mihai Cimpoesu, Dan Anton, Liviu Ciortuz, "Malware Detection Using Machine Learning," *The International Multiconference on Computer Science and Information Technology*, 2009.
- [11] Priyank Singhal, Nataasha Raul, "Malware Detection Module using Machine Learning Algorithms to Assist in Centralized Security in Enterprise Networks," 2015.
- [12] Baldangombo Usukhbayar, Nyamjav Jambaljav, Shi-Jinn Horng, "A Static Malware Detection System Using Data Mining Methods", Cornell University, 2013.
- [13] Alazab, Mamoun, Sitalakshmi Venkatraman, Paul Watters, Moutaz Alazab, "Zero-day Malware Detection based on Supervised Learning Algorithms of API call Signatures," *Proceedings of the 9-th Australasian Data Mining Conference*, pp. 171-181, 2011.
- [14] Nakajima, Tatsuo & Ishikawa, Hiroo & Kinebuchi, Yuki & Sugaya, Midori & Lei, Sun & Courbot, Alexandre & Zee, Andrej & Aalto, Aleks & Duk, Kwon, "An Operating System Architecture for Future Information Appliances," pp. 292-303, 2008, 10.1007/978-3-540-87785-1\_26.
- [15] C. Corinna, V. Vladimir, "Support-vector networks," *Machine Learning*, vol. 20, pp. 273-297, 1995.
- [16] S.S. Shai, B.D. Shai, "Understanding Machine Learning: From Theory to Algorithms," Cambridge University Press, 2014.

- [17] JohnShawe-Taylor, ShiliangSun, "Kernel Methods and Support Vector Machines," Academic Press Library in Signal Processing, vol. 1, pp. 857-881, 2014.
- [18] LEO BREIMAN, "Random Forests", Machine Learning, vol. 45, Issue 1, pp. 5–32, 2001.
- [19] Daniel Svozil, Vladimir Kvasnicka, Jiří Pospíchal, "Introduction to multi-layer feed-forward neural networks," Chemometrics and Intelligent Laboratory Systems, vol. 39(1), pp. 43-62.
- [20] Zewen Li, Wenjie Yang, Shouheng Peng, Fan Liu, "A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects," 2020, arXiv, arXiv:2004.02806.
- [21] Keiron O'Shea, Ryan Nash, "An Introduction to Convolutional Neural Networks," 2015, arXiv, arXiv:1511.08458.
- [22] Sepp Hochreiter, Jürgen Schmidhuber, "Long Short-Term Memory," Neural Computation, vol. 9(8), pp. 1735 – 1780, 1997.

# Efficient and Secure Group based Collusion Resistant Public Auditing Scheme for Cloud Storage

Smita Chaudhari<sup>1\*</sup>, Gandharba Swain<sup>2</sup>

Department of Computer Science and Engineering  
Koneru Lakshmaiah Education Foundation, Vaddeswaram-522502  
Guntur, Andhra Pradesh, India

**Abstract**—Tremendous changes have been seen in the arena of cloud computing from previous years. Many organizations share their data or files on cloud servers to avoid infrastructure and maintenance costs. Employees from different departments create their specific groups and share sensitive information among group members. Revoked users from the group may try to access this information by colluding with an untrusted cloud server. Many researchers have specified revocation procedures using re-signature, proxy-re-signature concept to deflect the collusion between the cloud server and a revoked user. But these techniques are costly in terms of communication overhead and verification cost if combined with auditing techniques to prove the integrity of outsourced data on the cloud server. To reduce this cost, a collusion resistant public auditing scheme with group member revocation is proposed in this paper. In this scheme, the data owner regularly updates the recent valid members list which is used by a third-party auditor to validate the signature so that collusion can be avoided. To verify the integrity of outsourced data, proposed scheme uses one of the modern cryptographic technique indistinguishability obfuscation combined with a one-way function which can reduce the verification time significantly. Experimental results show that the proposed scheme decreases the communication overhead and verification cost compared to existing schemes.

**Keywords**—Public auditing; collusion attack; ring signature; message authentication code; indistinguishability obfuscation; dynamic data

## I. INTRODUCTION

With the rapid growth of data, many organizations or even individuals has started outsourcing data at cloud storage. Outsourcing data at remote places reduces the burden of storage management at a local site as well as the infrastructure and maintenance costs of an organization. But this cloud paradigm has brought with it many new challenges related to security. Since data may be stored at different remote servers, cloud users are not having ownership of their own data. Data integrity at an untrusted Cloud Server (CS) is a major security concern [1]. Outsourced data may intentionally or accidentally be deleted at remote sites. CS may hide such incidents from users to maintain reputation. Periodic verification may consume resources and create a burden on the user side. To get rid of this, the cloud user delegates this verification responsibility to a Third-Party Auditor (TPA) who is a professional and having the capability to check the integrity of the outsourced data periodically on behalf of the user. Public auditing is a technique by which TPA can check the

correctness of data without copying the entire data file at its end.

Sharing services such as Dropbox and Google Drive are widely used by cloud users to share the data with multiple members in the group. Group Manager creates a group with multiple users. The group manager or any group user uploads shared data or files which can be retrieved or edited by all the group members. Before uploading a file on CS, group users need to calculate the signature to maintain and confirm the integrity of outsourced data. Whenever any user wishes to modify the data, that user has to resign that modified blocks. When users left the group, the revocation must be done properly so that revoked users are no longer able to access information from the group. The signature of blocks computed by revoked users must be recomputed by existing users. Wang et al. [2] proposed an efficient public auditing scheme Homomorphic Authenticable Proxy-Re-Signature scheme (HAPS) with user revocation. But with this scheme information may be revealed to the revoked user because of collusion between revoked user and CS.

Security threats can be classified as *internal* and *external* threats. Many organizations concentrate only on external threats because of confidence that internal threats can be monitored by organization policies and access rights. Hence they concentrate on an unfamiliar outsider who can get unauthorized access to their information. Although it is not possible for one entity to get unauthorized access, dishonest internal and external participants may collaborate and launch a collusion attack to get sensitive data [3].

Public auditing for cloud storage system comprises Cloud users, CS, and TPA. For the efficient processing of the auditing system, many auditing schemes assume all these entities to be honest and fully trusted. But in practice, some of these entities may be dishonest and can collude with each other to generate a collusion attack. Guo et al. [4] proposed an Outsourced Dynamic Provable Data Possession (ODPDP) scheme where any one of the three participants may be dishonest or two entities may collude with each other. By using a log-audit mechanism, the scheme resists any dishonest participant or collusion. In most auditing techniques, TPA is assumed to be expert, reliable, and having capability to validate the outsourced data on behalf of cloud user. But in real life, certain TPAs are honest but curious. They may collude with CS to pass the verification of some corrupted events. Many researchers have given solution [5]-[7] to detect

\*Corresponding Author

and prevent collusion from dishonest TPA using feedback method or game-theoretic analysis.

In certain situations during partial and total file loss, CS is one entity that is not trusted. CS may try to deceive users by manipulating verification tags and proving to possess correct files. CS may delete less frequently accessed user data to create space for new data. To manipulate this event, CS may collude with TPA to pass the verification and deceive the user. Many researchers [8]-[10] have given solution using pseudo-random string or pairing-based server aided verification scheme to detect and prevent collusion from malicious CS.

Cloud users many times create groups and share the contents with each other. Revoked users from group may collude with CS or TPA to get unauthorized access of sensitive information. To avoid collusion due to revoked user, it is necessary to re-sign the blocks signed by the revoked user previously or regularly update the valid user list to CS or TPA so that they can differentiate between valid and revoked user. Zhu and Jiang [11] proposed a secure anti-collusion data sharing as well as revocation scheme for a dynamic group. In this scheme, if a user is revoked, Group Manager generates a new random re-encryption key. Using this key encrypts the block and signs the message with latest timestamp. So, there is no need to re-compute and update the secret keys of other users.

Group signature is a cryptographic technique in which any group member can sign the data but the identity of signer is anonymous in generated signature. To create a confidential network among group members, Group Key Agreement (GKA) protocol is used. Rather than a common symmetric key among group members, Wu et. al[12] proposed Asymmetric Group Key Agreement (ASGKA) protocol in which public key can be used to validate signature as well as encrypt messages whereas any signature can be used to decipher the ciphertext under this public key. Many researchers [13-14] have proposed revocation techniques using ASGKA and verifier local verification to avoid collusion. However, these schemes create increased communication and computation overhead.

To overcome the overhead of computation, Hequn et.al. [15] utilized backup files for resigning after user has revoked. In this scheme, they store original as well as backup files on cloud during upload. When user is revoked, the existing user will resign on the backup file instead of original. So revoked users do not have to share their security credentials with cloud.

In previous schemes, after revocation, signature of a revoked user has to be re-calculated by the existing user. This may create computation and communication overhead on the existing user. Proxy re-signature scheme can be used in which semi-trusted proxy computes re-signature on behalf of group instead of existing user. Many revocation schemes are proposed [16-18] with proxies to convert signatures from revoked users which reduces overhead of CS and Group users. Yuan and Shucheng [29] proposed public auditing with data sharing between multiple users. They have proposed revocation technique in which constant size of integrity proof information is transmitted to verifier.

Ring Signature [19] is another variation of group signature in which user can sign messages using his own private key and the other's public key, without their consent or concern. Thokchom and Saikia [20] proposed collusion avoidance with integrity verification using ring signature approach.

To check the correctness of outsourced data or auditing, using traditional cryptographic techniques for example homomorphic authenticators, Elliptical curve cryptography, or identity-based cryptography, proof generation and verification time is a major challenging issue. Since most of these techniques are based on bilinear pairing, computation overhead leads to greater verification time. To reduce this, modern cryptography technique known as Indistinguishability Obfuscation (IO) [21] was used by many researchers [22]-[24] for public auditing. These researchers have shown that IO combined with one-way function (OWF) greatly reduces the verification time during auditing process. Sun et.al.[30] proposed auditing using IO with symmetric key. Rabaninejad et.al.[31] proposed lightweight auditing using ID-based cryptography.

The main contribution of our work is as follows:

- Zhang et.al [22] proposed public verification scheme using IO. In this scheme, group based verification is not considered. In this paper, Zhang et. al.[22] scheme is extended by forming group of members where different users can share the files.
- Zhang et.al.[22] scheme identified collusion attack between malicious auditor and cloud server but has not given any solution for this. Thokchom and Saikia [20] proposed collusion handling between revoked user and cloud server with integrity verification. This scheme uses vector commitment scheme for integrity verification which increases computation time because of bilinear pairing. Proposed scheme extends Zhang et.al[22] scheme with collusion handling of Thokchom and Saikia[20] between cloud server and revoked user.
- Comparison between existing scheme and proposed scheme is performed and shown that verification time is greatly reduced because of IO.

The remaining part of this paper is organized as follows: Section-II briefed related work. Section III elaborates brief idea about proposed work. Preliminaries for proposed scheme is in Section-IV. Section-V describes proposed work. Sections VI, VII and VIII discusses about security, performance analysis and implementation respectively.

## II. RELATED WORK

Many individuals or organizations are using different cloud services for storage as well as sharing information. Drop-box and Google Drive provides sharing services to cloud users. People communicate with each other by creating group and disclosing data among each other. To verify shared data integrity, users in group generate signature on blocks. Different blocks are signed by multiple users during modifications. To maintain security, revoked users must be treated properly. The blocks signed by revoked users must be resigned by existing user in the group to preserve integrity and

security. This may create unnecessary burden with respect to computation and communication cost. Yuan et al. [29] proposed integrity auditing scheme by multiuser modification using polynomial-based authentication tags as well as efficient user revocation. This scheme delegates user revocation process to CS to reduce the burden of user but it may create another security issue. Revoked user can collude with malicious CS to retrieve and update the data unnoticed.

Wang et al. [2] proposed a scheme named Panda that proposes public auditing of shared data with user revocation. This scheme uses homomorphic authenticators for integrity verification combined with proxy re-signature scheme. In this scheme, When a user is revoked, to reduce the resigning overhead of existing user, semi-trusted proxy is used to resign the blocks of revoked user. The idea of semi-trusted proxy avoids the collusion between CS and revoked user. But still collusion between revoked user and proxy can leak information. Again this makes system insecure since proxy can get the security credentials of revoked user during revocation.

So to create a collusion resistant public auditing system for shared dynamic cloud data, Jiang et al. [13] proposed another scheme using vector commitment and verifier-local verification group signature. The scheme is efficient but provides only partial data dynamics. Data insertion and data deletion operations are not supported by this scheme. Scheme also shows improvement during verification compared to Panda [2] Scheme.

One of the important functionality of public auditing system is lightweight. There has to be minimum communication as well as computation overhead on TPA and cloud user during verification. Zhang et al. [22] proposed public verification scheme using modern cryptography technique IO. Since IO alone is one of the weaker primitive, if combined with OWF, can implement different cryptographic primitives [21]. Zhang et al. [22] scheme has proposed lightweight public auditing scheme using IO and MAC to check the exactness of outsourced data on cloud storage. This scheme also provides dynamic data updation using Merkle Hash Tree (MHT) as well as Batch Updation. But this scheme faces collusion since user has to share MAC key to TPA. CS may collude with TPA to pass the verification of some malicious updations. Again this scheme doesn't support groups where user can share data and work in collaboration. If this scheme supports group, revoked user may collaborate with CS and TPA to generate collusion attack.

Thokcham [20] proposed collusion resistant public auditing scheme for shared data within a group. This scheme uses vector commitment for integrity verification and ring signature for group operations. Addition and revocation of group members is managed by data owner. During revocation, data owner refreshes valid member list to TPA. Collusion between revoked user and CS is not possible since during verification, TPA uses only this valid member list. Scheme also supports dynamic data updates such as insert, modify and delete. But the problem with this scheme is that as the data size is increased, computation cost during insertion operation is also increased as compared to delete and modify operation.

In conclusion, there is a need to construct lightweight collusion resistant public auditing scheme which support shared data with proper user revocation policy.

### III. OVERVIEW OF PROPOSED SCHEME

Proposed scheme involves mainly three entities: Cloud Server (CS), Cloud Users, and Third party Auditor (TPA). Cloud user encompasses data owner or other users in a group. Data owner is any group user who share a file with group members by uploading on CS. Groups are analogous to departments in organizational structure. Every department creates groups of employees in that department to share documents and files. Some employees may be a member of multiple groups.

Proposed scheme works mainly in five phases: Setup, Store, Audit, Prove, and Verify. In setup phase, security parameters are generated. User group is formed by generating private and public key pair for each user. During store phase, any group member or Data owner uploads a file  $F$  on CS. Before uploading a file, it is divided into number of blocks. Using secret parameters, file owner creates  $\tilde{F}$  which consist of file  $F$  comprising blocks  $n$ , a file tag  $\tau$ , and signatures of all data blocks  $\{\sigma_i\}_{i \in [1, n]}$ . Using ring signature scheme, file owner can sign a data with his private key and public keys of remaining members and uploads a file on CS.

During audit phase, Data Owner generates a challenging message and an auditing circuit corresponding to auditing program, obfuscates it, and passes it to CS. In the meantime, key parameters of obfuscated program are passed to TPA. It reduces the burden of computation on TPA. During prove phase, CS generates a proof based on challenge message and obfuscated program and passes it to TPA. TPA uses proof information, public parameters, challenging message and key elements of obfuscated program to generate a result of verification during verify phase by validating the proof. TPA also validates the signature with verification process of ring signature.

Collusion handling involves revocation scheme which avoid collusion between revoked user and CS. A revoked user is a group member who withdraws the group either because of retirement or any other reason. Such member must not have granted access to group information after leaving organization. File owner handles the addition and deletion of members in group. To avoid the collusion, file owner give updated list of valid users in group signed by him with timestamp to CS and TPA on periodic basis. During verification, TPA considers this latest list received to detect and avoid the collusion.

### IV. PRELIMINARIES

This section introduces Indistinguishability Obfuscation, Ring Signature and Merkle Hash Tree, which are basic building blocks of proposed scheme.

#### A. Indistinguishability Obfuscation

Concept of program obfuscation was first introduced by Barak et al. [25]. According to this work, program obfuscation is a method which create computer programs "unintelligible" but still preserve their functionality. They proposed two methods for IO: Virtual Black-Box Obfuscation(VBO) and

Indistinguishability Obfuscation (IO). VBO is nothing but a black box instantiating the program. This technique has several applications in cryptography but authors indicated that VBO is not possible to accomplish. So they have proposed another concept Indistinguishability Obfuscation (IO) which obfuscates any two different (same size) functions that implement unique functionalities, they are still computationally differentiable with respect to each other. This paper follows indistinguishability obfuscation defined by [26].

Amit and Brent [21] have shown how to create basic cryptographic primitives from IO. Pseudo-Random generator (PRG) approach produces public-key encryption where public keys are obfuscated programs and ciphertext are short. This scheme mainly contains three procedures: Setup, Encrypt and Decrypt.

Assume PRG, a pseudo random generator that maps  $\{0,1\}^\lambda$  to  $\{0,1\}^{2\lambda}$ . Let F is a puncturable PRF that contains input of  $2\lambda$  bits and generates a single bit output.

- Setup: This algorithm chooses puncturable PRF key k for F and generates an obfuscated program for PKE Encrypt function as below.

**PKE Encrypt**

Input: Punctured PRF key k, message m, random value  $r \in \{0,1\}^\lambda$ .

1. Calculate  $t = \text{PRG}(r)$
2. Produce  $c = (c_1 = t, c_2 = F(k, t) \oplus m)$ .

The obfuscated program PKE Encrypt\* is as below.

- The public key PK is the obfuscated program and secret key SK is k.

**PKE Encrypt\***

Input: Punctured PRF key  $k(t^*)$ , message m, random value  $r \in \{0,1\}^\lambda$ .

1. Calculate  $t = \text{PRG}(r)$
2. Produce  $c = (c_1 = t, c_2 = F(k, t) \oplus m)$ .

- Encrypt(PK, m): This algorithm selects an arbitrary value r and executes the obfuscated program of PK on input m, r.
- Decrypt(SK,  $c = (c_1, c_2)$ ): The output of decryption algorithm  $m' = F(K, c_1) \oplus c_2$ .

**B. Ring Signature**

Rivest et al. [19] formalized a notion of ring signature scheme for group. This scheme comprises only users. There is no centralized entity such as manager or data owner. This scheme is mainly suitable when the group members do not wish to participate or collaborate in generating signature. With this scheme, there are no prearranged groups, no procedures for altering, deleting groups, no means to issue specific keys among members and no way to revoke anonymity of genuine signer until signer's wish. These features make this scheme very useful for generating proofs in auditing system where groups are involved.

Proposed scheme utilizes CDH based Ring Signature Scheme [28] that is unforgeable and anonymous under CDH noton. Scheme uses multigenerator programmable hash function by Hofheinz and Kiltz [32]. This scheme is demarcated by two algorithms: Ring\_sign and Ring-verify.

Ring-sign: This procedure takes as input given message m. Each group member selects a secret key  $Sk = x_i$  that belongs to  $Z_p$  and public key  $Pk = g^{x_i}$ .

- Signer t uses global parameter h,  $u_0, u_1, \dots, u_l \in G_1$  of l random elements.
- Signer t will select random  $r_i \in Z_p$  for entire members of the group and calculate  $s_i = g^{r_i}$ . Signer again computes.

$$s_t = (h \cdot \prod_{i=1, i \neq t}^n Pk_i^{r_i} \cdot (u_0 \cdot \prod_{j=1}^l u_j^{f_j})^{-r_{n+1}})^{1/x_t}$$

The ultimate signature is  $\sigma = (s_1, s_2, \dots, s_{n+1})$ .

- Ring-verify: Using signature, message F, and public keys of all members, verifier checks the following equation.

$$\prod_{i=1}^n e(s_i, Pk_i) \cdot e(s_{n+1}, u_0 \prod_{j=1}^l u_j^{f_j}) \stackrel{?}{=} e(g, h)$$

**C. Merkle Hash Tree**

In cloud storage system, data holders may modify data dynamically at any time. During auditing process, the homomorphic authenticator scheme utilizes the index data that is to be used in tag computation. But modification in data results in the recomputation of all corresponding authenticators.

The Merkle Hash Tree (MHT) [27] is used to attain data dynamics through auditing. As shown in Fig. 1, the leaves of the MHT are assumed as the blocks  $f_i$  of file. A publicly qualified root value R and the Auxiliary Authentication Information (AAI) of individual leaf is utilized to check the block f. For the path that joins from the leaf to the root, AAI comprises whole siblings of the nodes. Zhang et al. [22] also used the MHT to support dynamic data during auditing. Proposed scheme uses this auditing scheme to support groups in cloud data storage.

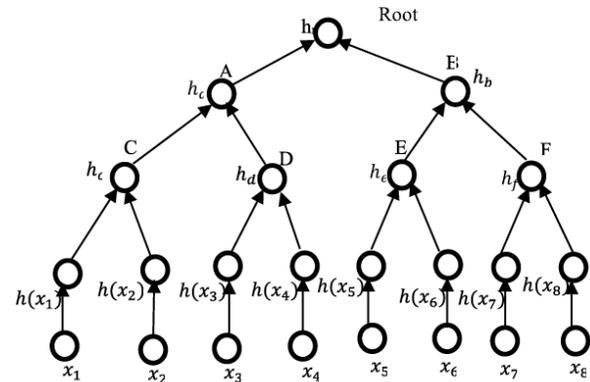


Fig. 1. MHT Authentication Tree.

V. PROPOSED SCHEME

A. System Framework

As shown in Fig. 2, proposed scheme comprises mainly three components: Cloud Server (CS), Cloud User, and Third-Party Auditor (TPA). Signer is any Cloud user form group who share file with group members by uploading it on CS. Before uploading, signer generates verification tags on file. Signer also creates an audit circuit (a program for auditing) which verifies the integrity of outsourced data. Signer obfuscates the audit circuit embedded with MAC key K. Signer shares MAC key K with TPA and obfuscated program with CS.

Based on the challenge message received from TPA, CS calculates the inputs for obfuscated program and runs the obfuscated program. Generated MAC tag is forwarded to TPA. TPA only desires to validate the MAC tag.

B. Group based Integrity Verification

The proposed scheme implements the Zhang et al. [22] framework that works in five phases: *Setup, Store, Audit, Prove, and Verify*. This scheme is modified to handle collusion attack because of group member revocation using ring signature [20].

**Setup:** Let  $G$  and  $G_T$  are two multiplicative groups produced by  $g$  with order  $p$  comprise bilinear map  $e: G \times G \rightarrow G_T$ . Data owner  $D$  selects a signing key pair  $(ssk, spk)$ ,  $\alpha, v$  where  $\alpha \rightarrow Z_p$  and  $v = g^\alpha \in G$ .  $D$  chooses  $s$  random elements.

$u_1, u_2, \dots, u_s$  and determines pseudorandom permutation and function key  $\pi_{key}(\cdot)$  and  $f_{key}(\cdot)$  respectively. The secret and public parameters are  $sk=(\alpha, ssk)$  and  $pk=(v, spk, u_1, u_2, \dots, u_s)$ . Using key generation of CDH based ring

signature scheme, group members randomly selects private key as  $x_i \in Z_p$  and  $y_i = g^{x_i} \in G$  as public key.

**Store:** Data owner transforms the data file  $F$  into blocks  $n$  and each block is again split into  $s$  sectors  $F = \{ f_{i,j} \}_{1 \leq i \leq n, 1 \leq j \leq s}$ .  $D$  computes file tag as  $\tau = \text{name} \parallel n \parallel u_1, u_2, \dots, u_s \parallel sig_{ssk}(\text{name} \parallel n \parallel u_1, u_2, \dots, u_s)$  based on randomly selected names. Also computes tag for each data block as:

$$\sigma_i = (H(i \parallel \text{name}) \cdot \prod_{j=1}^s u_j^{f_{ij}})^{\alpha}, i \in [1, n] \tag{1}$$

Where  $H()$  is any secure hash function.  $D$  has to outsource

$\tilde{F} = \{ F = \{ f_{i,j} \}_{i \in [1, n], j \in [1, s]}, \phi = \{ \sigma_i \}_{i \in [1, n]}, \tau \}$  on cloud. Before uploading on cloud,  $D$  has to sign a block on behalf of group using CDH based ring signature scheme.  $D$  randomly chooses  $u_0, r_i \in Z_p$  and compute.

$$W_i = g^{r_i} \text{ for } i = \{1, 2, \dots, n+1\} / \{j\} \tag{2}$$

Where,  $n$  – total number of user members in a group  
 $j$  – serial number of the user member in the signature who is signing it

Then compute  $h = H(\phi \parallel T)$  where  $T$  is timestamp.  $D$  again computes

$$W_j = (h \cdot \prod_{i=1, i \neq j}^n y_i r_i \cdot (u_0 \prod_{j=1}^l u_j^{F_j})^{-r_{n+1}})^{1/x_j} \tag{3}$$

The signature at time  $T$  is

$$\phi^T = (W_1, W_2, \dots, W_{n+1})$$

$D$  uploads  $F^T = \{ F = \{ f_{i,j} \}_{i \in [1, n], j \in [1, s]}, \phi^T, \tau \}$  on CS.

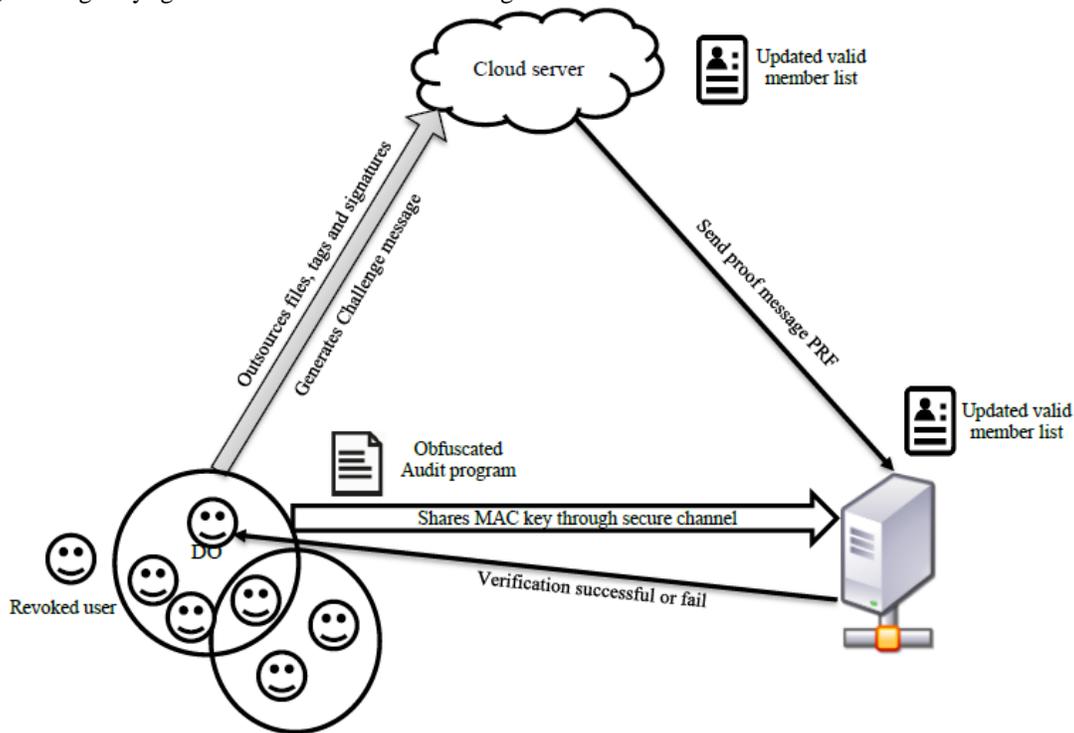


Fig. 2. Architecture of Proposed System.

**Audit:** During this phase, D selects a MAC key  $k$  and shares to TPA using a secure channel. D also generates a circuit.

*Audit<sub>k</sub>*  
 Input:  $\tau, \{(i, v_i), \mu_j\}_{i \in [1,n], j \in [1,s]}, \sigma, \{v, g, \text{spk}\}$   
 Constant: MAC Key  $K$

Validae  $\tau$   
 If no Valid  
 Output  $\perp$   
 Else  
 Deconstruct  $\tau$  to retrieve name,  $u_1, u_2, \dots, u_s$   
 If Ver  $(\{(i, v_i), \mu_j, u_j\}_{i \in I, j \in [1,s]}, \sigma, \text{name})=1$   
 Generate  $\text{MAC}_k(\text{name} \parallel \{(i, v_i)_{i \in I}\})$   
 Else  
 Output  $\perp$

*Audit<sub>k</sub>* as described above. Uniform PPT algorithm  $iO$  takes security parameters, audit circuit *Audit<sub>k</sub>* and computes public parameter  $P$  as  $P=iO(Audit_k)$ . TPA produces a challenge message using data blocks to be audited. Generates  $\{k_1, k_2\}$  which are keys for pseudorandom permutation and function respectively. TPA sends these keys to CS.

**Prove:** Using  $\{k_1, k_2\}$ , CS computes  $i=\pi k_1(\xi)$  and  $v_i=fk_2(\xi)$  where  $\xi \in [1,c]$  and  $c$  is size of  $I$  (Input blocks to be audited). Based on public parameters and corresponding  $\tau, f_{i,j}, \sigma_{i,c}$  CS computes  $\sigma=\prod_{i \in I} \sigma_i^{v_i}, \mu_j=\sum_{i \in I} v_i f_{ij}$  and

$$\text{Prf} = P(\tau, \{(i, v_i), \mu_j\}_{i \in I}, \sigma, \{v, \text{spk}\})$$

CS send this PRF to TPA for verification phase.

**Verify:** Using CDH based ring signature process, TPA verifies the group signature based on input signature  $\phi^T$  and public keys  $(y_1, y_2, \dots, y_n)$  of all members in group,  $F^T$ , public parameter  $u_0$ . TPA first calculate  $h=H(\phi \parallel T)$ . Then verifies

$$\prod_{i=1}^n e(W_{ij}, y_i) e(W_{n+1}, u_0) \prod_{j=1}^l u_j^{f_j} = e(h, g)$$

To verify the correctness of data, TPA computes  $\pi k_1(\xi)$  and  $v_i=fk_2(\xi)$  and verify  $\text{Prf} \stackrel{?}{=} \text{MAC}_k(\text{name} \parallel \{(i, v_i)_{i \in I}\})$ .

### C. User Revocation

Data owner D can revoke any user because of some reason. When data owner revokes user, the signatures calculated on file blocks by revoked user have to be re-calculated again by existing user. The re-signature process is as follows:

Initially, D selects any random user to take responsibility for the blocks earlier signed by revoked user. D selects randomly an element  $u_0$  and send it to existing user. Upon receiving this parameter  $u_0$ , existing user selects random  $r_i \leftarrow Z_p$ . Then Computes  $W_i$  using (2) for all members except himself.

The existing user also computes hash using timestamp  $T$  and then generates signature with his own secret key using (3). Re-calculated signature  $\phi^T = (W_1, W_2, \dots, W_{n+1})$  is outsourced on CS with tag calculated using (1) and original file blocks.

The existing user also prepares a valid group member list, sign the list and share it with CS and TPA. While verifying the signature, TPA uses this updated member list which helps to detect and avoid collusion attack.

### D. Dynamic Data Updation

The users can modify, insert and delete information in the files outsourced by D on CS. To enable this, Zhang et. al scheme [22] used MHT to avoid recalculation for block indexes of the file. In proposed scheme, during *Store* phase, D initially produces a tag for each data block and generates a tree with root  $\omega_{MHT}$  and sends it to TPA. During *Audit* phase, D also generates an audit circuit for dynamic support.

During *prove* phase, CS sends Prf and Auxiliary Authentication Information (AAI) which comprises path list of node siblings to reach from the leaves to the root. During *Verify*, TPA validates  $\omega_{MHT}$  and AAI. The dynamic updation scheme of Zhang et al. [22] is used as it is because even though any member of group has updated information in file, the changes are reflected in MHT during *Store* and *Audit* phase. TPA can verify the changes using  $\omega_{MHT}$  and AAI.

## VI. SECURITY ANALYSIS

This section describes security proof related to proposed system.

### A. Authenticity

**Theorem 1:** For the cloud, it is impracticable to deceive the TPA and user in case of forgery.

**Proof:** The contents of outsourced files on CS may be corrupted or deleted intentionally or unintentionally (Hardware Failures). With proposed scheme, CS can't hide these changes from TPA and user. We prove this by a simple game sequence as follows: Assume  $\widetilde{CS}$  as malicious who try to pass the verification for corrupted data blocks.

- 1) The challenger selects  $(\text{ssk}, \text{spk}), \alpha, K, u_1, u_2, \dots, u_s$  as described in section V.
- 2) The challenger produces the circuit *Audit<sub>k</sub>* and calculates  $v=g^\alpha, iO(Audit_k)$  and set it as public parameter.
- 3)  $\widetilde{CS}$  generates the proof  $\widetilde{prf}$  and send it to TPA.
- 4) Challenger verifies the proof by computing *prf*.
- 5)  $\widetilde{CS}$  wins, if  $\widetilde{prf}$  differs from *prf* while challenger does not reject.

In above game, it is not possible for  $\widetilde{CS}$  to cheat challenger because of secure HMAC scheme in the system. Even though  $\widetilde{CS}$  try to pass it's corrupted data blocks, there is a difference between the proof generated, which results in verification failure.

### B. Revocation

**Theorem 2:** In proposed scheme, the group together with the CS is capable of converting the signature from one revoked user into signature of an existing user after revocation and revoked user not able to access group information with his security parameters.

**Proof:** To prove this, we use an arrangement of game as follows:

- 1) User  $U_a$  is revoked from a group because of some reason. D randomly chooses an existing user  $U_b$ , who is responsible for computing the re-signature on the blocks signed by  $U_a$ .
- 2) D randomly selects  $u_0$  and send to  $U_b$ . User  $U_b$  make  $u_0$  public and select random  $r_i \leftarrow Z_p$ .
- 3) User  $U_b$  computes  $W_i = g^{r_i}$  for all members of group except himself.
- 4) Downloads the blocks signed by  $U_a$ . Computes the hash and calculate the re-signature with his own private key  $x_j$  using (3) as in section V.

After revocation, in above game, there is no need for D or any group member to manually delete the security parameters of user  $U_a$ . User  $U_a$  even though trying to access the group information, not able to do that since user  $U_b$  has already uploaded re-signed data blocks and valid user list on CS.

### C. Collusion Resistant

**Theorem 3:** It is impracticable for the CS to fabricate valid proofs to clear the verification test, even though a revoked user colludes with the CS.

**Proof:** Considering the above same game, assume that user  $U_a$  is revoked. He colludes with CS and modified some blocks of files. When TPA gives audit challenge for this file block, CS generate the fabricated proof.

$$Prf = P(\tau, \{(i, v_i), \mu_j\}_{i \in I}, \sigma, \{v, spk\})$$

User  $U_a$  wins, if TPA does not reject and pass the verification.  $U_a$  become successful in generating collusion attack. But collusion is not possible in proposed system since whenever member is revoked, D updates the current valid signed members list to CS and TPA. While validating the signature of users, the auditor utilizes only these valid members list signed by D.

## VII. PERFORMANCE ANALYSIS

To check the performance of public auditing system for cloud storage, different functionalities can be considered. These functionalities are: third party auditing, dynamic data operation, user revocation, immune to collusion attack, membership to several groups using the same key set.

Multiple schemes proposed by different researchers explore some functionalities. Some schemes provide partial dynamic data updates such as only insertion and modification of data excluding deletion. Another functionality, lightweight auditing is the scheme in which TPA and data owner has to incur less burden as per communication and resource cost to complete the auditing task. A detailed comparison of these schemes is as below in Table I.

Initially we analyze the communication cost of proposed scheme and then evaluate it with different existing schemes. In auditing system, to analyze communication overhead consider communication between three entities: User, CS and TPA. Mostly communication overhead between user and CS is insignificant since user uploads the entire data to CS initially. So the communication overhead between CS and TPA is analyzed since these are the two entities involved in proof generation and verification process.

In proposed scheme, TPA challenges CS for specific blocks. So communication overhead between TPA and CS is  $|K_1| + |K_2| + \text{HMAC}$  where  $K_1$  and  $K_2$  are transformed keys of HMAC. Based on challenge, CS generates the proof by calculating HMAC through obfuscated program. This proof submitted to TPA for verification. During verification, TPA checks the correctness of outsourced data by confirming:

$$Prf \stackrel{\Delta}{=} MAC_k(\text{name} || \{(i, v_i)_{i \in I}\})$$

So TPA has to only calculate the HMAC. Along with this TPA has to verify the signatures of users using verification method of CDH based ring signature. So communication overhead for TPA during verification is to calculate hash and verify each user using public key of each member. During user revocation, D revokes user and existing user has to resign the blocks signed by revoked user. The existing user has to download blocks signed by revoked user, calculates hash and recomputes the signature of all n group members and signs it with his own private key. The computation cost for the above three operations compared with existing methods is shown in Table II. The meaning of each notation is as follows: M for multiplication, P stands for pairing, H means for hashing, E for exponential, c is the number of challenged blocks, q is the total number of data blocks, s is the number of elements in a block and z is number of revoked user.

TABLE I. COMPARISON OF EXISTING SCHEME IN TERMS OF FUNCTIONALITY

Scheme	Third-Party Auditor	Dynamic Data Operation	User Revocation	Immune to Collusion Attack	Membership to several groups using same key set	Lightweight
Wang et.al.[2]	Yes	full	Yes	No	No	No
Jiang et. al.[13]	Yes	Partial	Yes	Yes	No	No
Thokcham et. al[20]	Full	Yes	Yes	Yes	Yes	No
Zhang et. al.[22]	Yes	Yes	No	No	No	Yes
Yuan and Shucheng[29]	Yes	Partial	Yes	No	No	No
Proposed System	Yes	Yes	Yes	Yes	Yes	Yes

TABLE II. COMMUNICATION OVERHEAD

Scheme	Proof Generation	Verification	User Revocation
Wang et.al.[2]	$cM+cE$	$(c+n)E+(c+3n)M+(n+1)P+cH$	$2E+M+2P+H$
Jiang et. al.[13]	$(q-1)(M+E)$	$7P+M+9E+5H+z(M+2P)$	$Z ( M + 2 P )$
Thokcham et.al[20]	$(q-c)(M+E)$	$(n+4)P+6E+7M+(c+1)M$	$(2n+2)E+nM$
Yuan and Shucheng[29]	$sE+(s+n)M+nP$	$6E+3M+3P$	CE
Proposed Scheme	cH	$(c+n)H$	$(c+n)E+H$

VIII. IMPLEMENTATION AND EVALUATION

In this section, the implementation and evaluation of proposed scheme are discussed with experiments. All the experiments are carried out on a system having Windows 10 with AMD A12 processor, 2.70 GHz, 4.0 GB RAM. Considering security level as 128 bits, experiments are tested 5 times and average values are taken. All algorithms are implemented using Python language. For implementation, some blocks are kept constant so the size of each block may vary.

The performance of proposed system is evaluated in terms of cost of dynamic data operations, verification time with respect to group size and communication overhead in terms of KB. To evaluate the dynamic data operation cost, mainly three operations are performed: delete, modify and insert. Verification time (in Sec) of these operations for different data sizes varying from 2KB to 1000KB files is analyzed. Fig. 3 shows the performance of proposed scheme compared with Thokcham[20] scheme. The graph shows that insertion operation cost in Thokcham [20] increases as the data size is increased whereas verification time for all three operations in proposed scheme is constant.

Verification time with respect to group size is analyzed as depicted in Fig. 4. The verification time of proposed scheme is compared with a different existing scheme such as Panda [2], Yuan [29], Jiang [13] and Thokcham [20]. PS indicates proposed scheme. Graph shows increase in verification time for scheme Panda [2] and Thokcham [20]. Whereas Yuan

[29], Jiang [13] and proposed scheme is constant even though the number of user members are increased. Evaluation of proposed scheme is performed by adding 100 users to the group. Graph proves that verification time in proposed scheme is not depending on the number of members in a group.

Table II shows the evaluation of communication overhead of proposed scheme where it is evaluated for proof generation, verification and user revocation. To calculate the complete communication overhead of auditing in terms of KB, the size of an auditing message is considered. The size of a message is calculated during integrity verification using IO technique and signature verification using CDH based ring signature scheme. The magnitude of an auditing message is  $2|MAC|.c+n+n|MAC|$  bits where,  $|MAC|$  is the size of MAC generated by CS and TPA,  $c$  is the number of challenged blocks and  $n$  is total number of users. Zhang et al. [22] scheme has given the performance of communication overhead in terms of KB by considering challenged number of blocks. Since proposed scheme is based on Zhang's [22] scheme, for comparison, communication overhead is computed with respect to the number of users in a group. Fig. 5 shows the performance of communication overhead in KB. For 10 users, the communication cost of auditing is 10.24KB. The graph shows that as the number of users are increased, auditing message size also increased. We have not compared this computation cost with existing work because in our scheme, we have kept number of blocks as fixed during splitting the file while in most existing work, size of block is fixed. We have given the computation cost results for 200KB file, which is divided into 5 blocks of 40KB each.

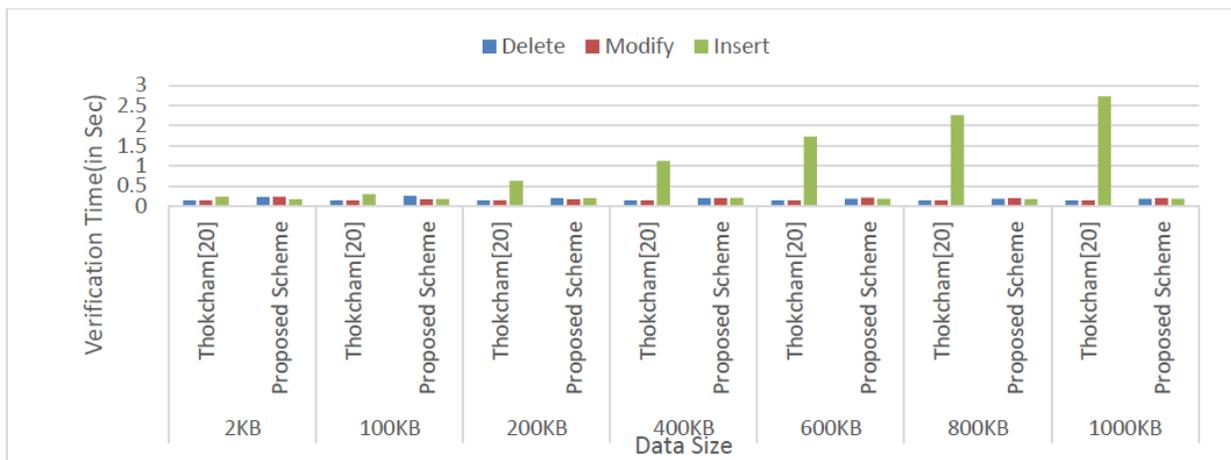


Fig. 3. Comparison of Cost for Dynamic Data Operation.

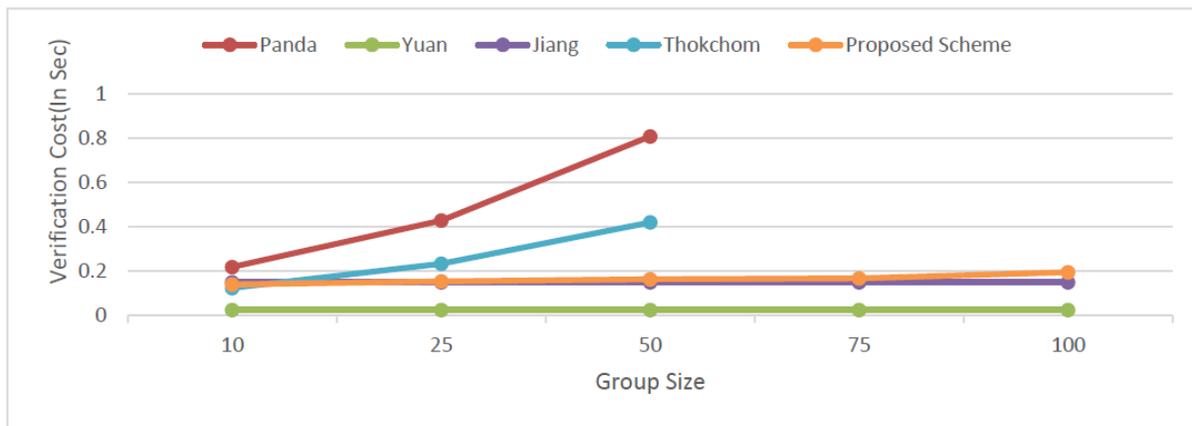


Fig. 4. Verification Time with respect to Group Size.

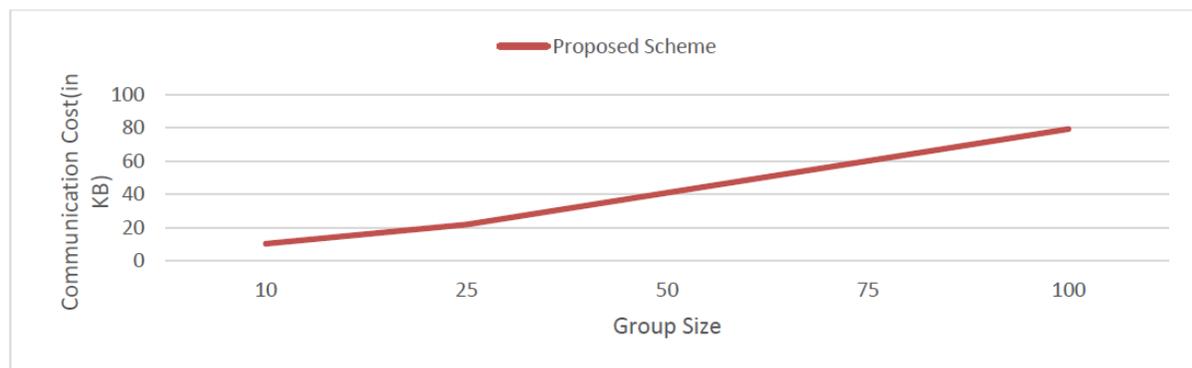


Fig. 5. Communication Cost with respect to Group Size.

## IX. CONCLUSION

This article proposes an efficient and secure auditing scheme for cloud storage using modern cryptographic technique, Indistinguishability Obfuscation. Proposed scheme allow cloud users to form a group and share information or files within group. Proposed scheme adopts ring signature scheme to sign the data files which are outsourced on cloud. During auditing, TPA check integrity of data by calculating MAC as well as signature of block using public keys of all users. Collusion may occur between revoked user and cloud if revocation not done properly. Our scheme proposed revocation policy as well as updates valid member list to CS and TPA which lead to avoid collusion in system.

The proposed scheme is efficient and lightweight since TPA only have to calculate the MAC tag for verification. The performance of proposed scheme is proved by comparing verification time during dynamic operations with existing schemes. Also analyzed the performance of communication overhead during auditing in terms of KB.

In regards to future work, we want to extend our scheme to include batch auditing in which TPA must have the competence to execute the auditing tasks concurrently. In our scheme, after revocation of any member data owner depute any existing user to re-computed the signatures of revoked user. This may create an additional burden on existing user. As a future work, we want to extend our revocation scheme to address this issue.

## ACKNOWLEDGEMENT

This research work is an independent work and no financial assistance has been received for this work.

## REFERENCES

- [1] S. Chaudhari, S. K. Pathuri, "A Comprehensive Survey on Public Auditing for Secure Cloud Storage," *International Journal of Engineering and Technology*, vol. 7, no. 2.7, pp. 564-569, 2018.
- [2] B. Wang, C. Li and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud" , *IEEE Transactions on Services Computing*, Vol. 8, No. 1, pp. 92-106, Feb. 2015.
- [3] Q. Chan, C. Zhang and S. Zhang, "Detection Models of Collusion Attacks," in *Secure Transaction Protocol Analysis- (Lecture Notes in Computer Science)*.
- [4] W.Guo , H. Zhang , S. Qin, F. Gao , Z. Jin , W. Li and Q.Wen , "Outsourced Dynamic Provable Data Possession with Batch Update for Secure Cloud Storage, *Future Generation Computer Systems* 95, pp.309-322, 2019.
- [5] K. Huang , M. Xian , S.Fu and J. Liu, "Securing the Cloud Storage Audit Service: Defending Against Frame and Collude Attacks of Third Party Auditor " , *IET Communications* , Vol 8 , No.12,pp.2106-2113,2014.
- [6] Z.Wang , S. Cheung and Y. Luo ,"Information-Theoretic Secure Multi-party Computation with Collusion – Deterrence " , *IEEE Transactions on Information Forensics and Security* , Vol.12, No.4,2017.
- [7] X.Wang, A.Hu and H.Fang , "Improved Collusion-resistant Unidirectional Proxy Re-encryption from Lattice , *IET Information Security* , Vol.14 , No.3 , pp.342-351,2020.
- [8] Z. Sun , Y. Yang , Q. Shen , Z. Wu and X. Li , "MB-DDIVR: A Map-based Dynamic Data Integrity Verification and Recovery Scheme in Cloud Storage " , In *ICICS (Lecture Notes in Computer Science)*, 2016 , pp.335-345.

- [9] S.S. Chow , M. H. Au and W. Susilo , “Server-Aided Signatures Verification Secure against Collusion Attack “, Information Security Technical Report 17 , 2013 , pp.46-57.
- [10] H. Carter and P. Traynor, “ OPFE: Outsourcing Computation for Private Function Evaluation , IACR Cryptology Epint Arch . 2016.
- [11] Z. Zhu and R. Jiang , “A Secure Anti-collusion Data Sharing Scheme for Dynamic Groups in the Cloud “ , IEEE Transactions on Parallel and Distributed Systems , Vol.27 , No.1, pp40-50 , Jan.2016.
- [12] Q. Wu , Y. Mu , W. Sucilo, B. Qin and J. Domingo-Ferrer , “A Symetric Group Key Management “ in Proc.International Conference On the Theory and Applications of Cryptographic Techniques , 2009,pp.153-170.
- [13] T. Jiang , X. Chan and J. Ma , “ Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation “ , IEEE Transactions on Computers , Vol.65 , No.8 , Aug.2016.
- [14] S. Kumar and L. Parthiban , “Cloud Data Integrity Auditing Over Dynamic Data for Multiple Users “ , International Journal of Intelligent Engineering and Systems , Vol.10 , No.5 , pp.239-246 , 2017.
- [15] L. Hequn , W. Baocang , L. Ke , G. Ziyuan and Z. Yu , “ Public Auditing for Shared Data Utilizing Backups with User Revocation in the Cloud “ , Journal of Natural Sciences , Vol.23, No.2, pp.129-138, 2018.
- [16] Y. Luo, M.Xu, K. Huang, D. Wang and S. Fu , “ Efficient Auditing for Shared Data in the Cloud With Secure User Revocation and Computations Outsourcing “ , Computers and Security , Vol.73 , pp.492-506, Mar.2018.
- [17] M. Liu , Y. Wu , J. Chang , R. Xue and W. Guo , “ Verifiable Proxy Re-encryption from Indistinguishability Obfuscation “ , in Proc.International Conference on Information and communication Security(Lecture Notes in Computer Science) , pp.363-378, 2016.
- [18] L. Zhu , H. Wang , C. Xu , K. Sharif and R. Lu , “ Efficient Group Proof of Storage with Malicious-member Distinction and Revocation “ , IEEE Access Vol.7 , pp.75476-75489, May.2019.
- [19] R. Rivest , A. Shamir and Y. Tauman , “ How To Leak A Secret “ , in Proc.Theory and Applications of Cryptology and Information Security-ASIA CRYPT , pp.552-565, 2001.
- [20] S. Thokcham and D. Saikia , “ Privacy Preserving Integrity Checking of Shared Dynamic Cloud Data with User Revocation” , Journal of Information Security and Applications , pp.2214-2126 , 2020.
- [21] A. Sahai and B. Sahai “ How To Use Indistinguishability Obfuscation : Deniable Inception and More , in Proc. 46<sup>th</sup> Annual ACM Symposium on Theory of Computing , pp.475-484 , May.2014.
- [22] Y. Zhang , C. Xu , X. Linag , H. Li , Y. Mu and X. Zhang , “Efficient Public Verification of Data Integrity for Cloud Storage Systems from Indistinguishability Obfuscation “ , IEEE Transactions on Information Forensics and Security , Vol.10 , No.3, pp.676-688, Mar.2017.
- [23] S. Chaudhari , G. Swain and P. Mishra , “ Secure and Verifiable Multiparty Computation using Indistinguishability Obfuscation “ , International Journal of Intelligent Engineering and Systems , Vol.13 , No.5 , pp.277-285, Jul.2020.
- [24] C. Guan , K. Ren , F. Zhang , F. Kerschbaum and J. Yu , “ Symetric-key Based Proofs of Retrivability Supporting Public Verification “ , in Proc.ESORICS (Lecture Notes in Computer Science) , pp.203-223, 2015.
- [25] B. Barak , O. Goldreich , R. Impagliazzo , S. Rudich , A. Sahai , S. Vadhan and K. Yang , On the (im) Possibility of Obfuscating Programs , in Proc.Advances In Cryptology – CRYPTO (Lecture Notes in Computer Science) , pp.1-18, Aug.2001.
- [26] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai and B. Waters, “Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits” , in Proceedings of FOCS, IEEE 2013,pp. 40-49.
- [27] Q. Wang , C. Wang , K. Ren , W.Lou and J. Li , “ Enabling Public Auditability and Data Dynamics for Storage security in Cloud Computing “ , IEEE Transactions on Parallel and Distributed Systems , Vol.22, No.5, pp.847-859, May.2012.
- [28] S. Schage, J. Schwenk, “A CDH-based Ring Signature Scheme with Short Signature and public keys”, in Proc. FC2020 (Lecture Notes in Computer Science 6052) , pp.129-142, 2010.
- [29] J. Yuan, S. Yu, “Public Integrity auditing for Dynamic Data Sharing with Multiuser Modification”, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 8, pp. 1717-1726, 2015.
- [30] L. Sun, C.Xu, Y. Zhang and K. Chen, “Public Data Integrity Auditing without Homomorphic Authenticators from Indistinguishability Obfuscation”, International Journal of Information security, Vol.19, pp. 711-720, 2020.
- [31] R. Rabaninejad, M. Attari, M. Asaar and M. Aref, “A Lightweight Identity-based Provable Data Possession Supporting User Identity Privacy and Traceability”, Journal of Information Security and Applications, Vol. 51, 2020.
- [32] D. Hofheinz and E. Kiltz, “Programmable Hash Functions and Their Applications”, in Proc. Advances in Cryptology, LNCS 5157, pp. 21-38, 2008.

# Fog Network Area Management Model for Managing Fog-cloud Resources in IoT Environment

Anwar Alghamdi<sup>1</sup>, Ahmed Alzahrani<sup>2</sup>, Vijey Thayanathan<sup>3</sup>

Department of Computer Science  
King Abdulaziz University  
Jeddah, Saudi Arabia

**Abstract**—The Internet of Things (IoT) paradigm is at the forefront of the present and future research activities. The enormous amount of sensing data needing to be processed increases dramatically in volume, variety, and velocity. In response, cloud computing was involved in handling the challenges of collecting, storing, and processing the data. The fog computing technology is a model used to support cloud computing by implementing pre-processing tasks close to the end-user for achieving low latency, less power consumption, and high scalability. However, some resources in fog computing network are not suitable for some tasks, or the number of requests increases outside capacity. So, it is more efficient to reduce sending tasks to the cloud. Perhaps some other fog resources are idle, and it is better to be federated rather than forwarding them to the cloud. This issue affects the fog environment's performance when dealing with large applications or applications sensitive to time processing. This research aims to propose a holistic fog-based resource management model to efficiently discover all the available services placed in resources considering their capabilities, deploy jobs into appropriate resources in the network effectively, and improve the IoT environment's performance. Our proposed model consists of three main components: job scheduling, job placement, and mobile agent software, explained in detail in this paper.

**Keywords**—Resource management; job scheduling; load balancing; mobile agent software; fog computing; Internet of Things (IoT)

## I. INTRODUCTION

Digital devices have been distributed rapidly in our virtual world. These devices continuously produce a massive amount of structured, semi-structured, or unstructured data such as temperature sensors, health care devices, and transport. The output of these devices and applications results in a considerable amount of process [1]. Most digital devices and applications are connected to the Internet to make our environment smart and provide services anytime and anywhere. Anything that can be connected to the Internet and provide or produce data can be considered as the Internet of Things (IoT), which may reach 75.4 billion things in 2025 [2][3]. The IoT devices have limited processing power and memory availability; therefore, the massive amount of data generated from the sensors is collected in clouds for providing many application accesses and services to the users. However, IoT devices have been rapidly increasing, and the clouds cannot serve all these devices efficiently. Also, some IoT applications need to have processes' results as soon as possible such as controlling the moving vehicles, congestion

through a mobile pilot, and medical applications. So, fog computing firstly has been proposed by Cisco in 2012 to address the challenges between IoT devices/sensors and clouds [28]. Fog computing is a modern model which considered an extension of clouds to provide services to network parties [4]. It consists of smaller processing power, smaller memory size, and closer to the end devices. Also, it does some processors before it sends them to a cloud. It can be a significant factor in the success of some applications that are sensitive to time processing when there is a high probability of speeding up emergency detection and warning to support appropriate intelligent decision making [6]. For instance, the author in [5] presents a framework of an early-warning system based on IoT. This kind of system is critical to saving human life by providing a high response warning if there is a flood. Another instance is illustrated in [7]. The face recognition method has been increasing in many fields. It is a significant factor in making security more effective by processing the job accurately and quickly. So, the authors try to conduct the task on fog computing rather than on the cloud side to achieve low bandwidth.

In this paper, we try to solve the problem of when one fog resource is not suitable for a specific task or the number of requests increases outside capacity; it is not efficient to send all tasks to the cloud. Perhaps some other fog resources are idle, and it is better to be federated rather than forwarding them to the cloud, as mentioned in [8]. This issue affects the fog environment's performance when dealing with huge applications or applications that are sensitive to time processing.

This paper aims to provide a new solution that can efficiently utilize the fog computing network's capability and increase the performance of IoT applications. We build a holistic fog-based resource management model which efficiently discovers all the available resources with their capabilities, deploys jobs into appropriate resources in the network effectively, and improve IoT applications' performance by implementing the job locally close to the end-users.

The objectives of this paper are listed as follows:

- Prioritize the jobs according to applications requirement.
- Balance and load the jobs among the fog nodes resources.

- Blend Mobile-Agent in the fog computing environment.
- Track and update the status of the cloud/fog resources.

The following is how the rest of this article is presented. In Section II demonstrates the related work for the relevant methods in the proposed solution. Section III presents the proposed (FNAMM) model. Section IV discuss the proposed model and reveals the benefits and compared to other models. Section V concludes the work and investigates the possibilities for the future work.

## II. RELATED WORK

This research's literature review can be classified based on the essential aspects that fulfil the proposed architecture. Initially, the massive amount of data generated from the smart devices would be underlined by considering their IoT environment challenges. Secondly, various studies will be presented covering resource allocation and discovering their specifications. Thirdly, some studies will illustrate the load balancing and selector techniques in the fog environment to achieve high performance.

The IoT devices have been increasing rapidly globally, leading to generating a massive amount of data through different sensors. IoT big data analytics' primary purpose is to enhance business performance by applying processes such as searching a database, analysing, and mining [9]. However, the statistics reveal that there will be around 1 trillion sensors in 2030 [10]. This challenge would be mitigated by providing enormous resources with efficient management.

Cloud computing is a powerful paradigm in providing computation and storage resources for IoT devices. However, the increasing amount of IoT devices leads to high power consumption and high latency; thus, there should be done some process in the edge of the network rather than in cloud computing [11]. Resource allocation and resource scheduling technologies manage the data centres in cloud computing. These technologies enhanced resource utilization and established load balancing for the data centres. As a result, bottlenecks and overloaded have been addressed [12]. Resource allocation is not an easy job in fog computing since the computing nodes are distributed in the network edge. In cloud computing, the computing nodes are distributed in a centralized data centre.

It is not an easy job of discovering edge resources to deploy workloads from IoT devices or clouds [13]. Many techniques are implemented for discovering edge resources using handshaking protocols, programming infrastructure, and message passing. A new handshaking protocols technique for discovering edge resources has been presented in [14]. This technique is based on the Edge-as-a-Service (EaaS) platform, which can discover a set of homogeneous edge resources. This kind of platform needs a master node that can execute a manager process and communicate with edge resources. After identifying the appropriate node, the Docker containers would be deployed on that node. The authors in [15] proposed a new programming infrastructure mechanism called Foglest that allows edge resources to join a cloud system. This mechanism's protocol can match the application's edge

resources requirements against the available and appropriate resources on edge.

Moreover, the protocol can select a node from a set of edge resources closer to the user. The last technique for discovering edge resources is message passing. In [16], the user can submit a query to an edge node in the network by relying on simulation-based validation. Nonetheless, the edge nodes are not necessary to be connected to the Internet.

Thus, there is a need for developing resource management for IoT applications to achieve efficient load balancing in the fog environment [17]. Moreover, a system model for managing mobile cloud network's network resources has been presented effectively in [18]. One of the challenges in fog computing is to select appropriate edge resources to place computation tasks from cloud and IoT devices. There is needed for efficient selector algorithms that can address this issue by considering the availability of edge resources with their capabilities [16]. In [19], the authors proposed a new method for managing mobile and edge devices. The fog resources are distributed in decentralized mode, and IoT devices connection is peer-to-peer in a decentralized mode as well. The problem of distributing tasks in fog computing has gained attention from researchers recently. The authors in [20] have analysed the offloading policy between multiple fog nodes in a ring topology. In [21], a distributed policy for tasks assignment that can be executed efficiently in the network edge cloud has been proposed. The author has not considered the communication between fog-to-cloud and IoT-to-cloud. This model's scalability is limited since the cloud servers send their status continuously to the mobile subscribers. It will not be comfortable with an immense amount of edge devices.

The authors in [22] proposed a new load balancing technique for fog nodes by combing graph partitioning theory and fog computing characterizing. To achieve a dynamic load balancing in fog computing, the authors considered graph repartitioning.

For managing a massive amount of data in a cloud environment with low cost, the authors in [23] replaced physical network balancers with virtualized network balancers. The virtualized network balancer consists of two parts; the first load is a master, and the other acts as a secondary, which includes network load balancers and load balancer selector.

This kind of balancer is better than a hardware balancer since the cost is reduced and the user can efficiently add or remove an algorithm to the system. The authors in [24] proposed a cooperative load-balancing model for fog/edge data centres to mitigate the delay services. The idea is to assign a specific buffer for each data centre to receive requests from other nodes. Once the number of requests exceeds a certain threshold, the coming request is moved or balanced to an adjacent node. This kind of work anticipates the nodes are connected by the high-speed connection for achieving effective load balancing.

Based on the literature review and to the best of our knowledge, there is no work yet that employs mobile agents, resource capabilities, and considering idle fog nodes to build a

fog-based resource management model for enhancing the performance of big data application in IoT environment and improving fog computing resource utilization.

A new formulation is introduced for combined Cloud-Fog architectures [25]. The formulation reduced the service latency with the fulfilment of the Quality of Service (QoS) requirements. Moreover, the author used Gurobi Optimizer for addressing the Integer Linear Programming (ILP) model. In [26], the authors focus on the application models that increase the application deployment region. Also, they considered the placement strategy on edge and cloud platforms. The author presented a framework that increases the utilization of fog resources [27]. When a service is requested, the provisioning plan is implemented. Considering the workload is mentioned in [28], a new policy is proposed to determine the workload allocation on Fog-Cloud computing services considering the trade-off between the delay and power consumption. The authors split the original problem into three sub-problems in order to address each sub-problem separately. Three methods have been used in this framework; Generalized Benders Decomposition, convex optimization, and Hungarian. The authors in [29] provided a new model that is based on the mathematical service placement for the fog computing environment. This research aims to reduce the blocking probability, the percentage between the rejected workloads and the total workloads. The purpose of the research in [30] is to reduce network usage by presenting an optimization policy for data placement in the fog environment. This can be achieved by finding out the closest path between the fog device and the data source (IoT device). Minimizing the response time and maximizing the throughput are achieved in [31]. The algorithm distributes the workload on the fog resources environment. A job scheduling technique is also applied for Virtual Machines (VM) based on the service level agreement. In [32], the authors proposed a system to allocate and offload the service between the cloud server and fog computing. The decision rule relies on three conditions: completion time, services sizes, and the capacity of fog resources. Another algorithm is proposed to satisfy the Service Level Agreement (SLA) and Quality of Service (QoS) and enhance the major data distribution in fog and cloud environments. Finally, the services mapping based on their priority level, the highest one would be mapped first, and so on. A new service placement framework is proposed in [33]. The authors attempt to reduce the latency considering the cost budget constraints. The Lyapunov optimization function is used in this framework to split the main problem into a set of problems with not considering user mobility. The author in [34] used machine learning to minimize the service costs and maintain the QoE. The Q-learning has been applied for defining the optimal migration for each service request. The authors in [35] demonstrate some of the service placement strategies in Edge-Cloud computing environments. This research aims to minimize the failed requests by formulating the problem as Mixed Integer Linear Programming (MILP). Two scheduling policies are used in this research: Earliest Deadline First (EDF), and First-In-First-Out (FIFO). The problem of dynamically deploying applications on fog resources, which should satisfy the Quality of Service (QoS) constraints, has been discussed in [36]. The authors expressed

the previous problem as Integer Non-Linear Programming (INLP). Two heuristics are used to address the problem: a) Min-Cost: it is used to reduce the overall cost. b) Min-Vol: it is used for reducing deadline violations. The authors in [37] proposed a methodology to illustrate when and where the services should be placed. The placement strategy is based on the request ratio and user mobility in the edge network. The issue is modelled as a sequential decision-making Markov Decision Problem (MDP). Then the authors apply Lyapunov optimization on the two divided MDPs. As a result, the cost is reduced for each of the location constraints, delay, and execution. In [38], the research reflects the data locality. The author's design architecture consists of three tiers. The aims are to dynamically route the data to an optimal server and optimize the computing capacity. The prototype was implemented on the OpenStack virtualization environment by integrating the Software-Defined Network and Network Functions Virtualization (NFV). The architecture implemented on IoT surveillance system application, also a specific scheme is proposed in case of an urgent situation. Considering the load balancing to reduce the fog nodes' power consumption only is proposed in [39]. The author proposed an algorithm to allocate the fog resource efficiently. This algorithm is based on ordering the fog resources increasingly according to two factors: the availability and capacity to serve more tasks. Then assigning a threshold for each resource to keep them in a stack this mechanism helps utilize all available resources in the network. The result shows that the power consumption is reduced slightly compared to load balancing algorithms such as Round Robin and Throttled.

The load balancing and task distribution policy play a significant factor in optimizing the fog system's application performance. The centralized load balancing controller must gather information about all network devices to generate global optimization decisions. However, this kind of controller may not be efficient on some applications since all the devices should send the applications to a manager. The centralized core will generate the decision. Besides, one of the centralized controller dilemmas is a single point of failure that makes the system weak. On the other side, the decentralized load balancing should not gather all the information of all devices in the network, so many managers are connected in this kind of controller. Also, make a decision is not on a single core as in the centralized controller, which makes the scalability in the decentralized controller is higher than a centralized one.

Moreover, a decentralized controller's performance exceeds a centralized one since network overhead is high in the centralized controller. Overall, it is better to adopt the centralized and decentralized approaches in a new approach that can overcome both approaches' limitations.

The task distribution or job scheduling approaches can be divided into static and dynamic. The necessary information about the demands and available resources has been accomplished in the static approach before receiving the tasks. Also, the tasks would be sent at one time, and the scheduling decision has already been made. This approach is not suitable for the fog system because it is not easy to have all the necessary information about all devices in fog networks before the execution time.

However, in the dynamic approach, the scheduling process is made once the task is received in the system. It is also efficient to build a hybrid approach that makes the fog system works more effectively with different demands and applications. A summary of some previous works, based on the load balancing controller and task distribution policy, is provided in Table I.

TABLE I. COMPARISON OF SOME WORKS BASED ON THE CONTROLLER AND POLICY

Ref. No.	Load Balancing Controller		Task Distribution Policy	
	Centralized	Distributed	Static	Dynamic
[34]	✓			✓
[33]	✓			✓
[25]		✓	✓	
[26]		✓	✓	
[32]		✓	✓	
[28]	✓		✓	
[29]	✓		✓	
[30]	✓		✓	
[35]	✓			✓
[36]	✓			✓
[37]	✓			✓
[38]	✓			✓
[31]		✓	✓	
[32]		✓	✓	

### III. PROPOSED MODEL

The proposed model aims to mitigate the drawbacks mentioned in the previous section. Initially, there is a need for a new method to handle the increase of incoming tasks from IoT devices. This can be handled by building an efficient job scheduling technique and effective job placement mechanism. Secondly, since IoT devices have been increasing recently, numerous data need to be proceed and analysed. The mobile agent software is involved in this model to reduce network cost by transferring the necessary data from the cloud server.

In our proposed model donates to the tasks that are sent from the IoT devices. The task priority plays a significant factor in reducing the responding time. On the other hand, an efficient resource management system will mitigate the cost of determining the suitable fog node from enormous resources, executing the tasks, reducing the delay, and saving power consumption by utilizing all available resources. This model consists of three main components: job scheduling, job placement, and mobile agent software. The job scheduling has a primary duty to determine the task type: mobile agent or not. Also sorts the tasks depending on the priority that is assigned from the application requirement. The mobile agent is responsible for dealing with tasks requiring service on the cloud server, such as inquiries in the cloud data center. The job placement sorts and ranks the available resources increasingly by free space for jobs and tracking each resource's status.

In Fig. 2, the IoT devices send a set of tasks  $T = \{t_1, \dots, t_m\}$  continuously to the fog layer. The FNAMM model receives the sent tasks to be executed in the fog nodes or cloud side. Initially, the model scans the network for discovering a set of resources  $N = \{n_1, \dots, n_m\}$  sort the incoming tasks by their accompanied priorities. Each fog area includes one master fog node (MFN) and many fog nodes (FNs) attached to the master fog node. The master node receives a series of tasks  $\langle M, P, R \rangle$ , where M is the task type mobile agent or not. The mobile agent will be forwarded to the cloud server, and not the mobile agent will be executed in local fog resource. The P defines the task priority, and R indicates the fog resources' availability in that area. If the task cannot be executed in this area, the master node will migrate the task to execute in the neighbour fog area instead of sending it to the cloud server and so on. This will reduce the delay by implementing the task as locally as possible.

#### A. Optimized fog Topology Job Scheduling (OFTJS)

This section proposes an optimized fog topology job scheduling (OFTJS) algorithm proposed in our solution in [40]. Most fog computing systems use the FCFS algorithm, which executes one job at a time. This strategy is not efficient when the system is dealing with a massive number of jobs. Moreover, the job priority is not considered in this strategy as well.

Suppose the system topology consists of 6 main areas, and each area has 10 fog resource nodes. So, we have 60 fog resources that can execute the job in a fog computing network. When any nodes in the system cannot accept any more jobs, they would be migrated to the cloud side. In the proposed approach, we add a job pool between the incoming jobs and the system. The model's size is L, which is the number of jobs to be executed in the system, as shown in Fig. 1.

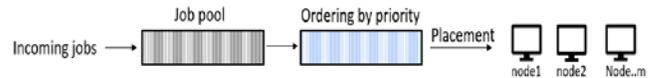


Fig. 1. Job Scheduling Process.

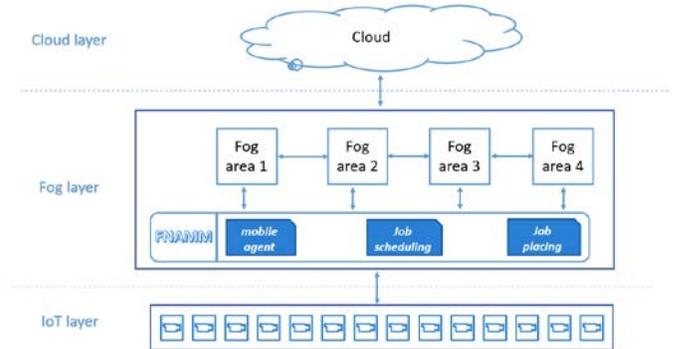


Fig. 2. High-Level Architecture for the Proposed Model.

Once the scheduling process starts, all the jobs would be placed into the job pool and allocated to the fog system's appropriate nodes. Also, the devices in the system would be scanned in each periodical scheduling cycle. The purpose of the scanning technique is to detect all available resources and their capabilities in the system. After determining the free and suitable resources in the system, we acquire a set of waiting jobs in the job pool ordered by the priority, as shown in Fig. 3.

The applications in IoT/fog computing environment have their requirements and characteristic. The end-user sends tasks to the fog layer to being executed then achieving the result. However, sorting the tasks in a queue is different from one application to another one. For instance, an eHealth application will give the tasks high priority if the patient has a high blood pressure to execute early. The priority mechanism is based on the task's type. In other words, each task has a deadline to be completed depending on the application requirements, as shown in Fig. 5. Based on the application requirement, we suggest a priority scheduling for the incoming tasks according to two factors:

- 1) The task would reach its threshold so that it will be considered a high priority.
- 2) The task has already been assigned as a high priority through the application requirement.

**Algorithm1: optimized fog topology job scheduling (OFTJS)**

```
1. If scheduling cycle s is launched then  
2. scan the fog system and discover the set N of M free resources:  $N = \{n_1, \dots, n_M\}$   
3. gather the set t of T from job pool:  $T = \{t_1, \dots, t_m\}$   
4. if task_type( $t_i$ ) == mobile_agent then  
    initates_mobile_agent_toCloud( $t_i$ )  
    else  
        Job Placement (J , N)  $\rightarrow$  Algorithm 2  
7. If all the tasks in T are executed then  
    terminate the scheduling cycle s+1  
    else if  $t_i \in T$  is rejected then  
        if service_not_aval( $t_i$ ) == true then  
            migrate_to_cloud( $t_i$ )  
            terminate the scheduling cycle s+1  
        else  
            reserve space in job pool
```

Fig. 3. Job Scheduling Algorithm.

**Algorithm2: job placement**

```
Input: i) the set N of M nodes:  $N = \{n_1, n_2, \dots, n_m\}$   
      ii) the set t of T waiting jobs in the task-pool:  $T = \{t_1, t_2, \dots, t_m\}$   
1. sort and rank each  $n_i$  increasingly by free space for tasks  
2. PR = priority_assign(t)  $\rightarrow$  Algorithm 3  
3. if PRi == H then  
    place  $t_i$  in TPH // high task pool  
    else  
        place  $t_i$  in TPN // normal task pool  
4. for each task  $\in TP^H$  DO // high task pool placement  
5. scan the system to obtain updated set N of free fog nodes  
6. if  $n_i$  has more space for TPHi then  
    return placing TPHi in  $n_i$   
    else  
        continue  
7. for each task  $\in TP^N$  DO // normal task pool placement  
8. scan the system to obtain updated set N of free fog nodes  
9. if  $n_i$  has more space for TPNi then  
    return placing TPNi in  $n_i$   
    else  
        continue
```

Fig. 4. Job Placement Algorithm.

**B. Job Placement**

The job placement algorithm plays a significant role in reducing the power consumption and the response time by placing the task close to the IoT device. Moreover, selecting the task to be executed early is essential for achieving the (QoS) and (SLA). In our job placement algorithm, it receives the tasks and the available and suitable resources. The first step is to sort the resources increasingly by free space to execute a task. Secondly, the priority function assigns priority for each task, as explained in the previous paragraph. Thirdly, if the task is assigned as a high priority, it will be placed in the high task pool; otherwise, it will be placed in the normal task pool, as shown in Fig. 4.

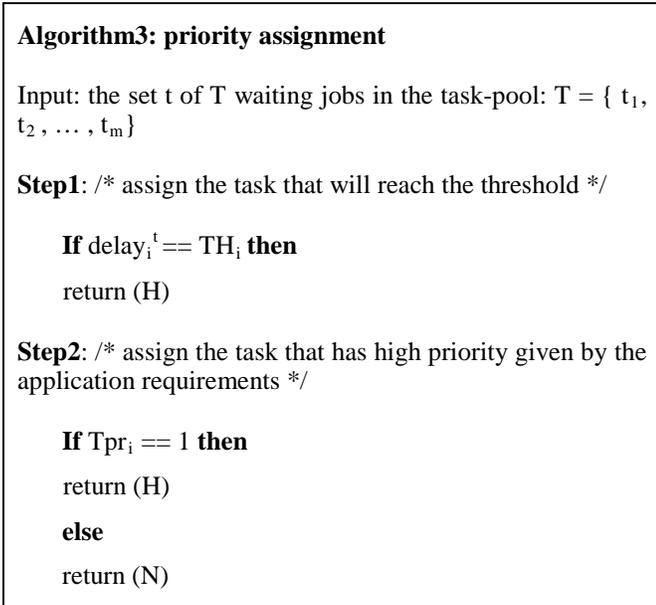


Fig. 5. Task Priority Assignment Algorithm.

C. Mobile Agent Software Technology

Once the job scheduling, as mentioned in the previous section, determines the task as a mobile agent software, the task will be considered as a mobile IoT agent. When the mobile IoT agent is launched, the discovery manager requests the cloud service pool to provide a set of available virtual machines in the cloud layer, high speed, and high processing power devices. Moreover, it determines the required service from the caller/IoT. Finally, the discovery manager generates an action plan including routing decisions for the mobile IoT agent, as shown in Fig. 6 and Fig. 7.

Upon the fog layer's migration to the cloud layer, the execution and data transmission paths select the same bridge. If the connection between the fog and the cloud is interrupted, the mobile IoT agent may remain on the cloud side till the caller reconnects to achieve the result.

The model consists of three main components as follows:

- **Discovery manager:** this agent aims to provide the available Virtual Machines in the cloud server and calculates the bandwidth between the caller/IoT and the VM host; as a result, the execution time would be minimized. This method can be achieved by sending a request to the cloud service pool to provide the available VMs in the cloud server.
- **Cloud service pool:** the cloud service pool is a database that continuously provides VMs hosts that implement the mobile IoT agent. All VMs hosts' specifications are provided by this database, such as CPU speed and cores number, storage size, and current capacity.
- **Cloud VMs:** these machines are available in the cloud layer for executing the incoming mobile IoT agent's task. In this case, the service is provided as platform as a service (PaaS) from the cloud server.

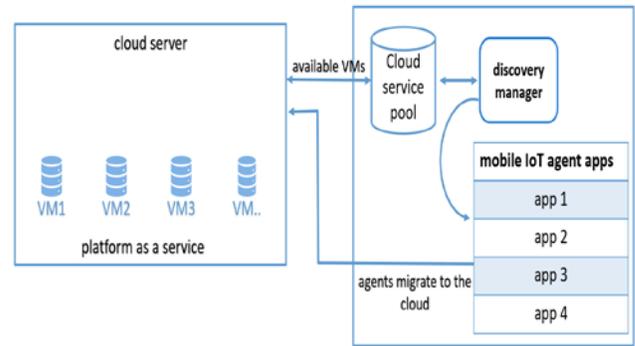


Fig. 6. Mobile Agent Architecture.

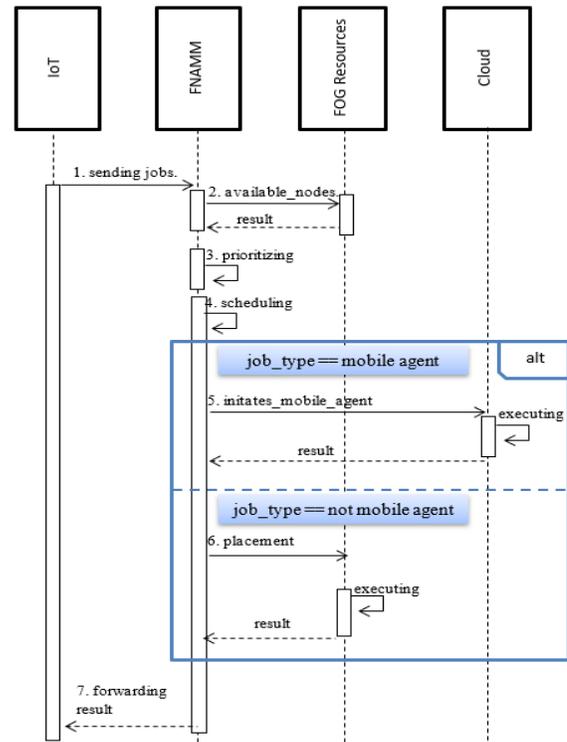


Fig. 7. FNAMM Sequence Diagram.

IV. DISCUSSION

The proposed solution's effectiveness compared to [25] and [38] architectures deals with high efficiency when dealing with big data in the cloud. In the proposed solution, we used a mobile agent to reduce the volume of data that is transferred between the end-user and the cloud server, which also contributed to reducing the cost of the network as well. As for the fog network, our task scheduling tries as much as possible to implement tasks locally, near the end-user. On both [25] and [38], when the device cannot perform the tasks, it sends it north towards the cloud server. While in the proposed solution, we try to implement the tasks in devices that are adjacent to this device, taking into account both the left and right directions. Finally, the proposed model differs from the compared architectures in that the task priority collaborates in our solution. Each IoT applications have their requirements that can affect the task priority. So, depending on the

REFERENCES

application requirements, the proposed task scheduling algorithm will regard these requirements in sorting the task in the queue.

Most of the recent architectures have not considered a massive amount of process in fog computing networks. When we compare it with other architectures, the proposed architecture's significant feature is considering the data velocity in the IoT environment. We can optimize the performance and scalability by building an efficient resource management model. Creating a repository that contains all available resources/service and their capability in the fog network can enhance task scheduling and load balancing. Also, the metadata in the repository can indicate the data locality and then decide if it would be implemented in the fog network or must be migrated to the cloud side in early stage.

The strength of this architecture can be demonstrated in the next point:

- **Dynamic:** the architecture supports the collaboration between the resources to scale the dynamic changes in the network. Also, the collaboration between the networks is dynamic, which can enhance the join process.
- **Saving energy:** since the architecture focuses on utilizing all the resources in the networks, the transferred process to the central cloud would be reduced.
- **Response Time:** the architecture determines the short path between the resource and the destination, leading to reduced latency, also, by early determining, on the distribution task phase, if the job would be executed in the fog resource or on the cloud server.

It is insufficient to use traditional methods when required data is transferred from the cloud servers to the user or IoT devices. In some cases, unused data is transmitted; thus, there is a waste of energy and delays in responding to demands. From this challenge, mobile agent technology which does analysis or processing on the cloud side, then transmits target data in a small amount to the end-user.

V. CONCLUSION AND FUTURE WORK

IoT applications generate massive tasks that need to be served adequately and received a fast-responding. Fog computing is proposed to accommodate the cloud server by providing the service close to IoT devices. However, many fog computing architectures are insufficient to utilize all available resources. A holistic fog-based resource management model is proposed to overcome the mentioned issue by building an efficient job scheduling and deploy the job to appropriate available resources considering capabilities. Our proposed model's benefits can be summarised in making a reduction in response time, network cost, and power consumption. These metrics play a significant factor in optimizing the performance of IoT applications. The future work is to implement this model in a simulation work or a real-time environment. Moreover, the mobility of IoT devices is not considered in our solution, which can be investigated in further research.

- [1] K. Kambatla, "Trends in big data analytics", *J. Parallel Distrib. Comput.*, vol. 74, no. 7, pp. 2561-2573, 2014.
- [2] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli, "Fog computing and its role in the internet of things", *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pp. 13-16, 2012.
- [3] Mckinsey Global Institute website "The Internet of Things: Mapping The Value Beyond The Hype". Accessed Jan. 10, 2021. [Online]. Available: <https://www.mckinsey.com>.
- [4] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, "Fog computing: Principles, architectures, and applications," in *Internet of Things*, Elsevier, ch.4, pp. 61-75, 2016.
- [5] J. Noymanee, W. San-Um, Theeramunkong, "T. A Conceptual Framework for the Design of an Urban Flood Early-Warning System Using a Context-Awareness Approach in Internet-of-Things Platform", In: Kim K., Joukov N. (eds) *Information Science and Applications (ICISA) 2016*.
- [6] P. Hu, H. Ning, T. Qiu, Y. Zhang, X. Luo, "Fog computing based face identification and resolution scheme in Internet of Things", *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1910-1920, Aug. 2017.
- [7] I. Gudymenko, K. Borcea-Pfitzmann, & K. Tietze, "Privacy implications of the Internet of Things", in *International Joint Conference on Ambient Intelligence*, Springer Berlin Heidelberg, pp. 280-286, 2011.
- [8] M. Aazam, S. Zeadally, K. A. Harras, "Fog Computing Architecture Evaluation and Future Research Directions", in *IEEE Communications Magazine*, vol. 56, no. 5, pp. 46-52, 2018.
- [9] O. Kwon and N. B. L. Shin, "Data quality management, data usage experience and acquisition intention of big data analytics", *Int. J. Inf. Manage.*, vol. 34, no. 3, pp. 387-394, 2014.
- [10] M. Marjani et al., "Big IoT data analytics: Architecture opportunities and open research challenges", *IEEE Access*, vol. 5, pp. 5247-5261, 2017.
- [11] K. Peng, R. Lin, B. Huang, H. Zou, and F. Yang, "Link importance evaluation of data center network based on maximum flow," *Journal of Internet Technology*, vol.18, no.1, pp.23-31, 2017.
- [12] X. Xu, X. Zhang, M. Khan, W. Dou, S. Xue, S. Yu, "A balanced virtual machine scheduling method for energy-performance trade-offs in cyber-physical cloud systems", *Future Generation Computer Systems*, 2017.
- [13] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and Opportunities in Edge Computing", in *IEEE International Conference on Smart Cloud*, pp. 20-26, 2016.
- [14] B. Varghese, N. Wang, J. Li, and D. Nikolopoulos, "Edge-as-a-Service: Towards Distributed Cloud Architectures", in *International Conference on Parallel Computing*, ser. *Advances in Parallel Computing*. IOS Press, pp. 784-793, 2017.
- [15] E. Saurez, K. Hong, D. Lillethun, U. Ramachandran, and B. Ottenwalder, "Incremental Deployment and Migration of Geo-distributed Situation Awareness Applications in the Fog", in *Proceedings of the 10th ACM International Conference on Distributed and Event-based Systems*, pp. 258-269, 2016.
- [16] R. Kolcun, D. Boyle, and J. A. McCann, "Optimal processing node discovery algorithm for distributed computing in IoT", in *5th International Conference on the Internet of Things*, pp. 72-79, 2015.
- [17] Xu, X.; Fu, S.; Cai, Q.; Tian, W.; Liu, W.; Dou, W.; Sun, X.; Liu, A.X., "Dynamic Resource Allocation for Load Balancing in Fog Environment", *Wirel. Commun. Mob. Comput.*, 2018.
- [18] W. Tarneberg, A. Mehta, E. Wadbro, J. Tordsson, J. Eker, M. Kihl, E. Elmroth, "Dynamic application placement in the mobile cloud network", *Future Generation Computer Systems*, vol. 70, pp. 163-177, 2017.
- [19] R.-I. Ciobanu, C. Negru, F. Pop, C. Dobre, C. X. Mavromoustakis, G. Mastorakis, "Drop computing: Ad-hoc dynamic collaborative computing", *Future Gener. Comput. Syst.*, vol. 92, pp. 889-899, Mar. 2017.
- [20] C. Fricker, F. Guillemin, P. Robert, and G. Thompson, "Analysis of an offloading scheme for data centers in the framework of fog computing",

- ACM Trans. Model. Perform. Eval. Comput. Syst., vol. 1, no. 4, p. 16, 2016.
- [21] X. Guo, R. Singh, T. Zhao, Z. Niu, "An index based task assignment policy for achieving optimal power-delay tradeoff in edge cloud systems", Proc. IEEE Int. Conf. Commun. (ICC), pp. 1-7, May 2016.
- [22] S. Ningning, G. Chao, A. Xingshuo and Z. Qiang, "Fog computing dynamic load balancing mechanism based on graph repartitioning", in China Communications, vol. 13, no. 3, pp. 156-164, Mar. 2016.
- [23] Po-Huei Liang and Jiann-Min Yang, "Evaluation of two level global load balancing framework in Cloud Environment", International Journal of Computer Science and Information Technology (IJCSIT), Vol. 7 No 2, Apr. 2015.
- [24] R. Beraldi, A. Mtibaa, and H. Alnuweiri, "Cooperative Load Balancing Scheme for Edge Computing Resources", in 2nd International Conference on Fog and Mobile Edge Computing. IEEE, pp. 94-100, 2017.
- [25] V. B. C. Souza, W. Ramirez, X. Masip-Bruin, E. Marin-Tordera, G. Ren, and G. Tashakor, "Handling service allocation in combined fog-cloud scenarios," Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumpur, Malaysia, pp. 1-5, 2016.
- [26] F. Faticanti, F. De Pellegrini, D. Siracusa, D. Santoro, and S. Cretti. "Cutting Throughput on the Edge: App-Aware Placement in Fog Computing". Proc. 6th IEEE Int. Conf. (CSCloud), pp. 196-203, 2019.
- [27] R. Deng, R. Lu, C. Lai, T. H. Luan, and H. Liang, "Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption," IEEE Internet Things J., vol. 3, no. 6, pp. 1171-1181, Dec. 2016.
- [28] O. Skarlat, S. Schulte, M. Borkowski, and P. Leitner, "Resource provisioning for IoT services in the fog," in Proc. IEEE 9th Int. Conf. ServiceOriented Comput. Appl. (SOCA), pp. 32-39, Nov. 2016.
- [29] K. Intharawijitr, K. Iida, and H. Koga, "Analysis of fog model considering computing and communication latency in 5G cellular networks," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), Sydney, NSW, Australia, pp. 1-4, 2016.
- [30] I. Lera, C. Guerrero, and C. Juiz, "Comparing centrality indices for network usage optimization of data placement policies in fog devices," in Proc. 3rd Int. Conf. Fog Mobile Edge Comput. (FMEEC), vol. 1, no. 1, pp. 115-122, Apr. 2018.
- [31] S. Agarwal, S. Yadav, and A. K. Yadav, "An efficient architecture and algorithm for resource provisioning in fog computing," Int. J. Inf. Eng. Electron. Bus., vol. 8, no. 1, pp. 48-61, 2016.
- [32] A. A. Alsaffar, H. P. Pham, C.-S. Hong, E.-N. Huh, M. Aazam, "An architecture of IoT service delegation and resource allocation based on collaboration between fog and cloud computing", Mobile Inf. Syst., vol. 2016, Aug. 2016.
- [33] T. Ouyang, Z. Zhou, and X. Chen, "Follow me at the edge: Mobility-aware dynamic service placement for mobile edge computing," IEEE J. Sel. Areas Commun., vol. 36, no. 10, pp. 2333-2345, Oct. 2018.
- [34] M. Chen, W. Li, G. Fortino, Y. Hao, L. Hu, and I. Humar. (Aug. 2018). "A dynamic service-migration mechanism in edge cognitive computing." [Online]. Available: <https://arxiv.org/abs/1808.07198>.
- [35] A. Ascigil et al., "On uncoordinated service placement in edge-clouds", Proc. IEEE CloudCom, pp. 41-48, 2017.
- [36] A. Yousefpour, A. Patil, G. Ishigaki, I. Kim, X. Wang, H. C. Cankaya, Q. Zhang, W. Xie, J. P. Jue, "FOGPLAN: A lightweight QoS-aware dynamic fog service provisioning framework", IEEE Internet Things J., vol. 6, pp. 5080-5096, Jun. 2019.
- [37] R. Urgaonkar, S. Wang, T. He, M. Zafer, K. Chan, K. K. Leung, "Dynamic service migration and workload scheduling in edge-clouds", Perform. Eval., vol. 91, pp. 205-228, Sep. 2015.
- [38] J. Wang, J. Pan, and F. Esposito, "Elastic urban video surveillance system using edge computing," in Proceedings of the Workshop on Smart Internet of Things, ser. SmartIoT '17. New York, NY, USA, pp. 7:1-7:6, 2017.
- [39] B. H. Malik, M. N. Ali, S. Yousaf, M. Mehmood, H. Saleem, "Efficient Energy Utilization in Cloud Fog Environment," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 10, No. 4, 2019.
- [40] A. Alghamdi, A. Alzahrani, V. Thayananthan, "Execution Time And Power Consumption Optimization In Fog Computing Environment," International Journal of Computer Science and Network Security (IJCSNS), Vol. 21 No. 1 pp. 137-142, 2021.

# Automata-based Algorithm for Multiple Word Matching

Majed AbuSafiya

Software Engineering Department  
Al-Ahliyya Amman University, Amman, Jordan

**Abstract**—In this paper, an automata-based algorithm that finds the valid shifts of a given set of words  $W$  in text  $T$  is presented. Unlike known string matching algorithms, a preprocessing phase is applied to  $T$  and not to the words being searched for. In this phase, a deterministic finite state automaton (DFA) that recognizes the words in  $T$  is built and is augmented with their shifts in  $T$ . The preprocessing phase is relatively expensive in terms of time and space. However, it needs to be done once for any number of words to match in a given text document. The algorithm is analyzed for complexity, implemented and compared with an adjusted version of KMP algorithm. It showed better performance than KMP algorithm for large number of words to match in  $T$ .

**Keywords**—Algorithms; finite state automata; word matching; KMP

## I. INTRODUCTION

In this paper, a special case of string matching [1] problem is considered that is called *multiple word matching*. Its input is a set of words  $W$  to match in a text string  $T$  of length  $n$ . Its output is a vector of the valid shifts of each word of  $W$  in  $T$ . The motivation for this research is that it is common to have a text document that need to be repeatedly searched for single words. Another motivation is the speed illustrated by the proposed algorithm to solve this problem compared with other matching algorithms for large  $|W|$ .

The proposed solution is based on a preprocessing phase that is applied on  $T$  not on the words to search for. The idea is based on scanning the words in  $T$  and incrementally building a deterministic finite automaton (DFA) [2] that recognizes only the words of  $T$ . Once created, the DFA is used to search for a set of words  $W$  (repetition of words in  $W$  is allowed). Although building this DFA is time consuming, it is needed to be built only once for searching any number of words in  $T$ . The search time for the individual words will be  $O(m \times |\Sigma|)$  where  $m$  is the length of the word searched for and  $|\Sigma|$  is the size of the alphabet. This means that search time will be independent of the length of  $T$ . The algorithm does better than other matching algorithms only in case of a large number of word searches in  $T$  is needed.

This paper is organized as follows: Section 2 introduces related work. Section 3 presents the proposed algorithm. Section 4 gives a rough complexity analysis of the proposed algorithm. Section 5 shows the experimental study that was conducted to compare the proposed algorithm with KMP string matching algorithm that is adjusted for multiple search words. The paper ends up with a conclusion and a list of references.

## II. RELATED WORK

String matching algorithms are well-known class of algorithms that have two inputs: a string to search in of length  $n$  called  $T$ , and a pattern string to search for of length  $m$  called  $P$ . Their output is the valid shifts of  $P$  in  $T$ . The simplest and the most expensive among these algorithms – with complexity  $O(m \times n)$  is the Naïve string matching algorithm [1]. In this algorithm,  $P$  is compared with every sub-string in  $T$  of length  $m$ . Many string matching algorithms with better efficiency were invented such as Boyer-Moore[3], Knuth-Morris-Pratt[4], Karp-Rabin [5], Horspool [6], Quick search [7], Shift-Or [8], Raita [9], Berry-Ravendran [10]. Knuth-Morris-Pratt (KMP) algorithm is widely known and proven to be a very efficient and generic. Its complexity is  $O(n)$  for small  $m$ . It requires computing a prefix-function on  $P$ , which costs  $O(m)$ , prior matching against  $T$ . A strong relation between string matching and the theory of finite automata exists, and this was discussed in detail in [11]. A very close work related to our work is the work of Aho-Corasick [12]. Their algorithm searches for a set of words in  $T$  by constructing a finite state automaton to recognize these words. This finite state automaton is then used to find the occurrences of these words in  $T$ . The main difference between our work and theirs is that in our algorithm, a finite automaton to recognize the words of  $T$  and not the words to search for is constructed. This means that Aho-Corasick approach will require  $O(n)$  string matching complexity, and our approach will have  $O(|W| \times m)$  where  $|W|$  is the number of words to search for and  $m$  is the length of words which is known to be short compared to  $n$  in the context of natural languages text. However, our algorithm pays for this shorter search time, by a pre-processing phase that takes longer time. This is because constructing a finite state automaton for  $T$  takes longer time. On the other hand, Aho-Corasick algorithm constructs the finite state machine for the words to search for, which is usually much smaller than the set of words of  $T$ .

The difference between our algorithm and other string matching algorithms can be summarized in two points: (1) Ours matches single words. So,  $m$  for our problem is relatively short. This means that our algorithm is less generic than other string matching algorithms where a pattern could be a sub-word or multiple words. (2) Ours is directed to solve the multiple word matching problem. The input is a set of words for each to be matched in  $T$ . One run of our algorithm will serve multiple search requests. Other string matching algorithms serve a search for one pattern in a single run. However, these string matching algorithms can be simply adjusted to solve the

multiple word matching problem by repeatedly applying them on a set of words on the same T.

KMP algorithm was chosen to evaluate the performance of our proposed algorithm. This algorithm is among the best and most generic known string matching algorithms. KMP is adjusted slightly to do multiple word search and hence can be used to study the performance of our algorithm. Through this comparison, the circumstances where the proposed algorithm out-performs other string matching algorithms is explored.

### III. PROPOSED ALGORITHM

MULTIPLE-WORD-MATCHING algorithm is shown in (Fig. 1). The input of the algorithm is a text to search  $T$  in and a set of words  $W$  to search for. The multiple searches for words in  $T$  is passed as an input to the algorithm. However, our algorithm may also be applied in the context where repeated search requests (for words in  $T$ ) successively arrive in the same session. A *word* is to be a sequence of characters that does not contain spaces nor white characters. It is the same known concept of “word” in the context of natural languages. Our algorithm will only match single words in  $T$ . So, patterns that are sub-words or multiple words will not be matched by our algorithm. For example, if  $T=\langle abc\ abd \rangle$ , our algorithm will assume that the only words existing in  $T$  are  $abc$  and  $abd$ . It will assume the strings “ $ab$ ” and “ $abc\ abd$ ” do not exist in  $T$ . This assumption is considered for simplicity. The output of the algorithm will be a vector of the valid shifts (in  $T$ ) for each  $w$  in  $W$ . The first step is to build a DFA that recognizes the words of  $T$ . Then, GET-SHIFTS(DFA, $w$ ) is called for every  $w$  in  $W$  and the valid shifts are returned. It is assumed that a  $w$  has an attribute called *shiftVector* that will be set by the shift vector that is returned by GET-SHIFTS(DFA, $w$ ).

The algorithm for BUILD-DFA( $T$ ) is shown in Fig. 2. In this algorithm, the DFA is initialized where the start state is created and its name field is set to the empty string. Each state  $s$  in the DFA will be augmented with a name field which corresponds to the string that takes the DFA from the start state to this state  $s$ . The loop will get the words of  $T$  one at a time and then add them to the DFA along with their shifts in  $T$ . ADD-TO-DFA will be called once for every word in  $T$ . The shift variable is updated to contain the shift of the next word by adding the shift of the current word, its length plus 1. For simplicity,  $T$  is assumed to be normalized. This means that  $T$  contains only words and these words are separated by single spaces. Additional processing may be needed to do this normalization. This assumption eases the calculation of the shifts of the words in  $T$ .

ADD-TO-DFA algorithm (Fig. 3) will set the currentState to be start state of the DFA. The loop gets the letters of the word, one at a time. In each iteration, the nextLetter of the word is taken. A transition with nextLetter from the currentState is checked. If no such transition was found, nextState will be null. This requires that a new state (is called nextState) to be created with a transition from the currentState to nextState and is labeled with nextLetter. The name field of the nextState will be set to be the concatenation of name field of the currentState with the nextLetter. The currentState is set to be the nextState. This should be done in each iteration, whether if nextState was created or found. Once the loop

terminates, all the letters of the word are consumed. The algorithm will set the current State to be a final state and shift is added to the shift vector of this final state. Note that only the final states are augmented with shifts vector. This is because augmenting all the states with shift vectors will result in too large shift vectors, especially for these states that are shallow in the DFA.

To illustrate this algorithm with an example (Fig. 4), assume that  $T=\langle ab\ ac\ a \rangle$ . Adding the word  $ab$  to the DFA will be done by calling ADD-TO-DFA(“ $ab$ ”, 0). The name field is shown for all states. For example,  $s_2.name$  is the word  $ab$  which corresponds to the prefix of the word  $ab$  that takes the DFA from the start state  $s_0$  to  $s_2$ . The name field of the start state ( $s_0$ ) is the empty string. Only  $s_2$  has the attribute shiftVector since it is a final state. Final states are distinguished with a different color.

The next call will be ADD-TO-DFA(“ $ac$ ”, 3) because the next word in  $T$  is  $ac$  with shift equals 3. The currentState is set to  $s_0$ . The word length is 2. So the loop will iterate twice. In the first iteration, nextLetter will be the letter ‘ $a$ ’. The algorithm finds a transition from  $s_0$  with ‘ $a$ ’. A nextState is found which is  $s_1$ . The currentState becomes  $s_1$ . In the second iteration, no transition from  $s_1$  with letter ‘ $c$ ’ is found. So, a new state is created which is  $s_3$ . When the loop terminates, the  $s_3$  is set to be a final state and the shift is added to the shift vector of  $s_3$ . The DFA will be as shown in Fig. 5.

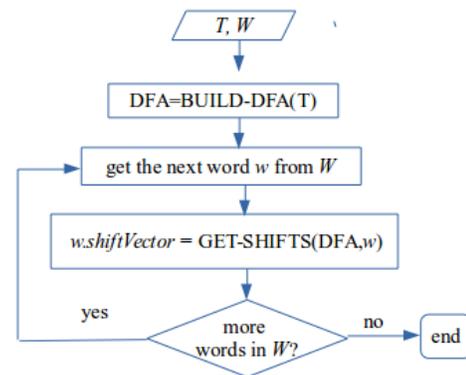


Fig. 1. Multiple-Word-Matching Algorithm.

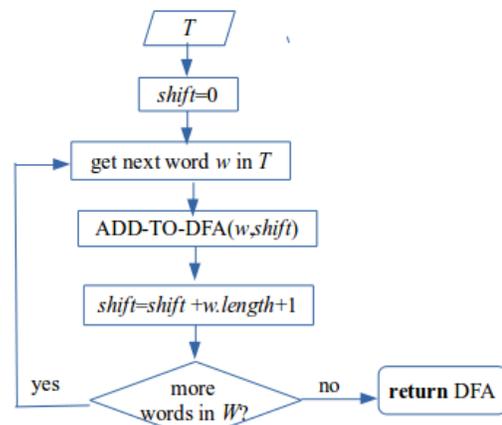


Fig. 2. BUILD-DFA Algorithm.

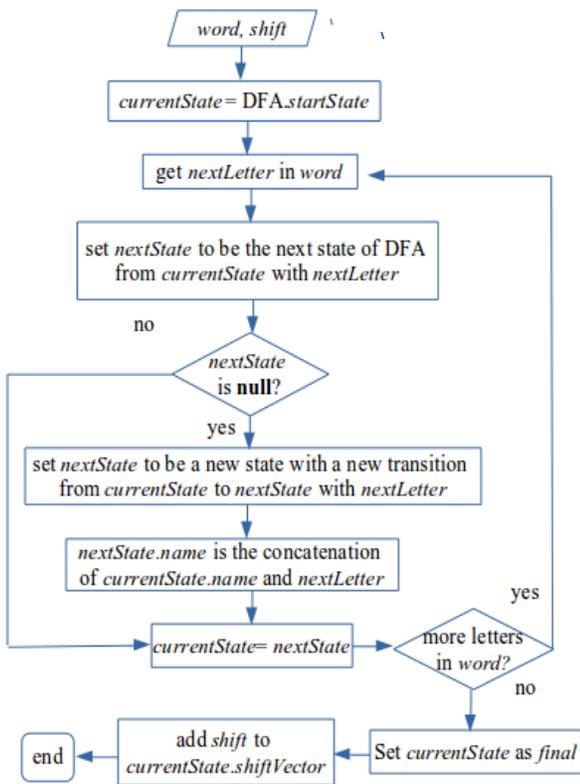


Fig. 3. ADD-TO-DFA Algorithm.

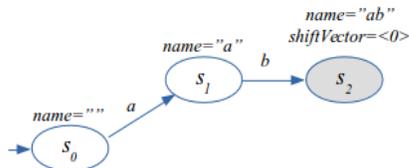


Fig. 4. DFA after ADD-TO-DFA("ab", 0) Call.

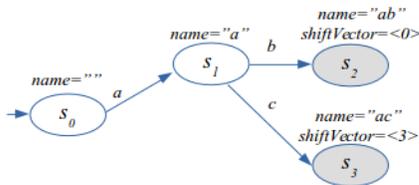


Fig. 5. DFA after ADD-TO-DFA("ac", 3).

ADD-TO-DFA will be called for the third word in  $T$  which is "a" ending with DFA in Fig. 6. Note that  $s_1$  became a final state and a shift vector is set.

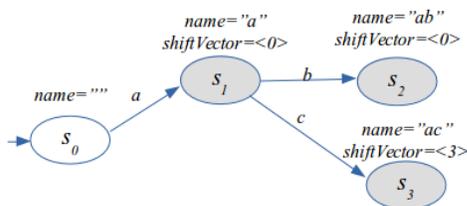


Fig. 6. DFA for  $T=<ab ac a>$ .

Next, how the DFA is used to get the shifts of a word  $w$  in  $T$  need to be defined. This is done by calling GET-SHIFTS(DFA,  $w$ ) as shown in Fig. 7. Initially, the variable  $currentState$  contains the start state. It will change to represent the state that is reached while scanning the letters of  $w$ . The letters of  $w$  are taken one by one. A check for a next state from the  $currentState$  with letter is made. If not found, this means that  $w$  does not exist in  $T$  and an empty shift vector is returned. However, if a next state is found, the  $currentState$  is updated to be the  $nextState$ . The loop will break either when (1) a null state is reached which means that  $w$  does not exist in  $T$  or (2) all the letters of the word were consumed. In case all the letters of  $w$  were consumed ending in a final state, then  $w$  is in  $T$  and the shift vector (augmented in the reached final state) is returned. An empty shifts vector is returned when (1)  $w$  could not be completely consumed because of reaching a null state, or (2) if  $w$  was completely consumed but a non-final state was reached.

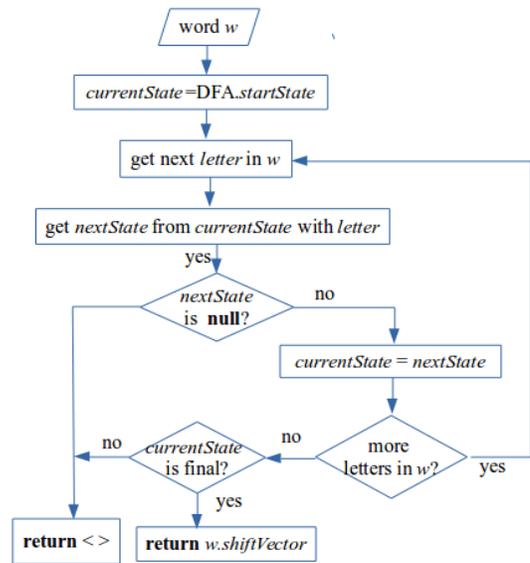


Fig. 7. Get-Shifts(DFA,  $w$ ).

For example, to search for the word "ac" in  $T$  using the DFA in Fig. 6, GET-SHIFTS(DFA, "ac") is called. The nextLetter will be "a" and next state will be found which will be  $s_1$  which is not null. This will result in another loop iteration where next letter will be "c". The next state will be  $s_3$  which is not null. The loop will break and since all  $w$ 's letters were consumed. Since the reached state ( $s_3$ ) is a final state, the shift vector will be returned which is  $\langle 3 \rangle$ .

#### IV. ANALYSIS OF THE PROPOSED ALGORITHM

To analyze the time complexity of the MULTIPLE-WORD-MATCHING algorithm, for each step, the following need to be found (1) its time complexity for a single run and (2) the number of times it's executed. These two values are multiplied and added up for all the steps. A bottom-up approach is taken, where we start analyzing the supporting algorithms and then find the complexity of the main algorithm.

Starting with ADD-TO-DFA, each statement is executed only once except for the statements within the loop which will

be run  $m$  times in worst case where  $m$  is the length of the word. All the steps take constant time to execute except for the step of finding the nextState for currentState with letter. It requires scanning the next states of the currentState to find a transition with nextLetter label. An upper bound on the number of the next states for a currentState is the size of the alphabet of the text language  $|\Sigma|$ . This is a loose upper bound, because in the words in natural languages, not all letters may appear next to a given letter. Adding the complexities of the statements, it is found that the complexity of ADD-TO-DFA algorithm is  $O(m \times |\Sigma|)$  which is constant and is independent of the size of  $T$ .

For a BUILD-DFA call, the loop will iterate a number of times equals to the number of the words in  $T$ . All the steps within the loop are of constant time complexity except for the step (ADD-TO-DFA call) which is  $O(m \times |\Sigma|)$ . The time complexity of BUILD-DFA will be  $O(n \times m \times |\Sigma|)$ . A tighter bound can be given, since the number of words multiplied by  $m$  will be roughly equal to  $n$ . That is, it can be said that the time complexity of BUILD-DFA will be  $O(n \times |\Sigma|)$ .

The statements of GET-SHIFTS will run only once, each with constant time complexity, except for the loop statements. The statements of the loop will run in the worst case  $m$  times where  $m$  is the length of the word that is searched for. The steps within the loop all take constant time expect for getting the nextState step which will take  $O(|\Sigma|)$  to search for the next state for a given letter. So the time complexity of GET-SHIFTS will be  $O(m \times |\Sigma|)$ .

Now, the main algorithm needs to be analyzed. BUILD-DFA step will run once and its complexity is  $O(n \times |\Sigma|)$ . The loop will iterate a number of times equals to the size of word set  $W$  to be searched for (i.e  $|W|$ ). GET-SHIFTS will be run  $|W|$  times with  $O(m \times |\Sigma|)$ . The total complexity of GET-SHIFTS will be  $O(|W| \times m \times |\Sigma|)$ . So the total time complexity of the main algorithm will be  $O(n \times |\Sigma|) + O(|W| \times m \times |\Sigma|)$  which will be  $O(n \times |\Sigma|) + O(|W| \times m \times |\Sigma|)$ . Since we know that the length of the words  $m$  and  $|\Sigma|$  in natural languages are relatively small constants, we can roughly say that the complexity of the MULTIPLE-WORD-MATCHING is  $O(n) + O(|W|)$  for very large  $n$  and  $|W|$ .

To compare our algorithm with KMP, it was slightly adjusted to solve our multiple word matching problem (Fig. 8).

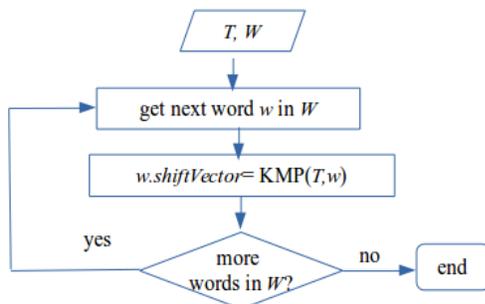


Fig. 8. Adjusted KMP.

The loop will iterate  $|W|$  times.  $KMP(T,w)$  is the same as KMP in [1] but adjusted to build a shift vector instead of printing the shifts. From [1] we know that  $KMP(T,w)$  is of

$O(n) + O(m)$  complexity. This is because,  $O(m)$  is needed to build the prefix function for  $w$  and  $O(n)$  is needed to scan  $T$  for  $w$ .  $KMP(T,w)$  will be called  $|W|$  times. So, the total complexity of the Adjusted KMP will be  $O(n \times |W|) + O(m \times |W|)$ . Knowing that  $m$  is relatively small constant in natural languages, it can be said that its complexity is  $O(n \times |W|) + O(|W|)$  which will be  $O(n \times |W|)$  for very large  $n$  and  $|W|$ .

For space complexity, our algorithm needs  $O(n)$  space. However a tighter analysis may be considered. It was found that the number of states of the DFA is linear with the set of prefixes of the words in  $T$ . Repeated words in  $T$  means less number of states. Repetition of words, is a common feature in natural language text documents. On the other hand, Adjusted KMP needs only  $O(m)$  space to store the prefix function of the current word being searched for. A comparison between MULTIPLE-WORD-MATCHING and Adjusted KMP is shown in Table I.

TABLE I. COMPARISON BETWEEN MWM AND ADJUSTED KMP

MWM	Adjusted KMP	Comparison Facet
$T$	$W$	Preprocessing phase is applied to
$O(n \times  W )$	$O(m \times  W )$	Preprocessing phase complexity for $W$
$O(m \times  W )$	$O(n)$	Search phase complexity for a single word
$O(n) + O( W )$	$O(n \times  W )$	Search phase complexity for a $ W $ words ( $ W $ large)
$O(n)$	$O(m)$	Space Complexity
large $W$	Small $W$	Better for

### V. EXPERIMENTAL STUDY

Both algorithms: MULTIPLE-WORD-MATCHING (MWM) and ADJUSTED-KMP were implemented. We chose  $T$  to be the text of the Holy Quran which is composed of 78,245 Arabic words. Fig. 9 shows the algorithm that was written to compare the two algorithms.

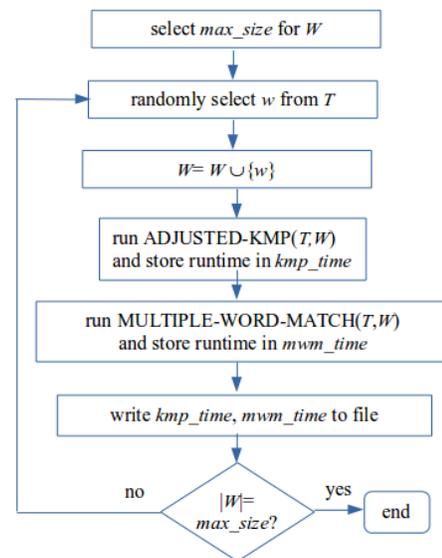


Fig. 9. Comparison Algorithm.

The comparison algorithm is based on measuring the running times for both algorithms for the growing sizes of  $W$ . Initially  $W$  is empty. The experiment was conducted by randomly selecting 200 words from the  $T$ . In each iteration, the newly selected word  $w$  is added to  $W$ . We record the start time, call the adjusted KMP algorithm for  $W$  and record the end time. The same is applied for MWM. The size of  $W$  and run time for both algorithms for this  $W$  is wrote into a file. The file is charted as shown in Fig. 10. The x-axis represents the growing  $|W|$  and the y-axis shows the run time needed by each algorithm. We have two graphs for each algorithm where a point  $(x,y)$  in any of these graphs means that searching for the  $x$  randomly selected words took  $y$  milliseconds.

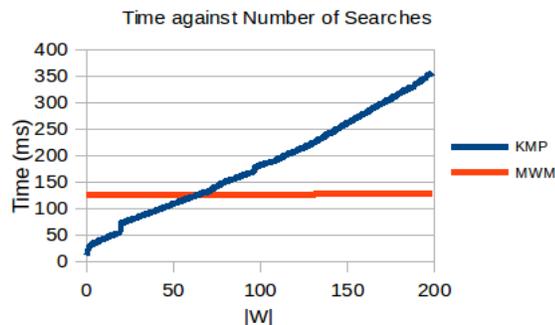


Fig. 10. Comparing MWM with Adjusted KMP.

The observations can be summarized as follows. The first search operation took too long time for MWM compared to the adjusted KMP algorithm. This is expected because of time needed to construct the DFA. However, our algorithm outperforms the adjusted KMP when  $|W|$  reaches 65 words. Although this number is not a fixed value, it gives a notion when our algorithm will out-perform the adjusted KMP for the given  $T$ . Note also that the accumulated time for MWM looks as if it is constant. However, it is increasing, but with very small value. The line has very small slope.

## VI. CONCLUSIONS

In this paper, we proposed a multiple word matching algorithm. The proposed algorithm showed competitive performance only in case of a large number of word matchings is to be applied on  $T$ . However, it is really very expensive if small number of word matchings is required on  $T$ . Preprocessing of  $T$  may open new horizons for better text search algorithms. As future work, we wish to work on optimizations on our algorithm so that it shows better performance than the adjusted KMP on lower  $|W|$ . We will relax the restriction of word matching so that the algorithm can be used to search for any pattern and not only for single words.

## REFERENCES

- [1] T. Cormen, C. Leiserson, R. Rivest, and C. Stein, Introduction to Algorithms, 3rd ed., Massachusetts: MIT Press, 2009.
- [2] J. Hopcroft, J. and Ullman, Introduction to Automata Theory, Languages and Computation, 1st ed., New York: Edison Wesley, 1979.
- [3] R. Boyer, and J. Moore, "A fast string searching algorithm," Communications of the ACM, vol. 20, pp. 762-772, 1977.
- [4] D. Knuth, J. Morris, and V. Pratt, "Fast pattern matching in strings," SIAM journal on Computing, vol. 6 No.2, pp. 323-350, 1977.
- [5] R. Karp, and M. Rabin, "Efficient randomized pattern matching algorithms," IBM journal of Research and Development, vol. 31, no. 2, pp. 249-260, 1987.
- [6] R. Horspool, "Practical fast searching in strings," Software: Practice and Experience," vol. 10 no. 6, pp. 501-506, 1980.
- [7] D. Sunday, "A very fast substring search algorithm," Communications of the ACM, vol. 33, no. 8, pp. 132-142, 1990.
- [8] R. Baeza-Yates and G. Gonnet, "A new approach to text searching," Communications of the ACM, vol. 35, no. 10, pp. 74-82, 1992.
- [9] T. Ratia, "Tuning the Boyer-Moore-Horspool string searching algorithm," Software: Practice and Experience, vol. 22, no. 10, pp. 879-884, 1992.
- [10] T. Berry, and S. Ravindran (1999), "A fast string matching algorithm and experimental results," Proceedings of the Prague Stringology Club Workshop, Prague, Czech Republic, pp. 16-28, 1999.
- [11] A. Aho, J. Hopcroft, and D. Ullman, The Design and Analysis of Computer Algorithms (1<sup>st</sup> ed.). Massachusetts: Addison Wesley. 1974.
- [12] A. Aho, and M. Corasick, "Efficient string matching: an aid to bibliographic search," Communications of the A vol. 18, no. 6, pp.333-340, 1975.

# Question Answering Systems: A Systematic Literature Review

Sarah Saad Alanazi<sup>1</sup>

Nazar Elfadil<sup>2</sup>

Department of Computer Science  
Fahad Bin Sultan University  
Tabuk, Saudi Arabia

Mutsam Jarajreh<sup>3</sup>

Computer Engineering Department  
Fahad Bin Sultan University  
Tabuk, Saudi Arabia

Saad Algarni<sup>4</sup>

Business Administration Department  
Fahad Bin Sultan University  
Tabuk, Saudi Arabia

**Abstract**—Question answering systems (QAS) are developed to answer questions presented in natural language by extracting the answer. The development of QAS is aimed at making the Web more suited to human use by eliminating the need to sift through a lot of search results manually to determine the correct answer to a question. Accordingly, the aim of this study was to provide an overview of the current state of QAS research. It also aimed at highlighting the key limitations and gaps in the existing body of knowledge relating to QAS. Furthermore, it intended to identify the most effective methods utilized in the design of QAS. The systematic review of literature research method was selected as the most appropriate methodology for studying the research topic. This method differs from the conventional literature review as it is more comprehensive and objective. Based on the findings, QAS is a highly active area of research, with scholars taking diverse approaches in the development of their systems. Some of the limitations observed in these studies encompass the focused nature of current QAS, weaknesses associated with models that are used as building blocks for QAS, the need for standard datasets and question formats hence limiting the applicability of the QAS in practical settings, and the failure of researchers to examine their QAS solutions comprehensively. The most effective methods for designing QAS include focusing on syntax and context, utilizing word encoding and knowledge systems, leveraging deep learning, and using elements such as machine learning and artificial intelligence. Going forward, modular designs ought to be encouraged to foster collaboration in the creation of QAS.

**Keywords**—Question answering systems; syntax; knowledge systems; deep learning; machine learning; systematic literature review; artificial intelligence

## I. INTRODUCTION

Information retrieval has undergone tremendous transformation in the recent past. Today, modern information access systems enable us to retrieve documents that may be linked to the input we supply the system. However, in most cases, the user is left to extract the important information from the retrieved documents. For example, the question “Who has finished a marathon race in under two hours?” Should return the answer “Eliud Kipchoge”. Instead, the user is supplied with a list of associated documents to explore and reveal the correct answer. Regardless of this limitation, Question Answering System (QAS) has been noted as an area with great potential in modern computing [3, 4, 5]. QAS allows access to information

in a very natural way, that is, by asking questions and getting related responses in natural language [9, 10, 12, 14, 41, 70].

### A. Current Research Limitations

Because of the great potential and usefulness of QAS, it will definitely be a subject to major advancement in the forthcoming years. Nonetheless, there are significant challenges that will require urgent resolving if we are to attain full potential of QAS. One of these challenges is the existing asymmetry between natural language and machine language. The asymmetry has delayed the ability of question answering systems to understand natural language-based input from users and interpret it correctly for an accurate retrieval of responses [43, 44, 45, and 46]. The language asymmetry has been a compound of several factors such as classification, construction of correct questions, ambiguity resolution, deficiencies in semantic equivalence recognition, and poor identification of sequential association in complex queries [50, 51, 52, 53, 54, 55, 56, 57, 58, 59, and 71]. Besides, there has also been a lack of accurate validation mechanism to guarantee accurateness in the responses produced by QAS (689). The unresolved nature of most of these challenges in the QAS literature is the most significant limitation of QAS research.

### B. Research Motivations

Despite the above limitation, among other challenges facing the development of perfect QAS, researchers have not given up on the quest to develop a more accurate QAS. Across all ages, human beings have always exhibited an acute thirst for information and a difference between this information and knowledge has always existed [17, 18, 19, 25, 32, 33, 35, 37, 38, 40]. Owing to this difference, consistent research has led to the maturity of modern information retrieval systems such as web searches, which allow users to access information related to their interests at their fingertips. QAS is a modern and specialized method of information access that seeks to bridge the gap between the information that users may have and the relevant knowledge. In a typical internet browsing session, an internet user is not interested in the relevant webpages that come up when making internet searches, rather, the interest is in the answers to the questions defining the searches. Bridging the gap between the questions and answers has been the main motivation of modern QAS research and the great potential of QAS makes it an exciting field to explore.

### C. Problem Statement

The working mechanism of modern question answering systems can be broken down into three broad stages, namely question analysis, document analysis, and answer analysis. The question analysis stage entails the parsing and classification of questions, as well as the development of queries that can be interpreted by the machine. The second stage of document analysis involves the extraction of documents that are relevant to the questions as interpreted by the machine and identification of suitable answers. The third stage of answer analysis involves a further breakdown of the individual documents to extract candidate answers and rank them according to their relevancy to the question.

In all the three stages, a combination of techniques from AI, NLP, statistical processing, pattern identification and matching, and information retrieval and extraction is used [2, 74, and ]. The majority of modern question answering systems incorporate most if not all the above techniques to deliver improved accuracy of results. In fact, the taxonomy of the modern QAS is derived from the techniques that forms the basis of the systems at different working stages. Such include, Linguistic-based QAS, Statistical-based QAS, and Pattern-based QAS approaches. Even the most sophisticated of these approaches has always faced the challenges of language asymmetry, among other challenges which have delayed the attainment of ultimate perfection in QASs. The desire to resolve the challenges has been a significant impetus for QAS research. A review of the literature on QAS is needed to understand the extent reached by current QAS research in resolving the outstanding challenges to the attainment of the perfect question answering system.

### D. Research Objectives

This paper provides a systematic review of the modern question answering systems' literature. The areas of interest to the paper are the current state of QAS research and identification of the most significant gaps and limitations in the reviewed studies. The three objectives of this research are broken down into three research questions.

### E. Research Questions

RQ1: What is the current state of QAS research?

RQ2: Which are the most significant gaps and limitations in the reviewed studies?

RQ3: What are the most effective techniques used in designing QAS?

### F. Summary

The remainder of the paper is organized as follows; following in the next section is a review of the recent literature on QAS then a methodology. The research methodology section emphasizes on planning, the review process, and reporting the results of systematic review. Lastly, the paper offers a conclusion relevant to the three research questions and the reviewed literature.

## II. RELATED WORKS

This section of the paper provides a review of modern studies on QAS. However, it is important to appreciate that the

development of the modern question answering systems has not been an event, but a process with a rich history. Modern studies have built on the findings of older studies to better the perfection of modern information retrieval systems. Advanced research on QAS extends back four decades ago and has grown parallel to the whole natural language processing field. Over the last four decades, hundreds of question answering systems have been developed following tremendous research efforts.

QASs are information retrieval-based tasks that process questions posed in natural language by using pre-organized databases or a large corpus of documents published in natural language. In another way, QAS accepts questions in a natural language and returns a collection of related responses in natural language. The demand for systems with this capability has been exponential owing to the growing quest for precision in the wake of increasing data and information. This has transformed it into a field with growing academic research interest from around the world.

Like any other technical field in the modern day computing, there are key terms that are related to QAS. Defining these terms will help us understand the concepts used in QAS. One of the key terms in the QAS literature is "Question Phrase", which is the section of the question that contains the search items (636). Another term is the "Question Type" which is identifies the kind of question given its purpose (636). In the QAS literature, the "Answer Type" means the classification of items that the question is seeking (636). "Question Focus" is the property related to the items of the sought by the question and "Candidate Passage" are the items identified by the search system as relevant to the search question. A candidate passage can be anything from a document or sentence in natural language that is retrieved by the search system. A "Candidate Answer" is response ranked as among the most suitable answer to the search question.

QAS literature divides the working mechanism of question answering systems into three broad modules, namely, question processing, document processing, and answer processing. As noted earlier, the question processing stage entails the parsing and classification of questions, as well as the development of queries that can be interpreted by the machine. The goal of the first stage is to identify the type, which defines the focus of the question. The focus of the question is identified by classifying as a "What", "Why", "Who", "Where" or "How" question so that the expected answer can be determined (141). This is important in bettering answer detection, which ultimately leads to acceptable accuracy of the returned answers.

The role of the document processing stage is to select a collection document that are related to the question posed by the user. The document processing stage also involve extracting few paragraphs from the selected documents that conform to the focus of the question. In modern QAS, this stage generates a dataset or a neural model which acts as the pseudocode for the process of answer extraction [13, 76, 77, and 78]. The data that is retrieved in the second stage is organized with preference inclined to those that are highly relevant to the question.

The third stage of answer processing involves a further breakdown of the individual documents to extract candidate

answers and rank them according to their relevancy to the question (5). This is often the most challenging task of the three. It involves further analysis of the document analysis stage to select the most suitable answer to the question. The complexity emanates from the need to make the answer as simple as possible even when it requires combining of information from different neural models.

### III. RESEARCH METHOD

This systematic review followed the guidelines provided eight steps, amongst which the most significant are the purpose for reviewing the literature, searching the literature, screening the literature, quality evaluation, and data abstraction. The following section outlines the stages of the systematic literature review conducted in completing the paper.

#### A. Planning the Review

The systematic review of literature started with the creation of an elaborate plan. The key components of the plan included identifying the resources required and defining the timeframes for the completion of the process. In addition to identifying the various scholarly databases, other components of the plan entailed timelines for deriving research questions from the topic, creating the search strategy, determining the search terms and strings, implementing the search strategy, selecting the most relevant studies, reviewing those studies, and writing the research paper. The detailed phases are provided in the following sections.

#### B. Specifying the Research Questions (RQS)

Over the years, we have seen an exponential expansion of digital databases that have increasingly pushed for sophisticated tools of information retrieval. With the data at hand, the challenge has always been to develop efficient techniques of consuming the data, which involves using the information we have to extract knowledge from the digital information. One of such techniques is the question answering system which allows human users to interact with computers in the most natural way as they seek answers to their questions from large corpus of unstructured data. In this review, we create three questions, as noted under section 1, subsection 4 to guide this systematic review of literature, which seeks to understand the current state of QAS research and identification of the most significant gaps and limitations in the reviewed studies.

RQ1: What is the current state of QAS research?

RQ2: Which are the most significant gaps and limitations in the reviewed studies?

RQ3: What are the most effective techniques (Method) used in designing QAS?

#### C. Defining Search Strategy

1) *Data retrieval*: The first step of the review was to index the journals and papers, including conference proceedings written and published in English. A date filter of the year of publication was limited to between 2015 and 2020. The journals and papers, including conference proceedings were pulled from five digital libraries, ACM Digital Library,

IEEE Xplore, Science Direct – Elsevier, Springer Link, and Wiley. This was achieved using a conceptual research string containing the keywords in the research questions.

2) *Screening of the journals and papers*: The choice of the papers included in this review were determined using an inclusion and exclusion criteria. The choice of the papers included in this review were determined using an inclusion and exclusion criteria to ensure that the study was explicit about the journals and papers included in the research. Only papers that met the criteria were included in the review. Table I provides more details about the inclusion and exclusion criteria used in recruiting reviewed literature.

TABLE I. INCLUSION AND EXCLUSION CRITERIA DEFINED FOR SCREENING

Inclusion Criteria	Exclusion Criteria
Only papers written and published in the English language	Non-English academic works
Academic research work published in conferences and journals	Duplicate papers existing in separate libraries
Question related to QAS, particularly those touching on the current state of QAS research and those with the potential to reveal the most significant gaps and limitations in the reviewed studies	Books, thesis, editorials among others that do not constitute published academic research
QAS studies published after January 1, 2018	Academic works published before January 1, 2018

#### D. Defining Data Sources (Eligibility of the Journals and Papers)

To ensure that only relevant papers were included in the review. The scheme involved answering quality assessment questions with a yes = 1.5, partial = 0.5, a no = 0 depending on a preliminary analysis of the individual papers. The papers that had been preselected but had a score of less than 0.5 were excluded from the review which resulted in a sample 130 papers. Purposive exclusion of 50 papers was done to remain with 80 papers.

#### E. Defining Search Keywords

The initial search words were derived from the three research questions. Additional search words were determined based on the results of the initial search. Table II highlights the main search words and offers an explanation of each one of them.

TABLE II. SEARCH KEYWORDS

QAS	Question answering systems
Syntax Knowledge systems Deep learning	Arrangement of phrases and words Collection of knowledge presented using some formal representation Artificial intelligence function that utilizes multiple layers to extract features from raw input.
Machine learning	Subset of artificial intelligence that entails utilizing statistical methods to enable machines learn automatically without explicit programming.
Artificial intelligence	Programming computers to mimic the behavior and thought of human beings.

Several search strings were developed using the search words shown in Table II and combined with Boolean operators. The utilization of Boolean operators, primarily AND and OR, was important in identifying the most appropriate studies.

### F. Conducting Review Process

The process entailed identifying records, screening them, determining their eligibility, and listing the included studies in accordance with PRISMA. Fig. 1 summarizes the search protocol.

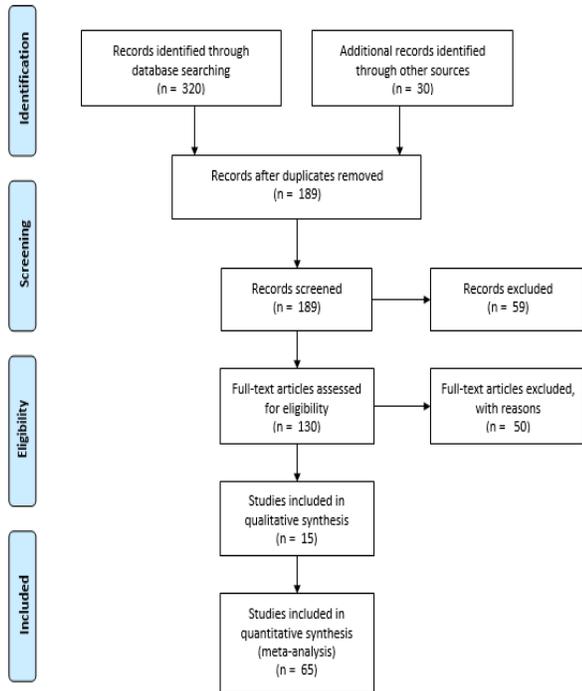


Fig. 1. Search Strategy.

### G. Selection of Study

The articles chosen for this study were determined using two-level inclusion and exclusion criteria. The identification process produced a total of 350 articles, with 320 being found through database searching whereas 30 were identified using other sources. After the exclusion of duplicates, 189 studies remained. The screening process resulted in the elimination of 59 studies. The resultant 130 studies were assessed for eligibility and 50 were excluded with reasons. Accordingly, eighty studies were included in the systematic review: 15 were qualitative whereas 65 were quantitative.

## IV. DATA SYNTHESIS

### A. Primary Studies Overview

Eighty studies formed the basis of the study: 20 on QAS based on syntax and context; 20 on QAS based on word encoding and knowledge systems; 20 based on forms of deep learning [73, 74]; and 20 based on modern components of machine learning and artificial intelligence. It was imperative to select an equal number of studies in each of the four categories to highlight the main directions in QAS research. In addition to being relevant to the research questions, the

selected studies adhered to the inclusion and exclusion criteria. This means that the selected studies were authored in English, published after January 1, 2018, and were academic research work found in scholarly journals and conferences. Out of the eighty studies surveyed, only sixty-nine were primary studies.

### B. Answering the Research Questions

This section discusses the relationship between the selected studies and the research questions. The relevant research articles extracted are utilized to answer each research question as shown in Table III.

TABLE III. STUDIES RELEVANCE TO RQs

RQ No.	No. of Studies
RQ1	69
RQ2	55
RQ3	41

This research paper conducted a systematic review of literature, rather than the conventional literature review, due to the need to attain scholarly vigor. In addition to enabling the researcher to obtain the most relevant studies, systematic reviews of literature adopt an objective perspective, which limits biases and enhances the usability of the research findings. Generally, systematic reviews of literature are implemented to summarize existing evidence in a given area, identify gaps for further investigation, and provide a framework for positioning new research activities. In this study, appropriate search terms were utilized in conjunction with various Boolean operators and search strategies to obtain studies to answer the three research questions.

The first research question (RQ1) focused on providing insights concerning the current state of QAS research. The idea is to provide the current understanding of QAS systems in terms of the approaches utilized, their effectiveness and accuracy, and potential areas of improvement. Accordingly, this study explored studies published after January 1, 2018. In total, sixty-nine studies were identified and examined to provide contemporary understanding of QAS research.

The second research question (RQ2) aimed at identifying the most significant gaps and limitations in the reviewed studies. One of the major gaps and limitations is the inability of the developed QAS systems to be utilized for a variety of tasks [1, 4, 6, 7, 15, 24, 30, 74, 75, 80, 81, 82, 83, 84, and 85]. From an ideal standpoint, a QAS system should be applicable to different questions and settings. For example, Utomo [4] developed a QAS system that can only be used with the Quran. Another critical limitation is that a typical QAS system exhibits weaknesses associated with the model or algorithm used [4, 23, 29, 31, 42, 47, 60]. For example, Jovita developed a model that required a long time to give an answer (about 29 seconds) [42]. Besides efficiency, some models are associated with poor precision. Deep learning models, in particular, require quality and large volumes of training data [47]. Thirdly, some of the QAS systems require question templates, selection of hot terms, and standard datasets, which limits their applicability in the practical environment [8, 13, 16, 20, 21, 22, 27, 28, 34, 36, 39, 48, 49, 62, 69]. Other limitations of the studies relate to the thoroughness of the assessments and explanations of the QAS

systems developed [11, 26, 40, 63, 72, 79]. For instance, Abdiansah developed a QAS system that was tested on only three search engines [11].

The final research question (RQ3) aimed at identifying the most effective techniques utilized in the design of QAS systems. Based on the search conducted, the four most effective approaches are syntax and context; word encoding and knowledge systems; forms of deep learning; and components of machine learning and artificial intelligence. Each of the four approaches was studied using 20 research articles. The syntax and context approach places questions within their context, both in terms of the semantic information carried by noun, preposition, and verb phrases and other syntactic entities, as well as the discourse roles relating to the entire question-answering activity. The word encoding and knowledge technique entails utilizing knowledge bases, in combination with question encoding at the character level or using word embedding, to answer a question. The deep learning technique encompasses multiple layers of algorithms to progressively extract high-level features from a question to enable accurate answering. Finally, some question answering systems employ diverse components of machine learning and artificial intelligence, other than deep learning, to answer questions.

## V. FINDINGS

This systematic review of literature demonstrates that the current state of QAS research is highly divergent. It appears that different scholars are setting out to develop their individual QAS systems from scratch. This trend could be explained by the fact that QAS is an emerging field. The diversity in QAS techniques means that it is almost impossible to compare them objectively. There is also an emerging trend of combining different components, which makes it difficult to evaluate the effect of each component individually. Accordingly, the adoption of a modular approach could be helpful as it would enable the scientific community to contribute by developing new plugins to improve or replace existing ones. Despite the challenges, QAS research is making positive strides towards the creation of accurate question answering systems.

The review also highlights various significant gaps and limitations in QAS research. A key limitation identified is the highly focused nature of the QAS developed. In addition, the models utilized have weaknesses, which limits the accuracy and efficiency of the entire QAS. Deep learning models, while suited to QAS applications, require vast amounts of quality training data during their development [61, 62, 63, 64, 65, 66, 67, and 68]. Without such data, their effectiveness and applicability reduce significantly. In research studies, particularly those targeting machine learning, the availability of unbiased training data is often a challenge. Moreover, some of the QAS developed only work well with standard datasets. Accordingly, when testing them, researchers are likely to obtain high accuracies. However, in practical settings, standard datasets are unavailable. Furthermore, the research methodologies adopted by the different scholars were deficient as some of the QAS developed were not evaluated comprehensively.

The design of QAS can take one of the four approaches identified. The first one encompasses examining the syntax of the question and the context in which it is placed to enable accurate answering. The second approach involves encoding words contained in the question and then utilizing knowledge bases to find the correct answer. The third method entails utilizing some forms of deep learning, which enables a progressive extraction of information from questions during the answering process. Fourthly, artificial intelligence and machine learning are routinely applied in question answering systems.

## VI. DISCUSSION

### A. Research Limitations

The findings of this study must be understood within the limitations encountered. One major weakness is that the systematic review of literature was limited to studies published in English. While this requirement was necessary to ensure that the selected studies were understandable to the author, it is possible that some helpful studies were eliminated. Another limitation is that only QAS studies published after January 1, 2018 were surveyed. This criterion might also have limited the inclusion of potentially helpful studies despite being fairly older. Besides, the systematic review of literature included studies that had different methodological weaknesses, including inadequate QAS system evaluation. Accordingly, limitations in individual studies affected the overall strength of this systematic review.

### B. Research Conclusion

The objectives of this study entailed providing a picture of the current state of QAS research, discuss gaps and limitations in the QAS research, and explore effective methods utilized in the design of QAS. The study adopted the systematic review of literature research methodology and encompassed examining relevant studies published in English after January 1, 2018. A total of eighty studies were selected for the research study. However, only 69 were relevant to the first research question, 55 were relevant to the second research question, and 41 answered the final research question. Based on the findings, QAS research literature is growing but is highly divergent as scholars adopt different techniques. The main techniques include syntax and context, word encoding and knowledge systems, deep learning [21, 28, 62, 66, 73, 83], and artificial intelligence and machine learning. Some of the significant gaps identified include ineffectiveness and inefficiencies associated with the models adopted, the highly focused nature of QAS systems developed, the reduced practicality of QAS due to the need for standard datasets or question formats, and the inability to test QAS thoroughly. Future research ought to focus on the development of QAS based on modular approaches to enhance collaboration within the scientific community. Future studies should also examine the applicability of some of the developed QAS in practical environments.

## REFERENCES

- [1] M. Al-Shanaq, K. Nahar. "Aqas: Arabic Question Answering System Based on Svm, Svd, and Lsi." *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 2, , pp. 681-91, 2019.
- [2] M. Anggraeni. "Literation Hearing Impairment (I-Chat Bot): Natural Language Processing (NLP) and Naïve Bayes Method." *Journal of*

- Physics: Conference Series, vol. 1201, no. 1, 2019. <https://doi.org/10.1088/1742-6596/1201/1/012057>.
- [3] A. Asai, K. Hashimoto, H. Hajishirzi, R. Socher, C. Xiong Asai. "Learning to Retrieve Reasoning Paths over Wikipedia Graph for Question Answering". *Proceeding of ICLR*, pp. 1-22, 2020. <http://arxiv.org/abs/1911.10470>.
- [4] A. Azmi, A. Omar, a. Hussain. "Computational and Natural Language Processing Based Studies of Hadith Literature: A Survey." *Artificial Intelligence Review*, vol. 52, no. 2, Springer, pp. 1369-414, 2019. <https://doi.org/10.1007/s10462-019-09692-w>.
- [5] A. NS, A. UTAMI. "Information Extraction from Web as Knowledge Resources for Indonesian Question Answering System". In *Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019)* (pp. 419-425), May 2020. <https://doi.org/10.2991/aisr.k.200424.064>.
- [6] A. Asma, P. Zweigenbaum. "MEANS: A medical question-answering system combining NLP techniques and semantic Web technologies". *Journal of information processing & management*, Volume 51, Issue 5, Pages 570-594, September 2015.
- [7] S. Banerjee, S. Naskar, S. Bandyopadhyay, P. Rosso. "Classifier Combination Approach for Question Classification for Bengali Question Answering System." *Sadhana - Academy Proceedings in Engineering Sciences*, vol. 44, no. 12, Springer India, 2019, doi:10.1007/s12046-019-1224-8.
- [8] R. Bakis, D. Connors, P. Dube, P. Kapanipathi, R. Kumar, D. Malioutov, & C. Venkatramani. "Performance of natural language classifiers in a question-answering system". *IBM Journal of Research and Development*, 61(4):14:1-14:10, 2017. <https://doi.org/10.1147/JRD.2017.2711719>.
- [9] P. Baudiš, J. Šedivý. "Modeling of the question answering task in the yodaqa system". In *International Conference of the Cross-Language Evaluation Forum for European Languages*. September 2015. [https://doi.org/10.1007/978-3-319-24027-5\\_20](https://doi.org/10.1007/978-3-319-24027-5_20).
- [10] A. Bhandwaldar, W. Zadrozny. "UNCC QA: biomedical question answering system". In *Proceedings of the 6th BioASQ Workshop A challenge on large-scale biomedical semantic indexing and question answering*. November 2018. <https://doi.org/10.18653/v1/W18-5308>.
- [11] C. Soares, M. Antonio, and F. Parreiras. "A on Question Answering Techniques, Paradigms and Systems." *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 6, King Saud University, pp. 635-46, 2020. <https://doi.org/10.1016/j.jksuci.2018.08.005>.
- [12] A. Chen, G. Stanovsky, S. Singh, M. Gardner "Evaluating Question Answering Evaluation". *Proceedings of the 2nd Workshop on Machine Reading for Question Answering* pp. 119-24, doi:10.18653/v1/d19-5817, 2019. <https://doi.org/10.18653/v1/d19-5817>.
- [13] C. Chen, C. Wu, C. Lo, F. Hwang. "An augmented reality question answering system based on ensemble neural networks". *IEEE Access*, August 2017. <https://doi.org/10.1109/ACCESS.2017.2743746>.
- [14] W. Cui, Y. Xiao, H. Wang, Y. Song, S. Hwang, W. Wang. "KBQA: Learning Question Answering over QA Corpora and Knowledge Bases." *Proceedings of the VLDB Endowment*, vol. 10, no. 5, pp. 565-576, 2016. doi:10.14778/3055540.3055549.
- [15] M. Dehghani, H. Azarbyonad, K. Kamps, M. Rijke. "Learning to Transform, Combine, and Reason in Open Domain Question Answering." *CEUR Workshop Proceedings*, vol. 2491, 2019. <https://doi.org/10.1145/3289600.3291012>.
- [16] D. Fushman, Y. Mrabet, A. Abacha. "Consumer Health Information and Question Answering: Helping Consumers Find Answers to Their Health-Related Information Needs." *Journal of the American Medical Informatics Association*, vol. 27, no. 2, Oxford University Press, 2020, pp. 194-201. <https://doi.org/10.1093/jamia/ocz152>.
- [17] D. Diefenbach, A. Both, K. Singh, Pierre Maret. "Towards a question answering system over the semantic web". *Semantic Web*, pp. 1-16, 2018. <https://doi.org/10.3233/SW-190343>.
- [18] E. Dimitrakis, K. Sgontzos, Y. Tzitzikas. "A Survey on Question Answering Systems over Linked Data and Documents." *Journal of Intelligent Information Systems*, vol. 55, no. 2, pp. 233-59, 2020. doi:10.1007/s10844-019-00584-7.
- [19] T. Dodiya, S. Jain. "Question classification for medical domain question answering system". In *2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*, December 2016. <https://doi.org/10.1109/WIECON-ECE.2016.8009118>.
- [20] M. Esposito, E. Damiano, A. Minutolo, G. De Pietro, H. Fujita. "Hybrid Query Expansion Using Lexical Resources and Word Embeddings for Sentence Retrieval in Question Answering." *Information Sciences*, vol. 514, Elsevier, 2020, pp. 88-105. <https://doi.org/10.1016/j.ins.2019.12.002>.
- [21] S. Gupta, N. Khade. "BERT Based Multilingual Machine Comprehension in English and Hindi". *Special Issue on Deep Learning of ACM Transactions on Asian and Low-Resource Language Information Processing (TALLIP)* no. 1, pp. 1-13, 2020.
- [22] H. Alami, N. Ennahnahi, K. Zidani. "An Arabic Question Classification Method Based on New Taxonomy and Continuous Distributed Representation of Words." *Journal of King Saud University-Computer and Information Sciences*, Elsevier, 2019.
- [23] S. Hamed, M. Ab Aziz. "A Question Answering System on Holy Quran Translation Based on Question Expansion Technique and Neural Network Classification." *Journal of Computer Science*, vol 12(3):169-177, January 2016. <https://doi.org/10.3844/jcssp.2016.169.177>.
- [24] S. Hazrina, N. Sharef, H. Ibrahim, M. AzmiMurad, S. MohdNoah. "Review on the advancements of disambiguation in semantic question answering system". *Information Processing & Management*, 2017. <https://doi.org/10.1016/j.ipm.2016.06.006>.
- [25] H. Xiao, X. Huang, J. Zhang, D. Li, P. Li. "Knowledge Graph Embedding Based Question Answering." *WSDM 2019 - Proceedings of the 12th ACM International Conference on Web Search and Data Mining*, no. Ccl, pp. 105-13, 2019. doi:10.1145/3289600.3290956.
- [26] D. Hudson, C. Manning. "GQA: A New Dataset for Real-World Visual Reasoning and Compositional Question Answering." *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. June 2019, pp. 6693-702, 2019. doi:10.1109/CVPR.2019.00686.
- [27] S. Jaya, M. Zidny, M. Gunawan. "Integrated Passage Retrieval with Fuzzy Logic for Indonesian Question Answering System." *International Journal on Perceptive and Cognitive Computing*, vol. 5, no. 2, pp. 31-34, 2019. doi:10.31436/ijpcc.v5i2.118.
- [28] K. Karpagam, K. Madusudanan, A. Saradha. "Deep Learning Approaches for Answer Selection in Question Answering System for Conversation Agents." *ICTACT Journal on Soft Computing*, vol. 10, no. 2, pp. 2040-44, 2020. doi:10.21917/ijsc.2020.0289.
- [29] Kitchenham, B. Kitchenham, O. Brereton, D. Budgen, M. Turner, J. Bailey, S. Linkman. "Systematic Literature Reviews in Software Engineering - A Systematic Literature Review." *Information and Software Technology*, vol. 51, no. 1, pp. 7-15, 2009. doi:10.1016/j.infsof.2008.09.009.
- [30] L. Kodra, K. Elinda. "Question Answering Systems: A Review on Present Developments, Challenges and Trends." *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 9, pp. 217-24, 2017. doi:10.14569/ijacsa.2017.080931.
- [31] M. Kowsher, M. Rahman, S. Ahmed, N. Prottasha. "Bangla Intelligence Question Answering System Based on Mathematics and Statistics." *2019 22nd International Conference on Computer and Information Technology (ICCIT)*, pp. 1-6, 2019. doi:10.1109/ICCIT48885.2019.9038332.
- [32] K. Krishna, M. Iyyer. "Generating Question-Answer Hierarchies." *ACL 2019 - 57th Annual Meeting of the Association for Computational Linguistics*, *Proceedings of the Conference*, pp. 2321-34, 2020. doi:10.18653/v1/p19-1224.
- [33] P. Rosso, Y. Benajiba, A. Lyhyaoui. "Towards a Passages Extraction Method for Arabic Question Answering Systems." *International Conference on Advanced Intelligent Systems for Sustainable Development*, Springer, pp. 230-37, 2019. [https://doi.org/10.1007/978-3-030-36653-7\\_23](https://doi.org/10.1007/978-3-030-36653-7_23).
- [34] G. Popek, W. Lorkiewicz. "Grounding of Modal Responses in Question Answering System Equipped with Hierarchical Categorisation." *Procedia Computer Science*, vol. 176, Elsevier B.V., pp. 3163-72, 2020. doi:10.1016/j.procs.2020.09.172.

- [35] T. Abedissa, M. Libsie. "Amharic Question Answering for Biography, Definition, and Description Questions". Information and Communication Technology for Development for Africa, vol 1026. Springer, Cham, 2019. doi.org/10.1007/978-3-030-26630-1\_26.
- [36] B. McCann, N. Keskar, C. Xiong, R. Socher. "The Natural Language Decathlon: Multitask Learning as Question Answering". 2018, <http://arxiv.org/abs/1806.08730>.
- [37] H. Mozannar, E. Maamary, K. El Hajal, H. Hajj. "Neural Arabic Question Answering". Proceedings of the Fourth Arabic Natural Language Processing Workshop, pp. 108-18, August 2019. doi:10.18653/v1/w19-4612.
- [38] G. Nanda, M. Dua and K. Singla, "A Hindi Question Answering System using Machine Learning approach". International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, India, pp. 311-314, 2016. doi: 10.1109/ICCTICT.2016.7514599.
- [39] A. B. Nassif, I. Shahin, I. Attili, M. Azzeh and K. Shaalan, "Speech Recognition Using Deep Neural Networks: A Systematic Review," in *IEEE Access*, vol. 7, pp. 19143-19165, 2019. doi: 10.1109/ACCESS.2019.2896880.
- [40] O. Bolanle, and E. Adebisi, "A Review of Question Answering Systems," *Journal of Web Engineering*, vol. 17, no. 8, pp. 717-58, 2019.
- [41] O. Chitu, and K. Schabram, "A Guide to Conducting a Systematic of Information Systems Research," *SSRN Electronic Journal*, vol. 10, pp. 1-3, 2012.
- [42] P. V. Rajaraman, and M. Prakash, "A Survey on Text Question Responsive Systems in English and Indian Languages," *International Conf. on Soft Computing and Signal Processing*, Springer, pp. 267-77, 2019.
- [43] P. Ranjan, and R. C. Balabantaray, "Question answering system for factoid-based question," *2nd International Conf. on Contemporary Computing and Informatics (IC3I)*, IEEE, 2016.
- [44] S. K. Ray, A. Ahmad, and K. Shaalan, "A Review of the State of the Art in Hindi Question Answering Systems," *Intelligent Natural Language Processing: Trends and Applications*, Springer, pp. 265-92, 2018.
- [45] A. Salunkhe, "Evolution of Techniques for Question Answering over Knowledge Base: A Survey," *International Journal of Computer Applications*, vol. 177, no. 34, pp. 9-14, 2020.
- [46] V. Sharma, N. Kulkarni, S. Pranavi, G. Bayomi, E. Nyberg and T. Mitamura, "BioAMA: Towards an End to End BioMedical Question Answering System," In *Proc. of the BioNLP 2018 workshop*, July, 2018.
- [47] Si. Shijing, W. Zheng, L. Zhou, and M. Zhang, "Sentence Similarity Computation in Question Answering Robot," *Journal of Physics: Conf. Series*, vol. 1237, no. 2, pp. 320-355, 2019.
- [48] K. Singh, S. A. Radhakrishna, and A. Both, "Why Reinvent the Wheel: Let's Build Question Answering Systems Together," *Proce. of the World Wide Web Conf., The Web Conf.*, pp. 1247-56, 2018.
- [49] K. Singh, A. Both, D. Diefenbach, S. Shekarpour, D. Cherix, and C. Lange, "Qanary-the fast track to creating a question answering system with linked data technology," In *European Semantic Web Conf.*, May, 2016.
- [50] R. A. Stein, P. A. Jaques, and J. F. Valiati, "An Analysis of Hierarchical Text Classification Using Word Embeddings," *Information Sciences*, vol. 471, pp. 216-32, 2019.
- [51] I. Thalib, and S. Indah, "A Review on Question Analysis, Document Retrieval and Answer Extraction Method in Question Answering System," *International Conf. on Smart Technology and Applications (ICoSTA)*, IEEE, pp. 1-5, 2020.
- [52] N. Tohidi, and S. Hossain, "Multi-Objective Question Answering System," *Journal of Intelligent and Fuzzy Systems*, vol. 36, no. 4, pp. 3495-3512, 2019.
- [53] F. S. Utomo, N. Suryana, and N. Azmi, "New Instances Classification Framework on Quran Ontology Applied to Question Answering System," *Telkommika (Telecommunication Computing Electronics and Control)*, Indonesian Journal of Electrical Engineering, vol. 17, no. 1, pp. 139-46, 2019.
- [54] B. Wanjawa, and L. Muchemi, "Question Answering Using Automatically Generated Semantic Networks-the Case of Swahili Questions," *IST-Africa Conference (IST-Africa)*, IEEE, pp. 1-8, 2020.
- [55] J. Yu, M. Qiu, J. Jiang, J. Huang, and S. Song, "Modelling Domain Relationships for Transfer Learning on Retrieval-Based Question Answering Systems in E-Commerce," *Proc. of the 11th ACM International Conf. on Web Search and Data Mining, WSDM*, February, no. 1, pp. 682-90, 2018.
- [56] D. Savenkov, and E. Agichtein. "Crowd-powered real-time automatic question answering system," *Fourth AAAI Conf. on Human Computation and Crowdsourcing*, pp. 189-199, 2016.
- [57] Z. Abbasiyantaeb, and S. Momtazi, "Text-based question answering from information retrieval and deep neural network perspectives: A survey," *Advanced Review*, 2020.
- [58] P. Baudiš, and J. Šedivý, "Modeling of the question answering task in the YodaQA system," *International Conf. of the Cross-Language Evaluation Forum for European Languages*, Springer, Cham, pp. 222-228, 2015.
- [59] A. Bouziane, D. Bouchiha, N. Doumi, and M. Malki, "Question answering systems: Survey and trends," *Procedia Computer Science*, vol. 73, pp. 366-375, 2015.
- [60] V. Datla, S. A. Hasan, Joey Liu, Y. Benajiba, K. Lee, A. Qadir, A. Prakash, and O. Farri, "Open Domain Real-Time Question Answering Based on Semantic and Syntactic Question Similarity," *Journal of Web Engineering (JWE)*, vol. 17, no. 8, pp. 717-758, 2016.
- [61] K. Höffner, S. Walter, E. Marx, J. Lehmann, A. N. Ngomo, and R. Usbeck, "Overcoming challenges of semantic question answering in the semantic web," *Semantic Web Journal*, pp. 1-21, 2016.
- [62] L. Tuan, T. Bui, and S. Li, "A review on deep learning techniques applied to answer selection," *Proc. of the 27th international Conf. on computational linguistics*, pp. 2132-2144, 2018.
- [63] L. Juan, C. Zhang, and Z. Niu, "Answer extraction based on merging score strategy of hot terms," *Chinese Journal of Electronics*, vol. 25, no. 4, pp. 614-620, 2016.
- [64] M. Amit, and S. K. Jain, "A survey on question answering systems with classification," *Journal of King Saud University-Computer and Information Sciences*, vol. 28, no. 3, pp. 345-361, 2016.
- [65] M. Ajitkumar, S. Khillare, and C. Namrata, "Question answering system, approaches and techniques: A review," *International Journal of Computer Applications*, vol. 141, no. 3, pp. 0975-8887, 2016.
- [66] S. Yashvardhan, and S. Gupta, "Deep learning approaches for question answering system," *Procedia Computer Science*, vol. 132, pp. 785-794, 2018.
- [67] S. Anjali, and P. K. Yadav, "A survey on question-answering system," *International Journal of Engineering and Computer Science*, vol. 6, no. 3, pp. 345-361, 2017.
- [68] S. Anbuselvan, M. Muniandy, and L. E. Heng, "Question Classification Using Statistical Approach: A Complete Review," *Journal of Theoretical & Applied Information Technology*, vol. 71, no. 3, pp. 386-395, 2015.
- [69] M. Schubotz, P. Scharpf, K. Dudhat, Y. Nagar, F. Hamborg, and B. Gipp, "Introducing A Math-Aware Question Answering System," *Journal of Information Discovery and Delivery*, vol. 46, issue 4, pp. 214-224, 2018.
- [70] F. Schulze, R. Schüler, T. Draeger, D. Dummer, A. Ernst, P. Flemming, M. Neves, "Hpi question answering system in bioasq," In *Proceedings of the Fourth BioASQ workshop*, pp. 38-44, August, 2016.
- [71] S. Shekarpour, E. Marx, A. C. N. Ngomo, and S. Aue, "Sina: Semantic interpretation of user queries for question answering on interlinked data," *Journal of Web Semantics* vol. 30, pp. 39-51, 2015.
- [72] D. Su, Y. Xu, G. I. Winata, P. Xu, H. Kim, Z. Liu, and P. Fung, "Generalizing Question Answering System with Pre-trained Language Model Fine-tuning," In *Proceedings of the 2nd Workshop on Machine Reading for Question Answering*, November, 2019.
- [73] M. Toshevskva, G. Mirceva, and M. Jovanov, "Question Answering with Deep Learning: A Survey," *16th International Conf. on Informatics and Information Technologies, CIIT*, 2019.
- [74] X. Yang, and P. Liu, "Question recommendation and answer extraction in question answering community," *International Journal of Database Theory and Application*, vol. 9, no. 1, pp. 35-44, 2016.
- [75] W. Yang, Y. Xie, A. Lin, X. Li, L. Tan, K. Xiong, and J. Lin, "End-to-end open-domain question answering with bertserini," *Proceedings of the*

- 2019 Conf.of the North American Chapter of the Association for Computational Linguistics (Demonstrations), pp.v2, 2019.
- [76] Y.Yang, W. T.Yih, and C.Meek, "Wikiqa: A challenge dataset for open-domain question answering," In Proceedings of the 2015 Conf. on empirical methods in natural language processing, Association for Computational Linguistics, pp.2013-2018, 2015.
- [77] Y. T.Yeh, and Y. N. Chen, " Qainfomax: Learning robust question answering system by mutual information maximization," Computer Science, Mathematics, 2019.
- [78] Y.Deepa, T. N. Manjunath, and R.S. Hegadi, "A Survey of Intelligent Question Answering System Using NLP and Information Retrieval Techniques," International Journal of Advanced Research in Computer and Communication Engineering vol. 5, no. 5, pp. 536-540,2016.
- [79] W.Yu, L.Wu, Y.Deng, R.Mahindru, Q.Zeng, S.Guven, and M.Jiang, "A Technical Question Answering System with Transfer Learning," In Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing, System Demonstrations, October, 2020.
- [80] A. Clementeena, and P. Sripriya, "A literature survey on question answering system in Natural Language Processing," International Journal of Engineering and Technology, vol. 7, no. 2, 2018, pp. 452-455.
- [81] A.Ansari, M.Maknojjia, and A.Shaikh, "Intelligent question answering system based on artificial neural network," IEEE International Conf. on Engineering and Technology, IEEE, Coimbatore, India,2016.
- [82] L.Jovita, A.Hartawan, and D.Suhartono, "Using vector space model in question answering system," Procedia Computer Science vol. 59, pp. 305 - 311, 2015. <https://doi.org/10.1016/j.procs.2015.07.570>.
- [83] Z. Huang et al., "Recent Trends in Deep Learning Based Open-Domain Textual Question Answering Systems," in IEEE Access, vol. 8, pp. 94341-94356, 2020. doi: 10.1109/ACCESS.2020.2988903.
- [84] R. Chakravarti, A. Ferritto, B. Iyer, L. Pan, R. Florian, S. Roukos and A. Sil. "Towards building a Robust Industry-scale Question Answering System." Proceedings of the 28<sup>th</sup> international conference on computational ligusitics: industry track, p.p. 90-101, 2020.
- [85] BB Cambazoglu, M Sanderson, F Scholer, B Croft - sigir.org. " A Review of Public Datasets in Question Answering Research". ACM SIGIR Forum. Vol. 54 No. 2. December 2020.

# Comprehensive Analysis of Flow Incorporated Neural Network based Lightweight Video Compression Architecture

Sangeeta<sup>1</sup>, Preeti Gulia<sup>2</sup>, Nasib Singh Gill<sup>3</sup>  
Department of Computer Science and Applications  
Maharshi Dayanand University, Rohtak  
India

**Abstract**—The increasing video content over the internet motivated the exploration of novel approaches in the video compression domain. Though neural network based architectures have already emerge as de-facto in the field of image compression and analytics, their application in video compression also result in promising outputs. Adaptive and efficient compression techniques are required for video transmission over varying bandwidth. Several deep learning based techniques and enhancements were proposed and experimented but they didn't exhibit full optimal behavior and are not end to end trained and optimized. In the zest of a pure and end to end trainable compression technique, a deep learning based video compression architecture has been proposed comprises of frame autoencoder, flow autoencoder and motion extension network for the reconstruction of predicted frames. The video compression network has been designed incrementally and trained with random emission steps strategy. The proposed work results in significant improvement in visual perception quality measured in SSIM and PSNR when compared to some state-of-art techniques but in trade-off with frame reconstruction time sheet.

**Keywords**—Deep learning; video compression; autoencoder; SSIM; PSNR

## I. INTRODUCTION

The growing video content over the internet motivated the researchers to look for more proficient and efficient video compression techniques. The traditional in-use video compression techniques are manually designed and optimized. In recent years, deep learning based techniques are applied in various domain-specific applications including image and video compression too. The application of deep learning in image compression resulted in satisfactory results [1-5]. These methods focused on producing the quantization based binary representation of the images exploring various techniques like transmission of a subset of the encoded representation, learning variable quantization, training multiple models etc. The enhanced implementation of recurrent approach considerably improved the performance of the compression architectures.

The expanded architectures developed for image compression extended for videos also. But the task of video compression emerged as challenging due to the inclusion of motion information. The training of neural networks emerged with motion information emerged as very challenging.

Recently, some developments have been made by the researchers to encode the video information in a trade-off with the complexity [6,7]. Though, some architecture resulted in superior performance in comparison to the traditional codecs, but with increased complexity and computation. This led to the exploration of learning based more efficient and less complex video compression methods.

The proposed method comprises of autoencoder style architecture. The architecture consists of frame compression/decompression, flow vector compression /decompression network, and finally a motion extension/frame reconstruction network. The frame and flow compression/decompression networks are composed of encoder and decoder networks. The encoder and decoder networks comprise of recurrent ConvGRU based frames with varying degrees of compression quality. The architecture has been designed and implemented incrementally. The performance analysis and ablation study reveals the significant improvement in compression quality when measured both in SSIM and PSNR with increased efficiency measured in time taken to generate a single frame, mentioned as TPF.

The work related to the proposed architecture has been described in Section 2. The detailed description of the architecture has been described in Section 3. The experimental details and results are presented in its subsequent section i.e. 3B. Section 4 presents the performance analysis of the proposed architecture with its comparative analysis. The whole work has been concluded in Section 5.

## II. RELATED WORK

The superfluous video content is taking a huge share of internet traffic [8]. The technological advancements have brought very high quality video formats and streaming of such formats over the web has brought new challenges to the compression standards. Although the in-use traditional techniques are performing well but doesn't give optimal results with the emerging new formats. Moreover, as the bandwidth is limited and varying, adaptive and highly efficient techniques are required to transmit the quality video content with minimal interruption. Discrete Cosine Transforms are mainly used in the block designed traditional techniques [9,10]. As these blocks based traditional techniques are developed incrementally, they cannot be end to end optimized.

The main focus of compression techniques is to remove redundancies and represent the frames in minimum number of bits. The reconstruction error got increased with the increment in compression rate. Initially designed video compression standards are the extended versions of image compression standards. In such techniques like motion JPEG, individual frames of the video are compressed to achieve whole compression. The exciting results in the field of deep learning based image compression attained the researchers' attention and found some of the autoencoder techniques more potent and proficient than traditional schemes [11-15]. Decreasing rate distortion error is the primary goal of these compression schemes. The use of RNNs in some image compression architectures also improved the performance [16]. RNN based architectures are more suitable for varying compression rate. Adaptive compression techniques are required to transmit the quality and uninterrupted video content over the varying bandwidth. Some variable image size compatible video compression architectures comprising of CNNs were proposed to remove spatial redundancies [11,14,17]. Entropy encoding has been used in such techniques to achieve improved compression. In addition to CNN and RNN based architectures, several different quantization and probability driven adaptive arithmetic coding based schemes were proposed and evaluated [18,19]. Such deep learning based explored techniques resulted in improved performance compared to the standard codecs.

The exciting compression quality achieved in the field of image compression using deep learning based approaches lead to exploration of their video compatible extended versions. As videos includes more redundant information, it is imperative to have rigorous approach in the expanded formats. The widely used traditional codecs like H.264 or H.265 are block designed [20]. Their recent used versions are evolved with time by extensive engineering efforts. Their incremental block based design does not support end to end optimization. Rather, each block can be optimized or extended individually. Their predictive coding is based on the continual prediction of P or B frames from I frames extracting the required information. Initially, extensions to the existing codecs were proposed based on deep learning based schemes.

Later, researchers' explored pure deep learning based end to end optimizable approaches using different architectures and strategies. Some of the video compression architectures based on image interpolation were designed [21-23]. Several flow based techniques were presented for the prediction of the frames and spatial varying data will be learned by the Convolutional kernel. For the slow and small video frames, image extrapolation has performed well in frame prediction [24-26]. The efforts put forth in the design of deep learning based architectures of DVC in [7] and adversarial video compressions in [28] are well appreciated. A number of efficient deep learning based architectures have been developed over the years but each having its own trade off. Some of them suffer from the performance trade off either with complexity or computation.. In addition to the compression

sphere, researches have also been extended to the extraction of information from compressed formats without decompressing [27]. Our research is also motivated from the same idea of designing of such compression architecture whose compressed format can also be parsed efficiently for analytics purpose.

### III. PROPOSED WORK

The proposed architecture is a neural network based scheme for video compression. A frame auto-encoder based compression network has been designed using CNN and ConvGRU units. The input frames are taken consecutively by the encoder network and presents the encoded form to the corresponding decoder. The reconstructed frames are generated by the decoder from the encoded format. The encoder and decoder networks of the frame autoencoder are trained together. A Flow Autoencoder is also incorporated to compute the optical flow. Optical Flow is used for the motion information lies between consecutive frames of a video. The Motion Extension Network is used to reconstruct the next frames using optical flow and decoded frame from frame autoencoder. The proposed system is modelled in Tensorflow.

#### A. Network Architecture

The frame autoencoder is the vital part of compression architecture. It comprises of the encoder and decoder networks comprising of CNN and ConvGRU units. The encoder encodes the frames with varying degrees of compression quality. The binary format has been quantized before passing to the decoder. The decoder regenerates the frame from the encoded format according to the degree of compression. Farneback based Flow computation has been used for the motion estimation and prediction among the consecutive frames. Flow autoencoder has been incorporated to compress the computed flow value. Motion extension network reconstructs the frames based on the current frame from the frame autoencoder, the previous frame and decoded flow value as illustrated in Fig. 2. The overview of the proposed architecture has been presented in Fig. 1.

Flow Vector estimation, compression and decompression is done using the traditional Farneback flow estimation method. The flow vectors between every two frames are estimated. The estimated flow vectors are then compressed using a standard CNN based encoder network with Generalized Divisive Normalization (GDN) layers as the nonlinearity (Fig. 3). A CNN based decoder network with Inverse GDN as the nonlinearity is used to decompress the flow vectors.

The structural distortion among the input and output frames has been minimized by following loss function:

$$F(x_t, x'_t) = \lambda_1 \text{SSIM}(x_t, x'_t) + \lambda_2 \text{MSE}(x_t, x'_t)$$

where  $x_t$  and  $x'_t$  represents the input and output videos frames respectively.  $\lambda_1$  is the multiplier and SSIM represents the Structural Similarity Index Metric Loss.  $\lambda_2$  is also the multiplier and MSE denotes the mean square error amid the video input and the output frames.

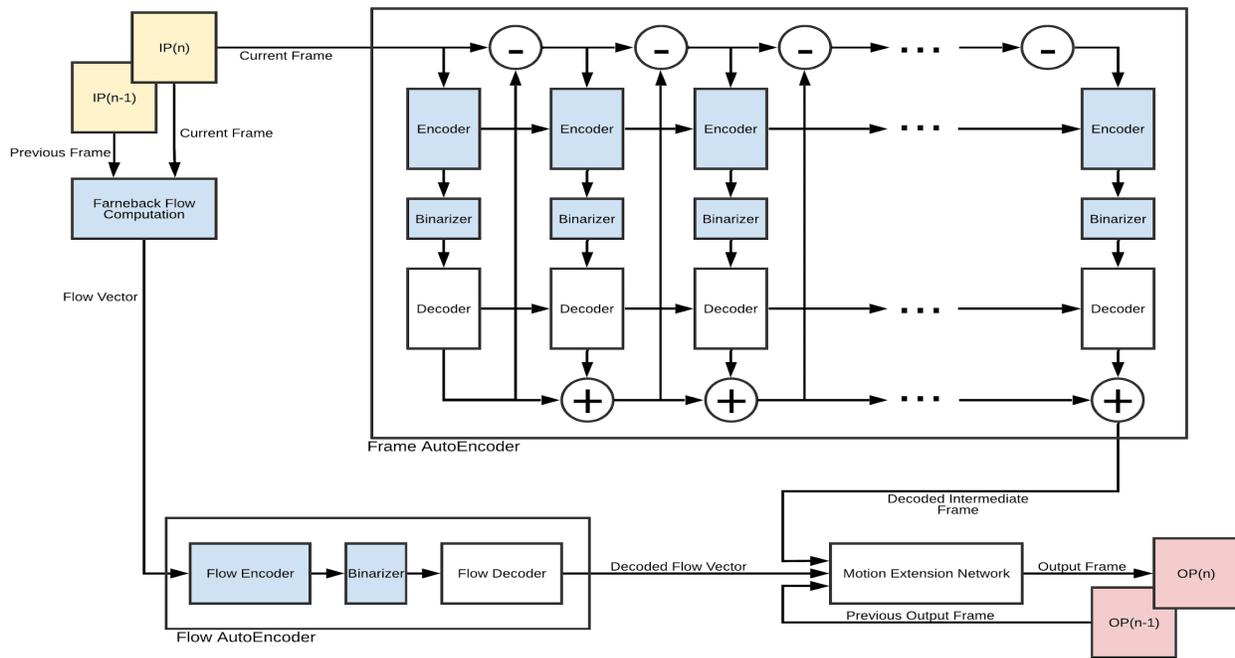


Fig. 1. The Compression Network Architecture.

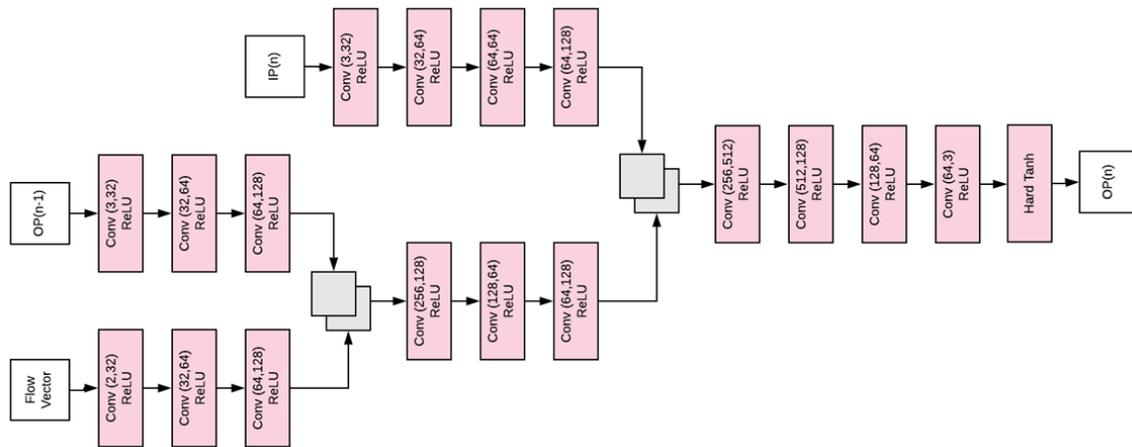


Fig. 2. Motion Extension Network.

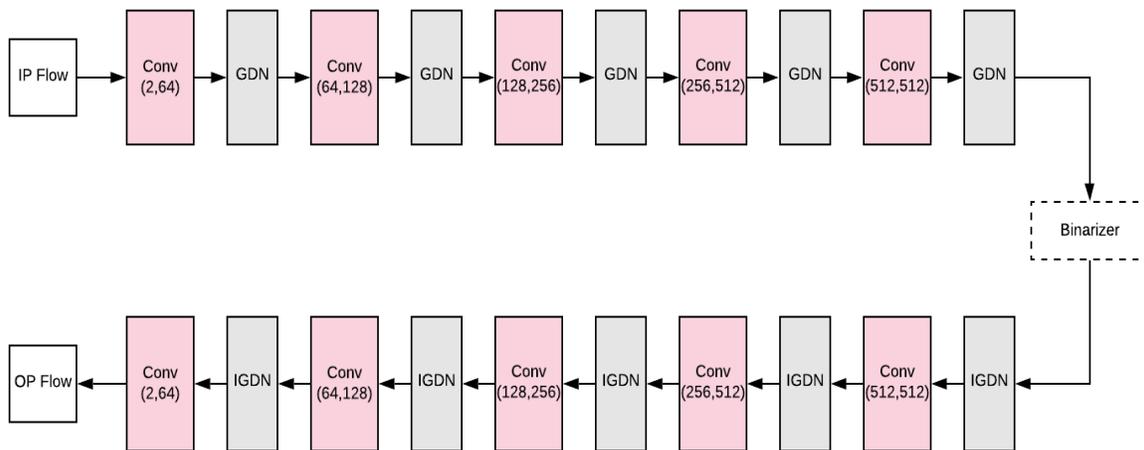


Fig. 3. Flow Autoencoder.

### B. Experiment

Dataset: A dataset comprising of 20s long 571 small videos out of total 826 videos from Youtube UGC has been used to train the network, remaining clips has been for testing and validation. Videos of varying quality have been chosen i.e. 480p, 360p and 720p. The frame size has been chosen as 64x64, so video clips of all quality firstly rescaled to the chosen format, and then training is performed. Videos frames are taken randomly during training but while testing the clips are chosen from the starting. The model has been trained with randomized emission step training strategy with emission steps varying from 1 to 10. Addition of each emission step improves the output but have an effect on the compression efficiency.

Implementation Details: For the implementation purpose, a single T4, K80 or P100 GPU has been used to train the network on the Google Colaboratory platform.  $\lambda_1$  is taken as one and  $\lambda_2$  be 10. The frames have been kept to the size of 64 x 64.  $10e-4$  be the learning rate with Adam Optimizer. During the training of frame encoder with 100 epochs; at 50th, 70th and 90th epoch; the learning rate has been divided by ten. But for the whole model training, only 70 epochs have been used after stacking the framer encoder first and learning rate has been altered at 35th and 55th epoch by dividing ten.

Evaluation: SSIM i.e. Structural Similarity Index and PSNR i.e. Peak Signal to Noise Ratio has been used to measure the visual quality of the reconstructed frames. The temporal distortion encountered among the frames has been evaluated by Flow EPE i.e. End Point Error. Moreover, the reconstruction time of individual frames has been measured by the TPF i.e. Time per Frame parameter.

## IV. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed architecture has been evaluated in terms of perception quality, residual error and efficiency. The experimental results of the network have been obtained for four performance parameters i.e. SSIM, PSNR, EPE and TPF. SSIM, Structural Similarity Index is a good measure of visual perception. Higher the SSIM value, good is the quality of image/video frames. PSNR presents Peak Signal to Noise Ratio. It represents the image quality in term of mean square error. Lower the value of PSNR better will be the image. Flow-EPE, Flow- End Point Error is used to measure the quality of video frames reconstructed in terms of residual error between consecutive frames of a video. The efficiency of the architecture is observed in terms of time required to generate a frame. The Green cell represents Highest achieved value and Red cell represents lowest achieved value.

### A. Performance Analysis

The performance of the proposed architecture is measured in terms of both visual perception and efficiency. The experimental values obtained for the performance parameters namely SSIM, PSNR, Flow EPE and Time per frame are given in the Tables I to IV respectively. Moreover, the corresponding change in the parameters' values with increment of each additional emission step has shown in Fig. 4 to 7. The proposed network has been designed incrementally. Firstly, the results were obtained with simple frame autoencoder trained with randomized training strategy. Secondly, Motion Extension

Network has been incorporated with Frame Autoencoder named as MotionNet Randomized. The values of all four parameters are obtained for each emission step. The graphical representation shows a significant rise in SSIM, PSNR and TPF with each additional emission step in all three randomized architectures. Incorporation of Optical flow and Motion Extension Network results in improved visual quality. The same can be observed by 0.044 rises in SSIM with 3.3 increments in PSNR value.

TABLE I. SSIM VALUES OBTAINED PER EMISSION STEP

SSIM	Baseline	ConvGRU Randomized	MotionNet Randomized	Flow-MotionNet Randomized
1.	0.67	0.652	0.706	0.709
2.	0.67	0.768	0.813	0.819
3.	0.67	0.823	0.866	0.874
4.	0.67	0.864	0.902	0.91
5.	0.67	0.883	0.924	0.932
6.	0.67	0.893	0.938	0.948
7.	0.67	0.916	0.948	0.957
8.	0.67	0.917	0.951	0.961
9.	0.67	0.92	0.953	0.963
10.	0.67	0.919	0.954	0.963

TABLE II. PSNR VALUES OBTAINED PER EMISSION STEP

PSNR	Baseline	ConvGRU Randomized	MotionNet Randomized	Flow-MotionNet Randomized
1.	18.9	18.3	20	20
2.	18.9	21.1	22.2	22.5
3.	18.9	22.4	23.5	24.1
4.	18.9	23.7	24.8	25.5
5.	18.9	24.3	25.8	26.7
6.	18.9	24.6	26.6	27.8
7.	18.9	25.8	27.2	28.4
8.	18.9	25.7	27.6	28.9
9.	18.9	26	27.8	29.1
10.	18.9	25.9	27.8	29.2

TABLE III. FLOW EPE VALUES OBTAINED PER EMISSION STEP

Flow EPE	Baseline	ConvGRU Randomized	MotionNet Randomized	Flow-MotionNet Randomized
1.	1.154	1.251	0.826	0.822
2.	1.154	0.613	0.477	0.577
3.	1.154	0.555	0.383	0.368
4.	1.154	0.409	0.35	0.276
5.	1.154	0.311	0.273	0.226
6.	1.154	0.319	0.248	0.253
7.	1.154	0.273	0.173	0.189
8.	1.154	0.221	0.199	0.17
9.	1.154	0.201	0.175	0.148
10.	1.154	0.173	0.189	0.17

TABLE IV. TIME PER FRAME VALUES OBTAINED PER EMISSION STEP

TPF	Baseline	ConvGRU Randomized	MotionNet Randomized	Flow-MotionNet Randomized
1.	0.015	0.0182	0.0208	0.0243
2.	0.015	0.0186	0.0214	0.0248
3.	0.015	0.0191	0.0218	0.0254
4.	0.015	0.0195	0.0224	0.0258
5.	0.015	0.0201	0.023	0.0263
6.	0.015	0.0205	0.0234	0.0268
7.	0.015	0.0211	0.0239	0.0274
8.	0.015	0.0216	0.0245	0.0279
9.	0.015	0.0221	0.025	0.0285
10.	0.015	0.0226	0.0255	0.029

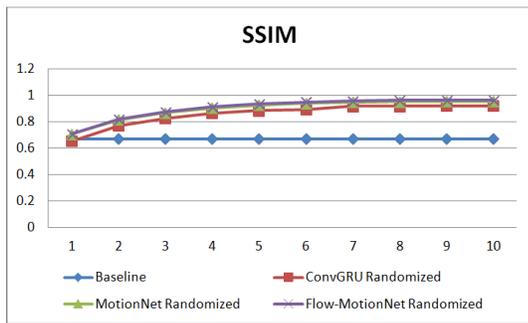


Fig. 4. SSIM Values per Emission.

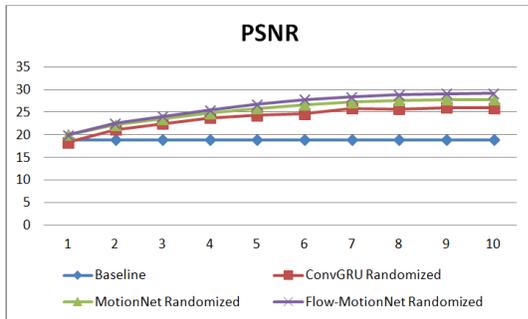


Fig. 5. PSNR Values per Emission.

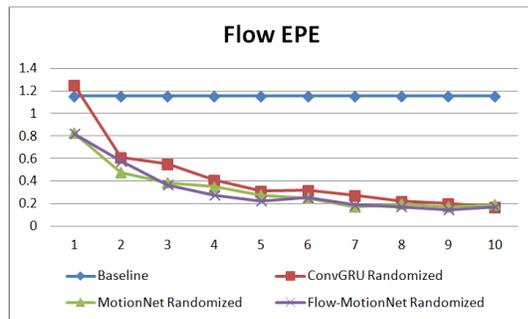


Fig. 6. Flow EPE Values per Emission.

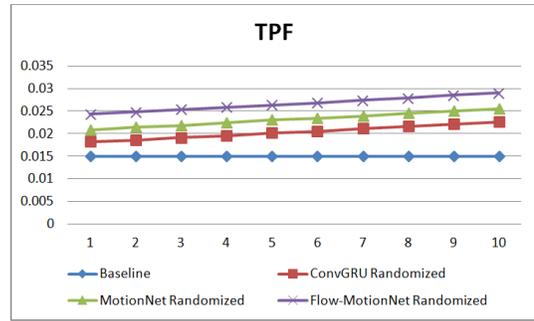


Fig. 7. TPF Values per Emission.

The error in consecutive frames of the video has been measured by Flow-EPE. In general, the EPE values are decreasing with each additional emission step but some fluctuations have been observed in some emission steps like the smallest value of EPE has been obtained after 9th emission step instead of 10th step. But in comparison to the simple frame autoencoder, a slight reduction of 0.003 EPE value has been observed if compared for last emission step. The efficiency of the network has been observed in terms of time required for the network to regenerate a single frame. As the proposed network comprises of optical flow and Motion Extension Network, the increase in computation resulted in slight increase in TPF value, so increased value of TPF has been observed for the proposed network. The analysis of the outcomes reveals that the proposed architecture shows a significant improvement in visual quality but with slight cost of regeneration time. This architecture can be further enhanced by plugging other optimized networks like optical flow, entropy coding etc.

The performance of adaptive bit rate video compression has been analyzed with the average values of performance parameters obtained for all emission steps. The below Table V show the average values of the performance parameters. Here also, the proposed architecture shows a significant improvement in SSIM and PSNR values eventually leading to better video quality frames. But the average TPF value has been increased by 0.00628 units. The incorporation of optical flow and motion extension network, though contributed in improving the visual quality of frames but increased the computation of the network leading to enhanced time in frame regeneration.

TABLE V. AVERAGE PERFORMANCE IN 10 EMISSION STEPS

	Avg. SSIM	Avg. PSNR	Avg. EPE	Avg. TPF
Baseline	0.67	18.9	1.154	0.015
ConvGRU Randomized	0.8555	23.78	0.4326	0.02034
MotionNet Randomized	0.8955	25.33	0.3293	0.02317
Flow-MotionNet Randomized	0.9036	26.22	0.3199	0.02662

### B. Comparison with State-of-Art Architectures

The outcomes of the proposed architecture have also been compared with the state-of-art conventional compression techniques like H.264 and H.265 and also with the deep learning based models proposed by authors of DVC [7] and Adversarial video compression [28].

For comparison, SSIM and PSNR metrics are used to relatively measure the perception quality. MS-SSIM correlates better with human perception of distortion. The proposed model outperformed in terms of MS-SSIM metrics. Table VI represents the MS-SSIM and PSNR values of the various architectures. The proposed model achieved good SSIM performance but with a drop in PSNR value.

TABLE VI. MS-SSIM VALUES OF VARIOUS ARCHITECTURES

Architecture	MS-SSIM	PSNR
H.264	0.955	34
H.265	0.96	36
Adversarial video compression [28]	0.9476	28.46
DVC [7]	0.955	35.5
Flow-MotionNet (Proposed)	0.963	29.2

### V. CONCLUSION

Deep Learning is becoming a milestone in the field of both compression and analytics. Some deep learning based enhancements and improvements surpass the traditional techniques in both qualitative and quantitative measurements. These positive outcomes motivated the exploration of pure deep learning based video compression strategies which can be end to end trained and optimized. This paper also presents a simple lightweight adaptive deep learning based architecture comprises of optical flow and motion extension network trained with randomized training strategy with ten varying emission steps. A ConvGRU unit has been used in each layer of both the encoder and decoder networks of frame autoencoder. Optical Flow has also been used for the motion depiction which eventually helps in frame regeneration with frame autoencoder decoded output in motion extension network. The performance analysis depicts a significant improvement in visual quality measured in terms of both SSIM and PSNR but in trade-off with frame regeneration time. The performance of the proposed architecture can be further improved by addition of other optimization strategies.

### ACKNOWLEDGMENT

The first author expresses her thanks to University Grant Commission, India for providing fellowship in form of JRF to support this work.

### REFERENCES

[1] J. Ball'e, V. Laparra, and E. P. Simoncelli. End-to-end optimized image compression. In Int'l. Conf. on Learning Representations (ICLR2017), Toulon, France, April 2017. Available at <http://arxiv.org/abs/1611.01704>.

[2] K. Gregor, F. Besse, D. Jimenez Rezende, I. Danihelka, and D. Wierstra. Towards conceptual compression. In D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett, editors, Advances in Neural

Information Processing Systems 29, pages 3549–3557. Curran Associates, Inc., 2016.

[3] L. Theis, W. Shi, A. Cunningham, and F. Huszar. Lossy image compression with compressive autoencoders. In Int'l. Conf. on Learning Representations (ICLR2017), 2017.

[4] G. Toderici, S. M. O'Malley, S. J. Hwang, D. Vincent, D. Minnen, S. Baluja, M. Covell, and R. Sukthankar. Variable rate image compression with recurrent neural networks. ICLR 2016, 2016.

[5] G. Toderici, D. Vincent, N. Johnston, S. J. Hwang, D. Minnen, J. Shor, and M. Covell. Full resolution image compression b jgwith recurrent neural networks. CVPR, abs/1608.05148, 2017.

[6] Zhibo Chen, Tianyu He, Xin Jin, Feng Wu, "Learning for video compression", arXiv:1804.09869v2 [cs.MM] 9 Jan 2019.

[7] Guo Lu, Wanli Ouyang, Dong Xu, Xiaoyun Zhang, Chunlei Cai and Zhiyong Gao. DVC:An End-to-end Deep Video Compression Framework. arXiv: 1812.00101v3 [eess.IV] 7Apr 2019.

[8] C.V. Networking Index, "Forecast and methodology," 2016-2021 CISCO White paper, 2016.

[9] I.E. Richardson, "Video codec design: developing image and video compression systems" John Wiley & Sons, 2002.

[10] H. Schwarz, D. Marpe, T. Wiegand, "Overview of the scalable video coding extension of the H.264/AVC standard," in TCSVT, 2007.

[11] J. Ball'e, V. Laparra, E.P. Simoncelli, "End-to-end optimized image compression" in ICLR, 2017.

[12] N. Johnston, D. Vincent, D. Minnen, M. Covell, S. Singh, T. Chinen, S.J. Hwang, J. Shor, G. Toderici, "Improved lossy image compression with priming and spatially adaptive bit rates for recurrent networks," arXiv preprint arXiv:1703.10114, 2017.

[13] O. Rippel, L. Bourdev, "Real-time adaptive image compression" in ICML, 2017.

[14] L. Theis, W. Shi, A. Cunningham, F. Huszar, "Lossy image compression with compressive autoencoders," in ICLR, 2017.

[15] G. Toderici, D. Vincent, N. Johnston, S. Jin Hwang, D. Minnen, J. Shor, M. Covell, "Full resolution image compression with recurrent neural networks," in CVPR, 2017.

[16] M.H. Baig, V. Koltun, L. Torresani, "Learning to inpaint for image compression," in NIPS, 2017.

[17] F. Mentzer, E. Agustsson, M. Tschannen, R. Timofte, L. Van Gool, "Conditional probability models for deep image compression" arXiv preprint arXiv:1801.04260, 2018.

[18] A.v.d. Oord, N. Kalchbrenner, K. Kavukcuoglu, "Pixel recurrent neural networks" in ICML, 2016.

[19] E. Agustsson, F. Mentzer, M. Tschannen, L. Cavigelli, R. Timofte, L. Benini, L.V. Gool, "Soft-to-hard vector quantization for end-to-end learning compressible representations," in NIPS, 2017.

[20] D. Le Gall, "MPEG: A video compression standard for multimedia applications," Communications of the ACM, 1991.

[21] X. Jia, B. De Brabandere, T. Tuytelaars, L.V. Gool, "Dynamic filter networks," in NIPS, 2016.

[22] Z. Liu, R. Yeh, X. Tang, Y. Liu, A. Agarwala, "Video frame synthesis using deep voxel flow" in ICCV, 2017.

[23] S. Niklaus, L. Mai, F. Liu, "Video frame interpolation via adaptive separable convolution" in ICCV, 2017.

[24] C. Vondrick, H. Pirsiavash, A. Torralba, "Generating videos with scene dynamics" in NIPS, 2016.

[25] T. Xue, J. Wu, K. Bouman, B. Freeman, "Visual dynamics: Probabilistic future frame synthesis via cross convolutional networks," in NIPS, 2016.

[26] M. Mathieu, C. Couprie, Y. LeCun, "Deep multi-scale video prediction beyond mean square error," in ICLR, 2016.

[27] Y. Wu, M. Zaheer, H. Hu, R. Manmatha, A.J. Smola, P. Kr'ahenb'uhl, "Compressed video action recognition," in CVPR, 2018.

[28] Sungsoo Kim, Jin Soo Park, Christos G. Bampis, Jaeseong Lee, Mia K. Markey, Alexandros G. Dimakis, Alan C. Bovik.: Adversarial Video Compression Guided by Soft Edge Detection. arXiv:1811.10673v1 [eess.IV] 26 Nov 2018.

# Empirical Study on Microsoft Malware Classification

Rohit Chivukula<sup>1</sup>, Mohan Vamsi Sajja<sup>2</sup>, T. Jaya Lakshmi<sup>3</sup>, Muddana Harini<sup>4</sup>

University of Huddersfield, Huddersfield, United Kingdom<sup>1</sup>

Department of Computer Science and Engineering, SRM University, Andhra Pradesh, India<sup>2,3,4</sup>

**Abstract**—A malware is a computer program which causes harm to software. Cybercriminals use malware to gain access to sensitive information that will be exchanged via software infected by it. The important task of protecting a computer system from a malware attack is to identify whether given software is a malware. Tech giants like Microsoft are engaged in developing anti-malware products. Microsoft's anti-malware products are installed on over 160M computers worldwide and examine over 700M computers monthly. This generates huge amount of data points that can be analyzed as potential malware. Microsoft has launched a challenge on coding competition platform Kaggle.com, to predict the probability of a computer system, installed with windows operating system getting affected by a malware, given features of the windows machine. The dataset provided by Microsoft consists of 10,868 instances with 81 features, classified into nine classes. These features correspond to files of type asm (data with assembly language code) as well as binary format. In this work, we build a multi class classification model to classify which class a malware belongs to. We use K-Nearest Neighbors, Logistic Regression, Random Forest Algorithm and XgBoost in a multi class environment. As some of the features are categorical, we use hot encoding to make them suitable to the classifiers. The prediction performance is evaluated using log loss. We analyze the accuracy using only asm features, binary features and finally both. xGBoost provide a better log-loss value of 0.078 when only asm features are considered, a value of 0.048 when only binary features are used and a final log loss of 0.03 when all features are used, over other classifiers.

**Keywords**—Multi-class classification; malware detection; XGBoost

## I. INTRODUCTION

There are several kinds of malware that can infect a computer system. The number of malwares exceeds 800M in 2019 [1]. Detecting a given file as malware is one of the interesting research problems. Malware detection is challenging because the cybercriminals continuously change the way of attacking the computer systems, resulting in change in the features of malware software. There is a long-lasting confrontation between cyber security experts and malware creators. Machine learning algorithms can be efficiently used to identify whether a given file is malware or not. These algorithms require features/attributes of malwares. Malware files exist either in the form of byte files or assembly language files. Features can be successfully extracted from these files.

Microsoft is one of the major companies that develop anti-malware products. Microsoft has launched a challenge to detect malwares on Kaggle.com [2]. Microsoft has provided nearly half a tera byte of data consisting of malware files. The

dataset given in [2] consists of 10,868 instances with 81 features, classified into nine classes.

Several works are available in the literature on malware classification. Ahmadi et al and Drew et al work on textual feature extraction from the challenge dataset [3,4]. The dataset is of huge size and it is difficult to work on a computer with moderate configuration. Hu et al. address scalability of the dataset [5]. Scofield et al. utilize an entity resolution strategy that merges syntactically dissimilar features [6]. Deep learning techniques are used in [7] and [8] to classify malwares based on the textual features. Narayanan et al. use the classifications like SVM, k-Nearest Neighbours and Artificial Neural Networks in their work [9]. More recent works can be found in [10].

In this work, we apply various multi class classification algorithms to predict the class of a given malware. The organization of this paper is as follows: Section 2 describes the research problem, dataset details, feature extraction and evaluation measures. Section 3 explains proposed approach to solve the problem. Section 4 details the experimental setup. Results are given in Section 5 along with some discussion. Conclusions are given at the end.

## II. PROBLEM DESCRIPTION

### A. Problem Statement

Microsoft has classified malware into 9 classes. Microsoft malware classification is the problem of determining in which class of malware, a given file belongs to. This is a multi-class classification problem. To problem can be elaborated as follows: Given a file, the problem is to estimate the probability of the file belonging to each type of nine classes of malware. In multi-class classification problems, the algorithm predicts the class with maximum probability as the target class. But this kind of approach is not probable for malware classification because, estimation of the probabilities that belong to each class is valuable. For example, the probability of a file belonging to class 3 is 0.5 and class 4 is 0.4. If the problem is modelled such that the file belongs to class 3 considering the maximum probability, we will lose the information of the file may also be affected by class 4 with slight margin. Therefore, our approach computes probability of a given malware belonging to each of the 9 classes. The structure of the solution followed in this work is given in Fig. 1.

### B. Dataset Description

The dataset available at Microsoft malware classification challenge webpage [1] has been used in this work. The organizers of this challenge have provided the training and test

datasets separately. There are two kinds of files in this dataset. (1): .asm file and (2): .bytes file. Total train dataset consists of 200GB of data, out of which 50GB is .bytes files and 150GB is .asm files. There is a total of 10,868 .bytes files and 10,868 asm files, comprising 21,736 files in total, with nine possible class labels denoting 9 types of malwares. The number of files in each kind of class is given in Table I.

Fig. 2 shows the distribution of instances among nine classes of malware in the given dataset. It is understood from Fig. 2 that the problem is highly imbalanced with 27% of instances belonging to class 3 and 0.4% of instances in class 5. Classes 4, 5 and 7 occur very infrequently whereas, classes 1, 2 and 3 are the malwares that occur frequently.

Box plot on asm file size is given in Fig. 3. This indicates that class 2 and 5 have some similarity. But from class distribution plot in Fig. 2 implies that class 2 is frequently occurring, and class 5 is the least occurring class. This signifies that file size is useful in predicting class labels.

Predicted Probability	0.5	0	0	0	0.1	0.4	0	0	0
Class Label	1	2	3	4	5	6	7	8	9

Fig. 1. Structure of Solution.

TABLE I. DATASET DESCRIPTION

Class ID	Family name	#files	Type
1	Ramnit	1541	Worm
2	Lollipop	2478	Adware
3	Kelihos_ver3	2942	Backdoor
4	Vundo	475	Trojan
5	Simda	42	Backdoor
6	Tracur	751	TrojanDownloader
7	Kelihos_ver1	398	Backdoor
8	Obfuscator.ACY	1228	Any kind of obfuscated malware
9	Gatak	1013	Backdoor

A sample data points in both files are given in Table II.

TABLE II. SAMPLE DATA POINT

Sample data point in .asm file	
1	.text:00401000 assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing
2	.text:00401000 56 push esi
3	.text:00401001 8D 44 24 08 lea eax, [esp+8]
Sample data point in .bytes file	
1	00401000 00 00 80 40 40 28 00 1C 02 42 00 C4 00 20 04 20
2	00401010 00 00 20 09 2A 02 00 00 00 00 8E 10 41 0A 21 01
3	00401020 40 00 02 01 00 90 21 00 32 40 00 1C 01 40 C8 18

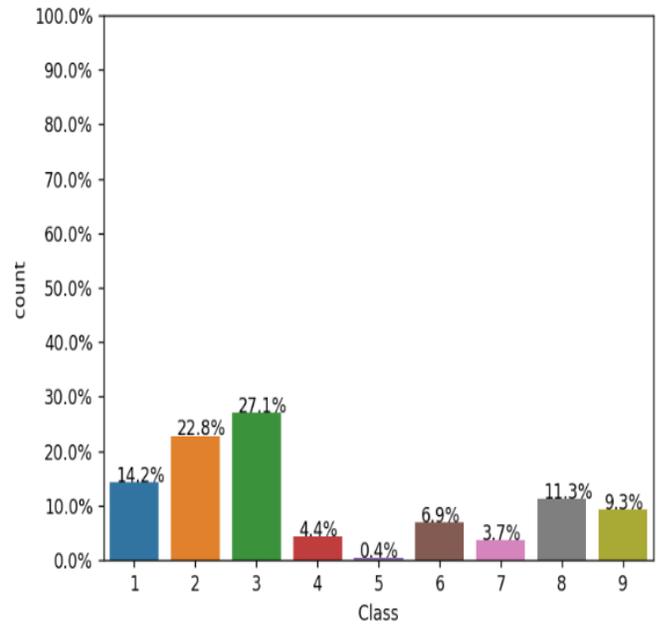


Fig. 2. Class Distribution of Instances.

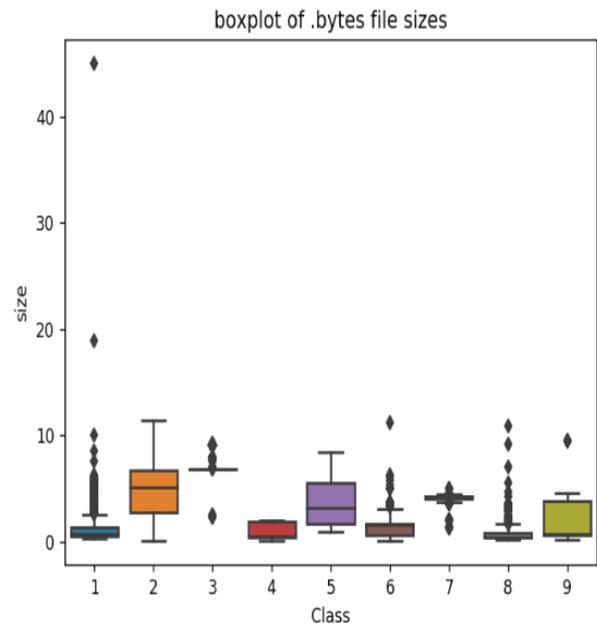


Fig. 3. Box Plot of Byte Files Sizes.

### C. Feature Extraction

1) *Features related to byte files:* As byte files are represented using hexadecimal values, there are 256 distinct values. To pose this as text processing problem, we encode all these 256 values as unigram bag of words. The t-SNE diagram with different perplexities is shown in Fig. 4 and 5. This indicates that some classes are well separated from others. Features extracted from byte files: file\_size, unigram\_bag\_of\_words of size 256.

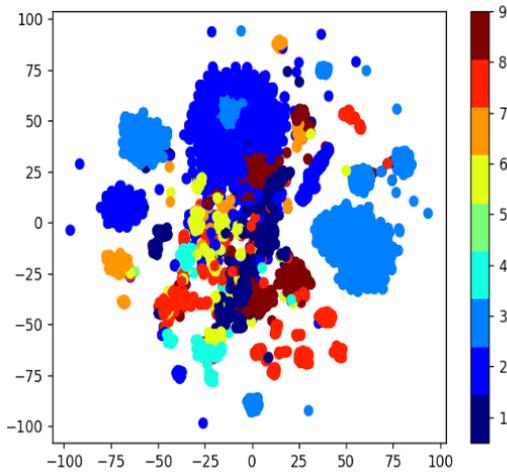


Fig. 4. t-SNE Diagram with Perplexity 50.

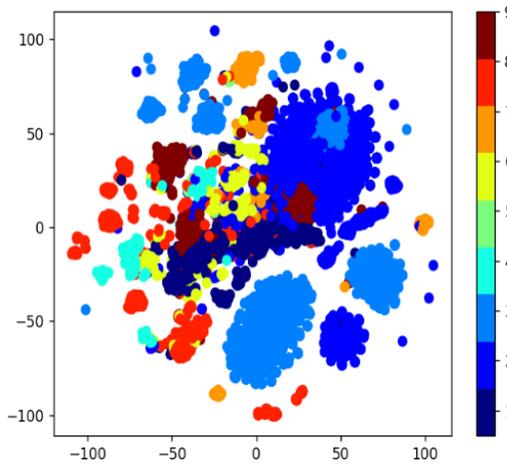


Fig. 5. t-SNE Diagram with Perplexity 30.

2) *Features related to asm files*: There are 10,868 files of asm of size around 150 GB. The initial observation of asm files says that there are Address, Segments, Opcodes, Registers, function calls and API related words in asm files. We have extracted 52 features from all the asm files. These features consist of file\_size, bag of words related to 13 prefixes, 26 opcodes, 3 keywords and 9 registers. As the file size is huge, we use multi-threading with 5 threads to extract these features.

#### D. Evaluation Measures

1) *Multi-class log-loss* [17, 18]: Log loss is the common evaluation measure used for multi class classification problems. Multi class log loss is defined as follows:

$$-\frac{1}{n} \sum_{i=1}^n \sum_{j=1}^c y_{ij} \log(p_{ij})$$

where,  $n$  is the number of instances,

$c$  is the number of classes,

$y_{ij} = 1$  if instance  $i$  belongs to class  $j$  and

$p_{ij}$  is the predicted probability estimate of instance  $i$  belonging to class  $j$ .

A pure classifier yields a log loss of 0. The log loss value increases as the probability estimate by the chosen algorithm goes wrong. The aim of machine learning algorithm is to minimize the log loss value.

2) *Confusion matrix*: A confusion matrix for a  $n$ -class problem will be an  $n \times n$  matrix, where columns correspond to the predicted class labels and the rows corresponds to the actual [19, 20, 21]. The main diagonal gives the correct predictions. That is, the cases where the actual values and the model predictions are the same. In malware classification problem, the matrix is of size  $9 \times 9$ . Each cell  $[i, j]$  represents number of points of class  $i$  are predicted to belong to class  $j$ . The ideal value of confusion matrix  $C$  can be

$$C[i, j] = 0 \text{ if } i \neq j$$

$$= \text{Number of instances of class } i \text{ (or } j) \text{ if } i = j$$

3) *Precision*: Precision is the fraction of correctly predicted instances out of total predictions for a given class [20, 21]. Precision is good if cost of wrong belongingness prediction to a class.

4) *Recall*: Recall is the capture of correct predictions among total instances belonging to the class [20, 21]. Recall is good if cost of identifying an instance which is a member of the class. If a patient who is cancerous is not predicted, it is a huge loss to the patient.

The proposed approach is explained in the next section.

### III. PROPOSED APPROACH

Various machine learning algorithms are used in a multi class environment in this work. The proposed approach is shown in Fig. 6. The algorithms used in this work are briefly explained.

#### A. Random Model

In random model, we compute the probabilities of each class in the solution shown in Table I purely in random and normalise the sum to be 1. A random model gives us the worst possible log loss value of any algorithm. Any model performing worse than random model can be immediately rejected.

#### B. $k$ -Nearest Neighbours ( $k$ -NN) Classifier [11]

$k$ -NN algorithm is a lazy learning algorithm. It doesn't train the model in advance. The algorithm computes distance of test instance from  $k$  nearest instances in the training data. The class to which majority of  $k$  nearest neighbours belongs to is taken as the class of the test instance. Determining right  $k$  is a challenge in this algorithm. Hyper parameter tuning helps us in finding right  $k$ .

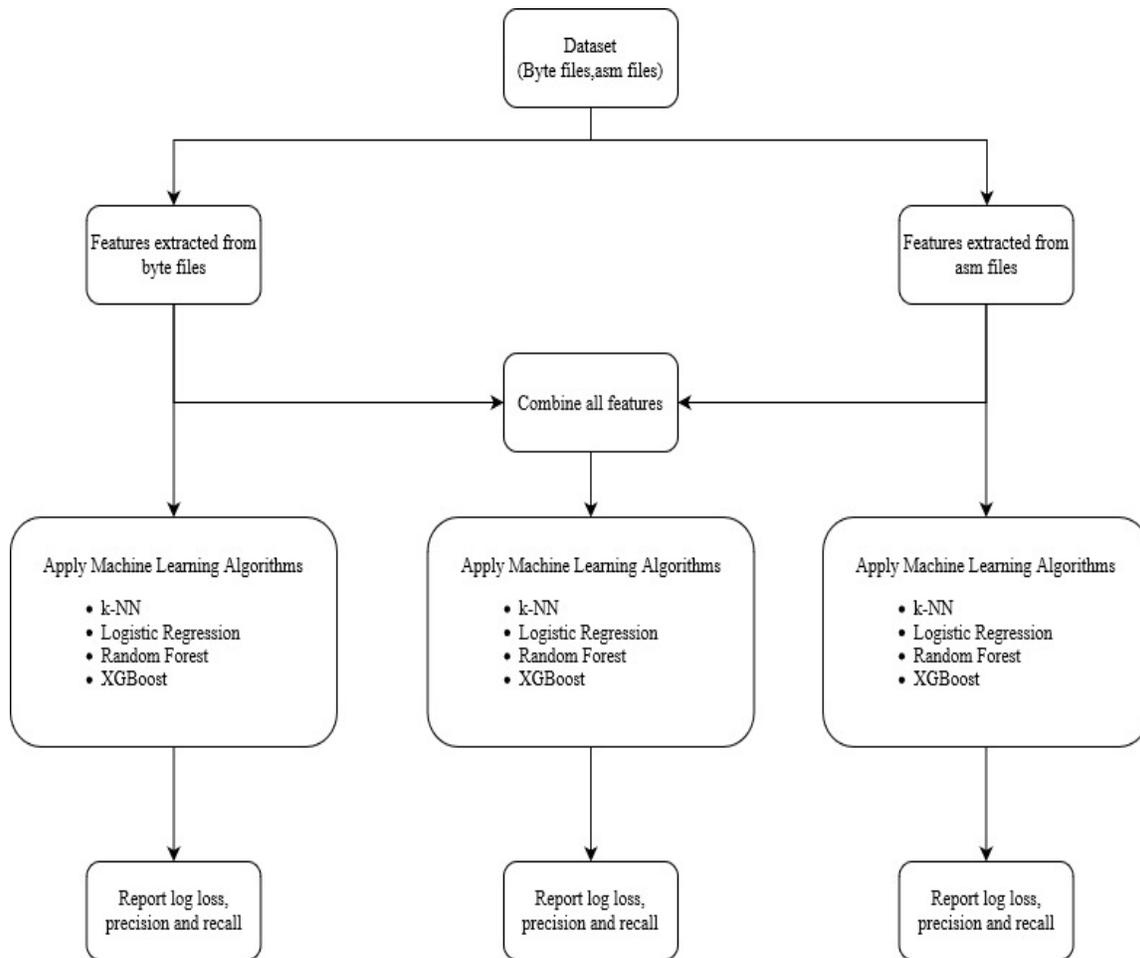


Fig. 6. Proposed Approach.

### C. Logistic Regression [12]

Logistic regression is basically defined for binary classification problem. We use multinomial logistic regression [13], which is a variant of logistic regression for multi class problem. This algorithm predicts the probability of test instance belonging to a class in multi class environment.

### D. Random Forest [14]

Random forest is an ensemble of decision trees trained with bagging. Random forest algorithm constructs n number of decision trees using train data. The class label will be determined by majority voting of all these constructed decision trees. The decision tree algorithm can naturally handle multi class case too.

### E. XGBoost [15]

XGBoost is an optimized distributed gradient boosting library. It utilises Gradient Boosting framework. XGBoost provides a parallel tree boosting method, which is very fast and accurate in many cases. XGBoost is a kind of ensemble. Ensemble learning constructs of a group of predictors that use multiple models and aggregates the performance of each tree. In Boosting technique, the errors made by previous models are

tried to be corrected by succeeding models by adding some weights to the models.

Characteristics of XGBoost:

- XGBoost is used in regression as well as classification problems.
- Supports parallel processing.
- Can be able to manage memory very efficiently for large datasets exceeding RAM.
- Supports different kinds of regularizations which helps in reducing overfitting.
- Provides auto pruning of tree.
- Efficiently handles missing values.
- Has inbuilt Cross-Validation.
- Takes care of outliers to some extent.

All the classification algorithms chosen are sensitive to parameters. The experimental setup and parameter setting is discussed in the next section.

#### IV. EXPERIMENTAL SETUP

This section describes the parameter selection of machine learning algorithms used for experimentation. Some classifiers we intend to use are sensitive to parameters. We perform hyper parameter tuning to fix the best parameter. The hyper parameter tuning is shown in Fig. 7 to 10.

$k$ -NN classifier is sensitive to the value of  $k$  [16]. To find best  $k$ , we have tested the model with different values of  $k$  from 1 to 15. The model gives best log loss for  $k=1$ , as shown in Fig. 7. Therefore, we use  $k=1$  in our experimentation.

For Random Forest classifier, we have tested with number of trees varying from 10 to 3000 (Fig. 9). With 1000 trees we could achieve best log loss and low misclassification error. Therefore, we use 1000 trees in random forest. We use XGBoost classifier with 500 trees, 500 estimators with a maximum depth of 5 and learning rate 0.05.

Any machine learning algorithm needs training and testing to determine the performance of the classifier. We split the dataset randomly into three parts train, cross validation and test with 64%, 16%, 20% of data respectively. We use 80% of data for training and 20% for testing.

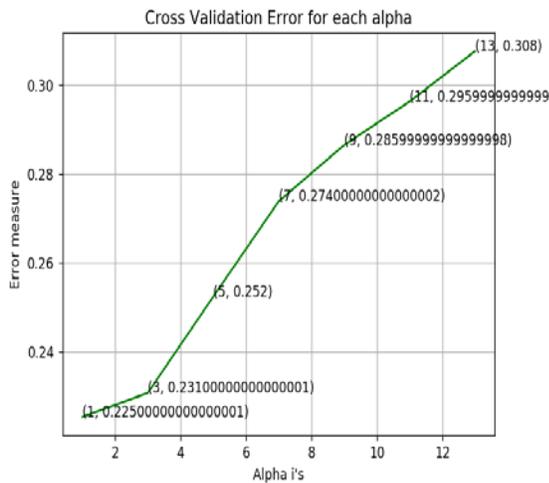


Fig. 7. Hyper Parameter Tuning for k-NN.

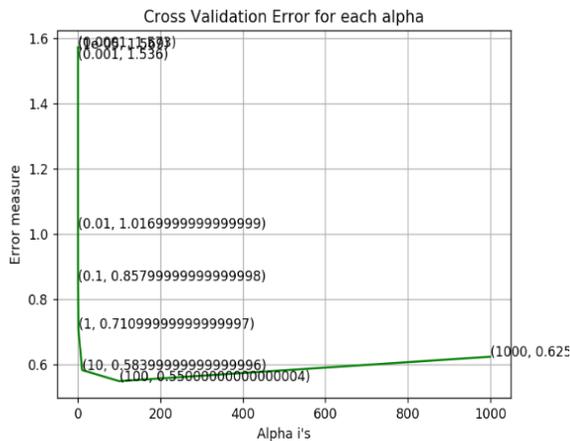


Fig. 8. Hyper Parameter Tuning for Logistic Regression.

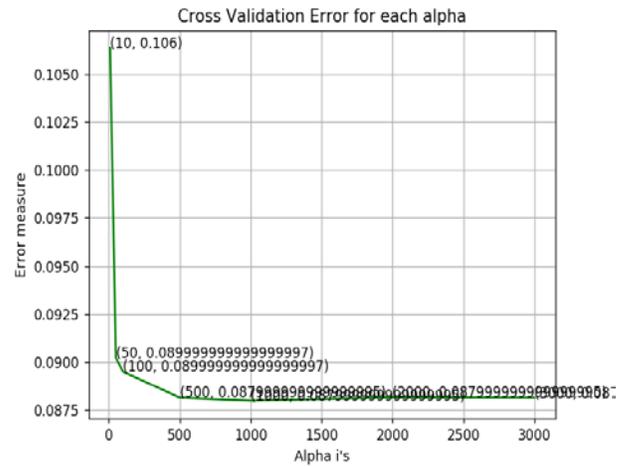


Fig. 9. Hyper Parameter Tuning for Random Forest.

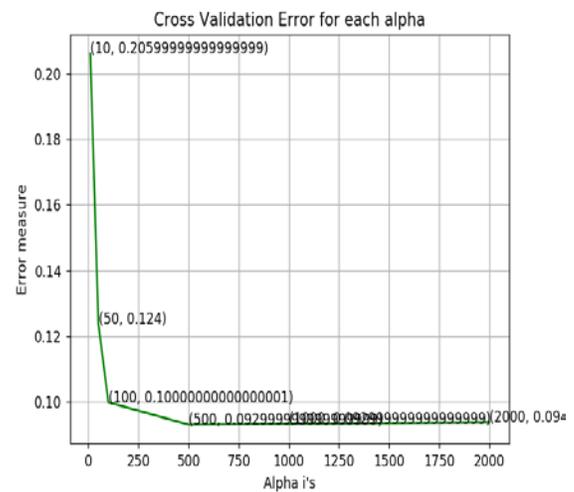


Fig. 10. Hyper Parameter Tuning for XGBoost.

#### V. RESULTS AND DISCUSSION

We experiment with the features extracted from byte files, asm files individually and by combining them all. The following sections present the results.

##### A. Results on Byte Files

The log loss values on cross validation as well as test data are tabulated in Table III. Random forest classifier achieves low log loss value on cross validation data, whereas XGBoost is the winner on test data as well as misclassified errors.

From Table IV, we can see that the precision and recall of  $k$ -NN for class 5 is low compared to other classes. We guess that this is because of very few number of instances in class 5 (Fig. 1). From precision matrix, it is understood that there is a confusion between class 1 and class 5.

##### B. Results on Features Extracted from asm Files

The log loss values computed using features extracted from asm files are tabulated in Table V. XGBoost obtain better log loss on test data. But precision and recall for class 5 is improved using asm file features as shown in Table VI.

TABLE III. LOG LOSS RESULTS USING ONLY BYTE FILES

Algorithm	Log loss		#misclassified points
	cross validation	test data	
Random model	2.4561	2.4850	88.5000
k-NN	0.2253	0.2415	4.5078
Logistic Regression	0.5499	0.5283	12.3275
Random Forest	<b>0.0879</b>	0.0858	2.0239
XGBoost	0.0928	<b>0.0782</b>	<b>1.2419</b>

TABLE IV. PRECISION AND RECALL USING ONLY BYTE FILES

Classifier↓	Class →	1	2	3	4	5	6	7	8	9
KNN	Precision	0.88	0.97	1.00	0.97	0.75	0.89	0.94	0.96	0.91
	Recall	0.96	0.93	1.00	0.96	0.75	0.92	0.91	0.93	0.92
Logistic Regression	Precision	0.76	0.96	0.99	0.78	0.00	0.78	0.96	0.70	0.86
	Recall	0.78	0.89	0.99	0.97	0.00	0.68	0.95	0.88	0.70
Random Forest	Precision	0.94	0.99	0.99	0.95	1.00	0.95	1.00	0.95	0.98
	Recall	0.98	0.99	1.00	0.96	0.87	0.95	0.95	0.93	0.97
XGBoost	Precision	0.95	0.99	1.00	0.95	1.00	0.97	1.00	0.99	0.99
	Recall	0.99	0.99	1.00	0.98	0.75	0.98	0.96	0.95	0.98

TABLE V. LOG LOSS RESULTS USING ONLY ASM FILES

Algorithm	Log loss		#misclassified points
	cross validation	test data	
Random model	2.4561	2.4850	88.5000
k-NN	0.0958	0.0894	2.0239
Logistic Regression	0.4244	0.4156	9.6136
Random Forest	<b>0.0496</b>	0.0571	1.1499
XGBoost	0.0560	<b>0.0491</b>	<b>0.8739</b>

TABLE VI. PRECISION AND RECALL USING ONLY ASM FILES

Classifier↓	Class →	1	2	3	4	5	6	7	8	9
KNN	Precision	0.96	1.00	0.99	0.96	0.70	0.98	0.95	0.95	0.97
	Recall	0.97	0.99	0.99	0.91	0.87	0.95	0.97	0.94	1.00
Logistic Regression	Precision	0.89	0.97	0.84	0.97	0.00	0.93	0.47	0.89	0.95
	Recall	0.91	0.99	0.99	0.71	0.00	0.88	0.10	0.83	0.95
Random Forest	Precision	0.97	1.00	0.99	0.98	1.00	0.99	0.96	0.97	0.98
	Recall	0.99	1.00	0.99	0.95	0.87	0.96	0.98	0.96	0.99
XGBoost	Precision	0.97	1.00	0.99	0.98	1.00	1.00	0.96	0.98	0.98
	Recall	0.99	1.00	0.99	0.95	0.87	0.97	0.98	0.98	0.99

### C. Results on Both Byte and asm Files

Random forest ensemble and XGBoost clearly obtain better accuracy in both cases of asm as well as byte files. We have used both features in these two models and present results in Table VII. When 257 features related to byte files as well as 53 features extracted from asm files are used for training, log loss result of XGBoost is improved for both cross validation as well as testing data from 0.048 to 0.031.

TABLE VII. LOG LOSS RESULTS USING ASM AND BYTE FILES

Algorithm	Log loss	
	cross validation	test data
Random Forest	0.0355	0.0401
XGBoost	0.0315	0.0323

### VI. CONCLUSION

In this paper, we detect the type of malware that a given file belongs to. We use unigram model to construct bag of words from byte files as well as asm files. Random forest and XGBoost classifiers achieve a better log loss value of 0.031 over other classifiers used in this work. Usage of only byte files failed to detect some class of malware especially class 5, where the number of files are few, but the other information pertaining to asm files could succeed in detecting malwares belonging to all class. In future, we would like to apply advanced text retrieval features on byte files to improve the log-loss.

### REFERENCES

- [1] Beek, C., et al. "Mcafee labs threats report: August 2019." McAfee Labs (2019).
- [2] <https://www.kaggle.com/c/malware-classification/data>.
- [3] Ahmadi, Mansour, et al. "Novel feature extraction, selection and fusion for effective malware family classification." Proceedings of the sixth ACM conference on data and application security and privacy. 2016.
- [4] Drew, Jake, Tyler Moore, and Michael Hahsler. "Polymorphic malware detection using sequence classification methods." 2016 IEEE Security and Privacy Workshops (SPW). IEEE, 2016.
- [5] Hu, Xin, et al. "Scalable malware classification with multifaceted content features and threat intelligence." IBM Journal of Research and Development 60.4 (2016): 6-1.
- [6] Scofield, Daniel, Craig Miles, and Stephen Kuhn. "Fast model learning for the detection of malicious digital documents." Proceedings of the 7th Software Security, Protection, and Reverse Engineering/Software Security and Protection Workshop. 2017.
- [7] Kebede, Temesguen Messay, et al. "Classification of malware programs using autoencoders based deep learning architecture and its application to the microsoft malware classification challenge (big 2015) dataset." 2017 IEEE National Aerospace and Electronics Conference (NAECON). IEEE, 2017.
- [8] Yuxin, Ding, and Zhu Siyi. "Malware detection based on deep learning algorithm." Neural Computing and Applications 31.2 (2019): 461-472.
- [9] Narayanan, Barath Narayanan, Ouboti Djaneye-Boundjou, and Temesguen M. Kebede. "Performance analysis of machine learning and pattern recognition algorithms for malware classification." 2016 IEEE National Aerospace and Electronics Conference (NAECON) and Ohio Innovation Summit (OIS). IEEE, 2016.
- [10] Zagi, Luqman Muhammad, and Baharuddin Aziz. "Searching for Malware Dataset: a Systematic Literature Review." 2020 International Conference on Information Technology Systems and Innovation (ICITSI). IEEE, 2020.
- [11] Aha, David W., Dennis Kibler, and Marc K. Albert. "Instance-based learning algorithms." Machine learning 6.1 (1991): 37-66.
- [12] Kleinbaum, David G., et al. Logistic regression. New York: Springer-Verlag, 2002.
- [13] Böhning, Dankmar. "Multinomial logistic regression algorithm." Annals of the institute of Statistical Mathematics 44.1 (1992): 197-200.
- [14] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.
- [15] Chen, T., & Guestrin, C. (2016, August). Xgboost: A scalable tree boosting system. In Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining (pp. 785-794).
- [16] Zhang, Shichao, et al. "Learning k for knn classification." ACM Transactions on Intelligent Systems and Technology (TIST) 8.3 (2017): 1-19.
- [17] Ferri, César, José Hernández-Orallo, and R. Modroiu. "An experimental comparison of performance measures for classification." Pattern Recognition Letters 30.1 (2009): 27-38.
- [18] Read, Jesse, et al. "Classifier chains for multi-label classification." Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, Berlin, Heidelberg, (2009): 254-269.
- [19] Townsend, James T. "Theoretical analysis of an alphabetic confusion matrix." Perception & Psychophysics 9.1 (1971): 40-50.
- [20] Powers, David MW. "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation." arXiv preprint arXiv:2010.16061 (2020).
- [21] Ting, K. M. "Confusion Matrix, Encyclopedia of Machine Learning and Data Mining." (2017).

# Smart Intersection Design for Traffic, Pedestrian and Emergency Transit Clearance using Fuzzy Inference System

Aditi Agrawal<sup>1</sup>, Rajeev Paulus<sup>2</sup>

Department of Electronics and Communication Engineering  
VIAET, SHUATS, Prayagraj, India

**Abstract**—Traffic flow is regulated and controlled with the aid of traffic signals implemented at all major intersections in urban areas. With the increase in vehicles, the traditional control strategies are incapable of clearing heavy traffic which leads to long traffic queues and prolonged waiting time at intersections. Smart cities are increasingly adopting solutions by developing smart traffic lights to improve the flow of vehicles. A major demand arises to increase the efficiency of traffic controllers with the objective to minimize traffic congestion, prioritize emergency transit and give way to pedestrians to cross the lanes at an intersection. This requires leveraging the existing techniques that identify the best solutions at the lowest possible cost. This paper proposes Fuzzy Adaptive Control System (FACS) that uses fuzzy logic to decide the phase sequence and green-time for each lane based on sensed input parameters. It is designed with an aim to improve traffic clearance at isolated intersection especially in peak traffic hours of the day along with giving precedence to emergency vehicle as soon as it is detected and also assist pedestrian passage thus reducing their waiting time at the intersection. Performance of the proposed Fuzzy Adaptive Control System (FACS) is evaluated through simulations and compared with Pre-Timed Control System (PTCS) and Traffic Density-based Control System (TDCS) at a busy intersection with lanes leading to offices, schools and hospitals. Simulation results show significant improvement over PTCS and TDCS in terms of traffic clearance, immediate addressing of the emergency vehicle and giving preference to pedestrian passage at the intersection.

**Keywords**—Adaptive traffic light control; smart intersection; fuzzy logic; emergency vehicle; pedestrian crossing

## I. INTRODUCTION

Traffic signals are installed at road intersections and play a major role to control the traffic flow and avoid congestion. The increased number of vehicles and greater urbanization create critical problems of traffic jam, increased wait time and fuel consumption at intersections. This problem occurs mainly due to the most common version of traffic light controllers, the Pre-Timed Control System (PTCS) that gives way to lanes based on fixed signalling plans. This system is easy to install but is effective only in situations with low traffic density that does not show large variations in time. In case of heavy traffic and varied flow, it is necessary to keep a greater control over the traffic configuration at intersections. Some intersections are equipped with Traffic Density-based Control System (TDCS) that uses information on current traffic obtained from detectors and necessary control logic to prioritize certain

phases or traffic movements to be serviced. This system shows improved performance over PTCS. However, they are ineffective in clearing heavy traffic during peak hours. An effective approach is an adaptive and intelligent design that can respond to the random traffic flow behavior and even consider other decision parameters. Rule-based fuzzy logic control scheme helps in the development of multi-criteria control procedures very similar to human thinking and can best replace an ideal policeman at the intersection. Use of fuzzy logic in taking decisions for existence of roundabout to assist in path planning of a wheeled mobile robot is presented in [1]. In an in-depth review [2] the authors have summarized a wide literature of fuzzy logic-based traffic light controllers in an effective tabular representation. A detailed survey of use of in-vehicle and on-road sensors to serve as data collection components in Intelligent Transportation System (ITS) is discussed in [3]. Comparison between different sensor technologies giving the advantages and disadvantages was also discussed.

Fuzzy logic started by Zadeh [4] has been commonly used by researchers in solving traffic congestion problem at intersections and the development of fuzzy logic in traffic control was extensively discussed in [5]. The advantage of using this kind of traffic signal control in Saudi Arabia was illustrated in [6]. A fuzzy based system used to adjust the phase sequence and duration of traffic lights at isolated intersection [7] was tested by collecting real time data from signalized intersection in State of Kuwait. This system showed improved performance in case of heavy traffic volume. Various other research efforts have been conducted to combine fuzzy logic in providing solution for traffic management at intersections. An isolated T-junction was considered [8] and fuzzy logic-based traffic light controller was designed by taking fuzzy inputs as vehicles on arrival side, queue side and right side to decide for the output variable extension time. Better performance was achieved in terms of decreased waiting time but the authors proposed to conduct future research by taking pedestrians and emergency movement into account. A two-stage fuzzy control for traffic light was suggested [9] by calculating traffic urgency degree for all red phases using traffic urgency evaluation module and a decision module to decide green time extension of current green phase. Similar two stage fuzzy system [10] included the first stage named as urgency decision module which decided the next green phase based on urgency. The second module

calculated the green time extension of the chosen phase with the help of queue length as input. Another work [11] considered the possibility to change the green light duration at an isolated four-lane intersection using fuzzy inference system by taking the road condition, traffic and time of the day as major deciding inputs. Researchers in [12] applied fuzzy logic to improve traffic light by taking queue length, arrival flow and exit flow as inputs and calculated the urgency degree using fuzzy rules. The variable cycle length was obtained by extending or shortening the phase time in accordance with the urgency degree. Comparison with fixed time control system showed significant improvement. Traffic flow of a four-way intersection and T-crossing was studied in [13] and traffic flow probability for the lanes was considered. The designed fuzzy logic controller used inputs as queue length and waiting time of vehicles, decided using the rule base for the output variable green-time. This traffic light system followed the fixed phase sequence and only altered the green time of the lanes. Results showed significant improvement over the static phase traffic light system. A recent research [14] used queue lengths as input given to two controllers used to select the green phase and decide the green time. These designs showed improved performance as compared to pre-timed system by reducing the average waiting time of vehicles but in the absence of emergency transit and pedestrian consideration.

In view of the risk of pedestrians who are waiting long to cross the lane while green and their proneness to accidents, the adaptive traffic light design must also consider giving way to pedestrians while addressing traffic at the intersection. Another important consideration is giving way to emergency transit such as ambulance, fire brigade, police van, etc. immediately as they are detected at the intersection. Some research works that considered emergency transit includes [15] by using three-stage fuzzy control. They considered queue length and waiting time of vehicles as two input variables and green time extension as output variable of the first stage. The output from the first stage works as input to the next stage and the third stage switches current phase to the demanded next phase by output of its previous stage. A separate function block was developed to detect emergency vehicle siren and switch to green to prioritize its passage which added to the design complexity. Fuzzy control system [16] designed by taking queue lengths, traffic arrival rate and emergency vehicle as inputs to two controllers for phase selection and green-time extension. Simulation results showed noticeable improvements when compared with pre-timed system. However, in real time scenario the use of two controllers may lead to high response time as compared to a single controller design. A dynamic traffic management center was proposed in [17] to determine the priority of road segment using fuzzy logic. The two input parameters taken namely vehicle count and presence of emergency vehicle were taken to output the phase priority. Green duration was calculated mathematically on account of the number of vehicles present on the road segment. The designed controller prioritized emergency vehicle clearance and optimized wait time of vehicles at intersection. This work also used congestion-aware routing algorithm to transmit sensed data from roadside sensors to the controller with minimum delay. The authors

further proposed to test and validate the designed system in the real time scenario and also proposed to work on connected intersections.

A smart portable wireless control system for pedestrian crossing was developed [18] to manage the traffic automatically and assist the pedestrians to cross the road safely. The system infrastructure and cost-effective design finds application to develop smart pedestrian crossings especially near schools. Smart solution to regulate traffic lights in signalized pedestrian crossings by use of fuzzy logic controller was also proposed [19]. Time of the day and the number of pedestrians about to cross the road were considered. The pedestrian flow was analyzed and performance was compared with static traffic lights. The designed system reduced the average queue length of the pedestrians waiting to cross. A controller using three fuzzy modules [20] was designed to find the extension degree of green phase and urgency degree of red phases. The controller showed enhanced performance under low and medium traffic conditions but only small improvement was achieved under heavy traffic conditions. The past works projected the need of an integrated design to support vehicle, emergency and pedestrian clearance at the intersection.

This paper proposes an integrated design of Fuzzy Adaptive Control System (FACS) with an objective of reducing congestion, prioritizing emergency transit and giving way to pedestrians thus, reducing their waiting time at the intersection. Another feature of the designed system is that the design makes use of a single controller with four fuzzified inputs and two fuzzified outputs and an optimized rule base. This simple design helps in reducing the response time of the controller which is a desirable feature in real time applications. To evaluate the performance of proposed FACS a realistic traffic model is used to obtain traffic variation for 24 hours of the day at a busy intersection.

## II. PROPOSED SYSTEM DESIGN

### A. Implementation Scenario

The traffic intersection under study is considered to be a four-lane intersection. This is assumed to be one of the major and most occupied intersection of an urban area with lanes leading to offices, schools and hospitals. So, a need arises incorporate an intelligent traffic light system to manage traffic, emergency transit along with giving way to pedestrians to cross. The real-time traffic inflow on the lanes existing throughout the day is modelled as a stochastic process. The implementation scenario of the proposed system at a congested intersection is shown in Fig. 1. The vehicle and pedestrian detectors are employed as considered in [20]. Roadside detectors are used to count vehicles on lanes and a push-to-walk button is deployed at sidewalks to collect information about pedestrians. The pedestrians who wish to cross the road can push this button and timer gives information about the duration since button is pressed. This duration is termed as Pedestrian Wait Time (PWT). Acoustic sensors are deployed way ahead of the intersection to sense the emergency vehicle headed towards the intersection.

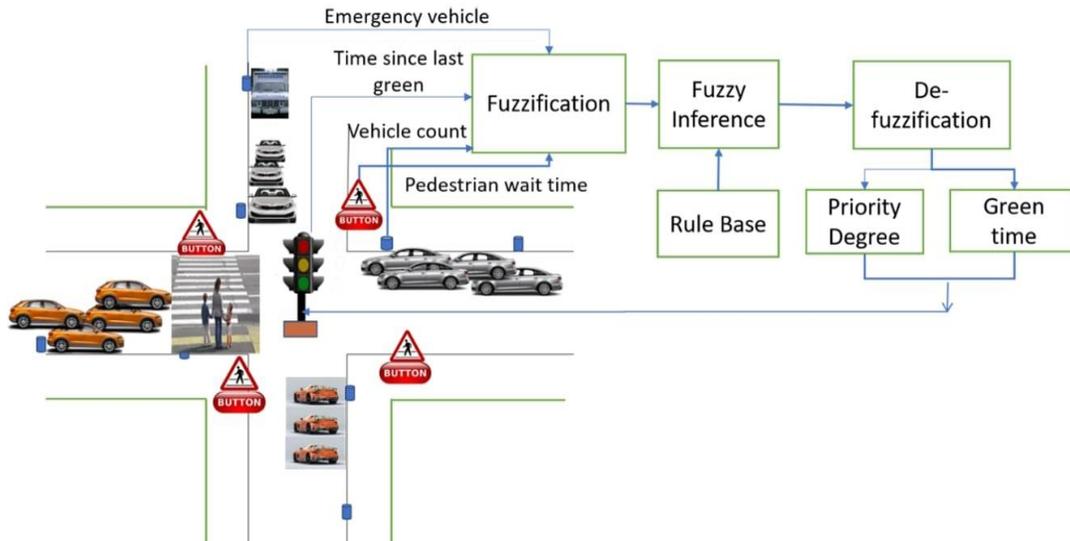


Fig. 1. Implementation Scenario of Proposed Fuzzy Adaptive Control System.

### B. Fuzzy Inference System Design

The proposed FACS system is designed and modelled in MATLAB using Fuzzy Logic Toolbox.

A simplistic approach having four inputs and two outputs is used in order to design FACS. The inputs are taken as Vehicle Count (VC), Pedestrian Wait Time (PWT), Time since last Green (TG) and Emergency Transit (ET) as they are important parameters in deciding the green passage for lanes. Two outputs of the fuzzy inference system are Priority Degree (PD) and Green Time (GT). A single controller is preferred over multiple controllers in stages for low data processing and realistic control actuation times. Fuzzy Parameters and their membership function design are as shown in Fig. 2 to 7. Trapezoidal and triangular membership functions are used to represent the input and output fuzzy variables.

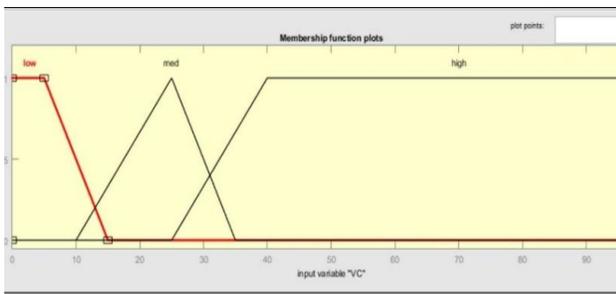


Fig. 2. Membership Function of Vehicle Count.

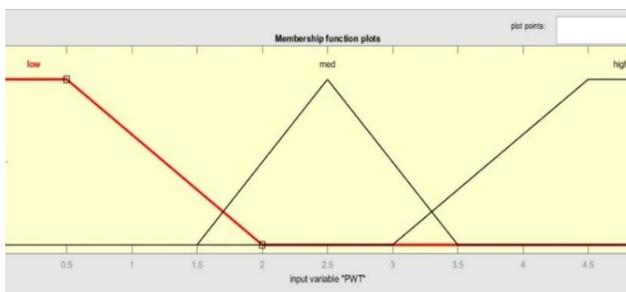


Fig. 3. Membership Function of Pedestrian Wait Time.

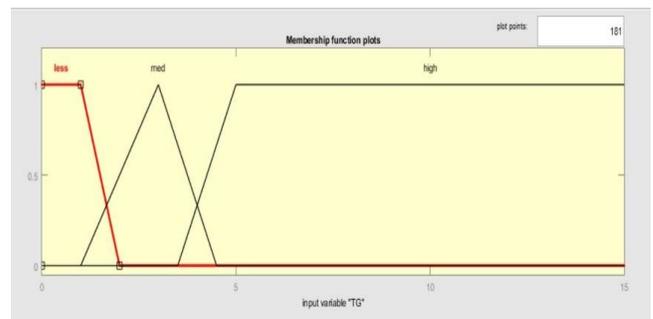


Fig. 4. Membership Function of Time since Last Green.

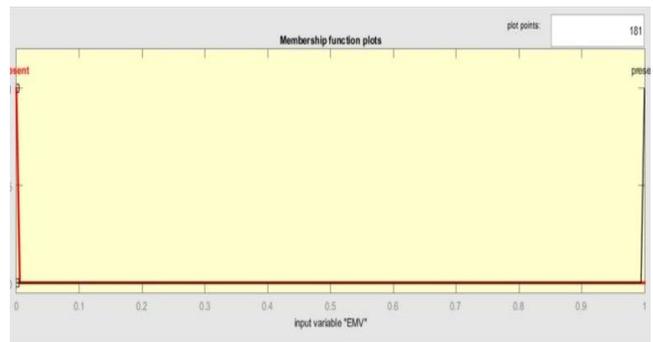


Fig. 5. Membership Function of Emergency Transit.

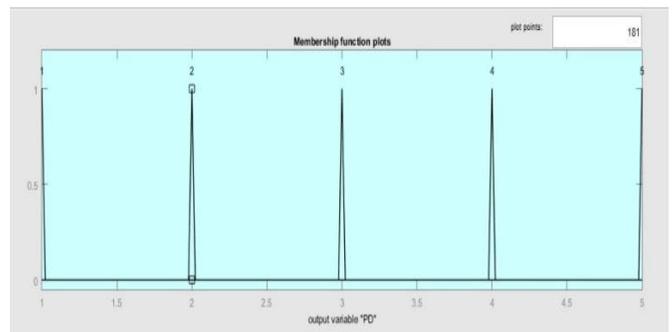


Fig. 6. Membership Function of Priority Degree.

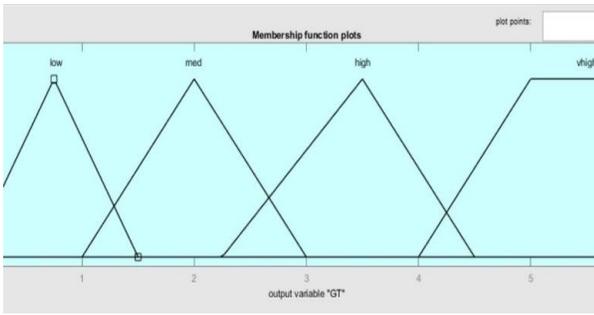


Fig. 7. Membership Function of Green Time.

### C. Rule Base Design

Rules of the fuzzy inference system are fabricated with an aim to maximize traffic clearance even in peak traffic hours along with highest priority to emergency transit and preference to pedestrian waiting on the sidewalk to cross. While designing the rules in MATLAB's fuzzy inference system highest priority is given to the lane detected with Emergency Transit (ET). Vehicle Count (VC) is considered as the second most important factor as it indicates the degree of traffic congestion. The lane with maximum Pedestrian Wait Time (PWT) is given low priority for green phase so that pedestrians could cross. Time since last Green (TG) is an input to avoid the situation when lane with low traffic does not get green signal and vehicles in that lane undergo a prolonged waiting time. The output is Priority Degree (PD) for the lanes. It is arranged in decreasing order for green phase sequencing in next cycle. The second output is Green Time (GT) that corresponds to the time for which the traffic signal is green for the corresponding lane. The Rule editor of the proposed fuzzy system is given in Fig. 8. Design is optimized with 30 rules in the rule base. Less number of rules minimizes the processing time of the controller and hence fast response time is achieved which is a desirable QoS parameter while dealing with real time inputs.

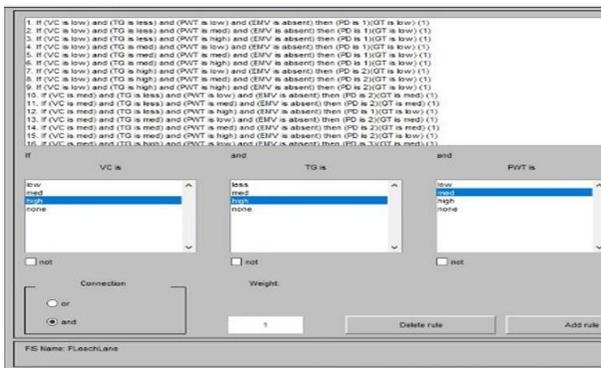


Fig. 8. Rule Editor of Proposed Fuzzy Adaptive Control System.

### D. 3-D Surface Plots of Fuzzy Inference System

After designing the rule base of proposed FACS, the impact of input variables on output variables can be seen by studying the surface plots. Surface plot in Fig. 9 illustrates that output variable Green Time (z-axis) rises and takes maximum value as the Vehicle Count (x-axis) increases at low values of Ped Wait Time (y-axis) whereas at high values of Ped Wait Time (PWT) the Green Time (GT) rises with increasing

Vehicle Count (VC) but takes low values to allow traffic to pass as well as ensuring that even pedestrians do not wait for increased time.

Surface plot in Fig. 10 shows that output variable Priority Degree (z-axis) has maximum value when Vehicle Count (y-axis) is high but decreases with increasing Ped Wait Time (x-axis). The value of Priority Degree (PD) decreases sharply if Ped Wait Time (PWT) is high for low value of Vehicle Count (VC).

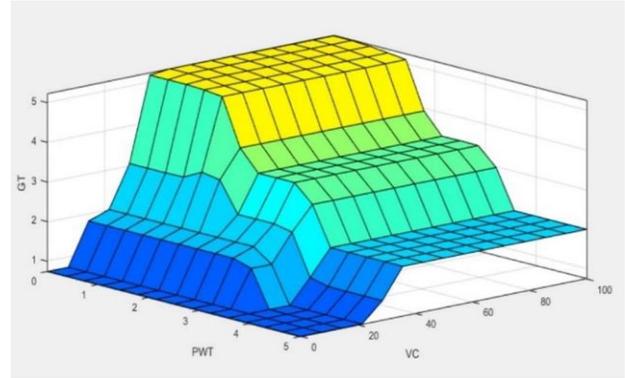


Fig. 9. Surface Plot of Output Variable Green Time.

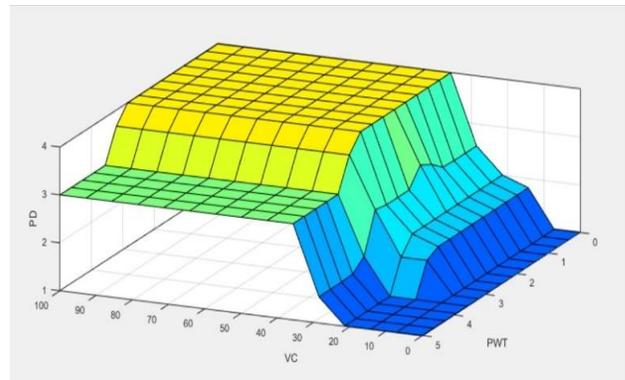


Fig. 10. Surface Plot of Output Variable Priority Degree.

## III. SIMULATION SETUP

### A. Traffic Distribution

Traffic analysis and good traffic modelling is an essential requirement for accurate planning of traffic capacity. There are many traffic models among which the Poisson distribution [21] has been widely used to model the incoming traffic [8]. Number of vehicles arriving per unit of time interval has been modelled using parameter  $\lambda$  of the Poisson distribution. A realistic simulation environment is chosen to model a busy traffic intersection. The traffic distribution on lanes at various intervals of time in the day has been characterized by values of  $\lambda$  as stated in Table I.

Random distribution of vehicle arrival at low traffic hours ( $\lambda=8$ ) and peak traffic hours ( $\lambda=25$ ) obtained for 100 iterations is shown in Fig. 12. The traffic flow on any lane for the entire day showing peak traffic hours to emulate actual traffic scenario at the intersection is represented in Fig. 11. The time of the day between 10 am to 11 am and 4 pm to 6 pm are considered to be the peak traffic hours.

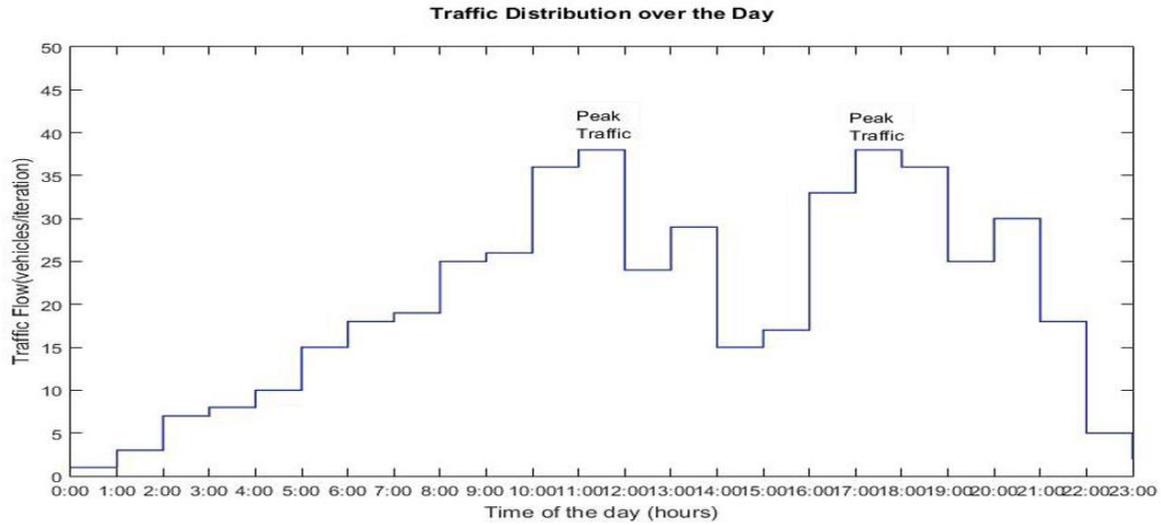


Fig. 11. Traffic Flow on a Lane throughout the Day Showing the Peak Traffic Hours.

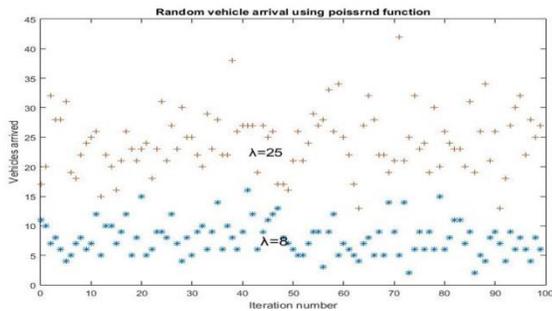


Fig. 12. Random Distribution of Vehicle Arrival.

### B. Comparative Analysis

Performance of the proposed FACS is evaluated by comparing it with the PTCS and TDCS. The pre-timed control system (PTCS) is considered to have a regular green light switching sequence and fixed green time of one minute irrespective of the traffic conditions. This is the traditional system which is mostly implemented at intersections. The traffic density-based control system (TDCS) is designed to switch green light between lanes and adjust the green light time in pre-defined steps of half, one and one and a half minute according to the vehicle density at lanes. The proposed fuzzy adaptive control system (FACS) decides the lane sequence and green time by fuzzification of inputs and application of rules from the designed rule base. The output from the inference engine is de-fuzzified to generate priority degree and green time for lanes.

### C. Simulation Scenario

The three systems PTCS, TDCS and FACS considered for performance evaluation are simulated under same traffic conditions for each hour of the day in ten observation sets of 100 iterations each. The traffic distribution on all the lanes of the intersection is identical and varies in accordance with the time of the day as in Table I. Emergency vehicles are assumed to enter any lane randomly and the probability of detecting an

emergency vehicle is more during the peak traffic hours. A random pedestrian wait time varying from zero to maximum value of GT is generated for each lane.

TABLE I. TRAFFIC DENSITY ON LANES FOLLOWING POISSON DISTRIBUTION

Time of the day (hours)	Value of $\lambda$	Traffic distribution (vehicles /time interval)
00:00-5:00 22:00-23:00	8	1-15
6:00-7:00	10	3-20
8:00-9:00 14:00-15:00 20:00-21:00	15	8-25
10:00-11:00 16:00-18:00	25	16-40
12:00-13:00	18	10-28
19:00-20:00	20	14-30

## IV. RESULTS AND DISCUSSIONS

Simulations are performed through MATLAB codes. Traffic on lanes for each hour of the day is simulated in ten observation sets of 100 iterations each. The average value of these ten observation sets is considered and results are plotted. Performance analysis is done on the basis of percentage of vehicles left on a lane, number of times emergency vehicle is addressed and prioritized for clearance and on the basis of giving way to pedestrians with the maximum wait time to cross the lane. The obtained results are comparatively analyzed and discussed.

### A. Performance Analysis on the basis of Percentage of Vehicles Left on a Lane

Simulated results of the three systems considered for performance analysis are shown in Fig. 13. The percentage of vehicles left on a single lane when the systems were simulated for ten sets of 100 iterations each at each hour of the day. The

simulation result of vehicles left on a single lane is clearly represented in a graphical manner with x-axis representing the time of day in hours, y-axis representing the PTCS, TDCS and designed FACS systems considered for comparison and z-axis shows the percentage of vehicles left on the lanes. PTCS shows the worst performance with approximately 50% vehicles left on lanes in the peak traffic hours of the day. TDCS shows an improved performance with average of 25% vehicles left in the peak traffic hours. The designed FACS shows the best clearance with less than 5% vehicles left in the peak traffic hours and full clearance in the less and moderate traffic condition.

**B. Performance Analysis on basis of giving Highest Priority to Emergency Transit**

Another important criterion to analyze the system performance is the number of times highest priority is given to the lane on which emergency transit is detected or in other words we can say that the emergency transit is addressed as soon as it is detected on a particular lane. Emergency vehicle is assumed to arrive at any lane of the intersection randomly with a certain probability. The simulation results obtained are shown with the help of a bar graph in Fig. 14. The designed FACS shows 100% performance in addressing the Emergency vehicle at all traffic flow conditions throughout the day irrespective of traffic flow condition. The simulation result obtained for PTCS and TDCS clearly signifies that they are not able to address emergency transit effectively.

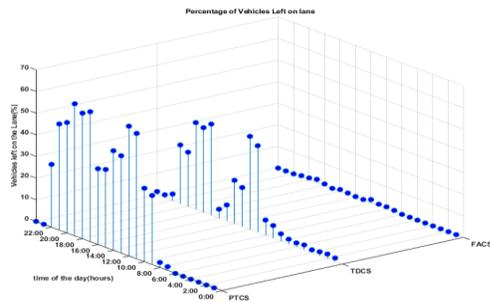


Fig. 13. Percentage of Vehicles Left on Lanes.

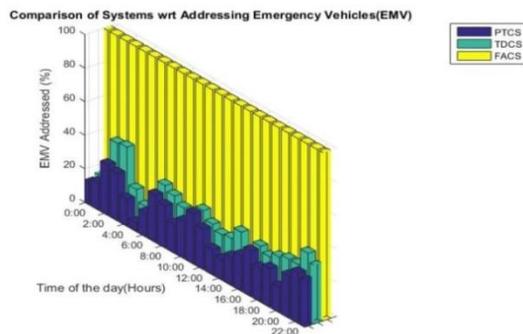


Fig. 14. Comparison of Percentage of Times Emergency Transit is addressed.

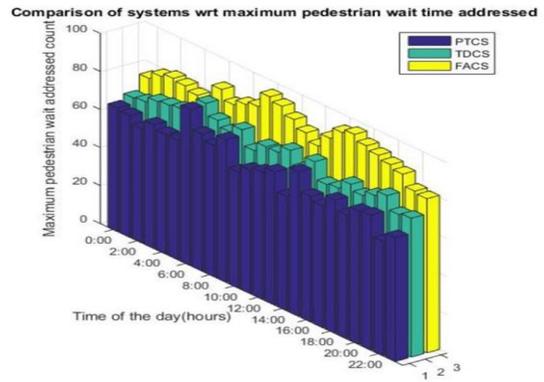


Fig. 15. Comparison of Percentage of Times Maximum Pedestrian Wait Time is addressed.

**C. Performance Analysis on the basis of giving way to Pedestrians**

To evaluate the performance of the designed system with respect to assisting pedestrians waiting at the intersection, the PTCS, TDCS and FACS systems are simulated in ten sets of 100 iterations for each hour of the day. Fig. 15 illustrates the measure of number of times the lane with pedestrians waiting for maximum time is given highest priority for red light to allow pedestrians to cross. The data plotted for each hour of the day is an average of the values obtained in ten observation sets of 100 iterations each. The designed FACS shows maximum clearance of pedestrians with highest waiting time and the performance of the system is better even in the peak traffic hours.

**V. CONCLUSION**

The proposed FACS performs better than the PTCS and TDCS due to its flexible design. The simulation results clearly show that the designed system gives better clearance to vehicles, emergency transit and also to pedestrians in all traffic flow conditions throughout the day. This system can be realized and implemented on any major traffic intersection to address all types of movements and enhance the traffic as well as pedestrian handling capability of the intersection.

In future these smart intersections can be interconnected through the major routes of the city such as routes leading to hospitals to give a thorough passage to emergency transit.

**ACKNOWLEDGMENT**

The authors are grateful to SHUATS, Prayagraj (formerly Allahabad) for providing the opportunity to write this research paper.

**REFERENCES**

- [1] Ali MAH, Mailah M, Jabbar WA, Moiduddin K, Ameen W, Alkhalefah H. Autonomous Road Roundabout Detection and Navigation System for Smart Vehicles and Cities Using Laser Simulator–Fuzzy Logic Algorithms and Sensor Fusion. *Sensors*. 2020; 20(13):3694.
- [2] Agrawal A, Paulus R. Intelligent traffic light design and control in smart cities: a survey on techniques and methodologies. *International Journal of Vehicle Information and Communication Systems*. 2020;5(4):436-81.

- [3] Guerrero-Ibáñez J, Zeadally S, Contreras-Castillo J. Sensor technologies for intelligent transportation systems. *Sensors* 2018;18(4):1212.
- [4] Zadeh, Lotfi A. "On fuzzy algorithms." In *fuzzy sets, fuzzy logic, and fuzzy systems: selected papers By Lotfi A Zadeh*, pp. 127-147. 1996.
- [5] Koukol M, Zajíčková L, Marek L, Tuček P. Fuzzy logic in traffic engineering: a review on signal control. *Mathematical Problems in Engineering*. 2015 Jan 1;2015.
- [6] Rahman SM, Ratroun NT. Review of the fuzzy logic based approach in traffic signal control: prospects in Saudi Arabia. *Journal of transportation Systems engineering and information Technology*. 2009 Oct 1;9(5):58-70.
- [7] Abdel Nasser H. Zaied, Woroud Al Othman "Development of a fuzzy logic traffic system for isolated signalized intersections in the State of Kuwait", *Expert Systems with Applications: An International Journal*, Volume 38 Issue 8, 9434–9441, August, 2011.
- [8] Alam J, Pandey MK , 'Development of Intelligent Traffic Light System Based On Congestion Estimation Using Fuzzy Logic' *IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 3, Ver. VI ,May-Jun. 2014, pp 36-44.
- [9] Ge, Yan. "A two-stage fuzzy logic control method of traffic signal based on traffic urgency degree." *Modelling and Simulation in Engineering* 2014.
- [10] Alam J, Pandey MK. Design and analysis of a two stage traffic light system using fuzzy logic. *J. Inf. Technol. Softw. Eng.* 2015;5(03).
- [11] Rocha, J., Martínez, S., Menchaca, J., Villanueva, J., Berrones, M., Cobos, J. and Agundis, D. 'Fuzzy Rules to Improve Traffic Light Decisions in Urban Roads', *Journal of Intelligent Learning Systems and Applications*, Vol. 10, pp. 36-45, 2018.
- [12] Vogel, Alan, Izidor Oremović, Robert Šimić, and Edouard Ivanjko. "Fuzzy Traffic Light Control Based on Phase Urgency." In *2019 International Symposium ELMAR*, pp. 9-14. IEEE, 2019.
- [13] M. Firdous, F. U. Din Iqbal, N. Ghafoor, N. K. Qureshi and N. Naseer, "Traffic Light Control System for Four-Way Intersection and T-Crossing Using Fuzzy Logic," *2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, Dalian, China, 2019, pp. 178-182.
- [14] Onoriode UM, Guo T, Pan S. Division of Green Time for Adaptive Traffic Signal Control Method based on Fuzzy Logic. *International Journal of Transportation Systems*. 2019;4.
- [15] Jha, Mohit, and Shailja Shukla. "Design Of Fuzzy Logic Traffic Controller For Isolated Intersections With Emergency Vehicle Priority System Using MATLAB Simulation." *arXiv preprint arXiv:1405.0936* (2014).
- [16] Homaei, Hamed, S. R. Hejazi, and Seyed Ali Mohamad Dehghan. "A new traffic light controller using fuzzy logic for a full single junction involving emergency vehicle preemption." *Journal of Uncertain Systems* 9, no. 1 (2015): 49-61.
- [17] Shelke, M., Malhotra, A., & Mahalle, P. N. "Fuzzy priority based intelligent traffic congestion control and emergency vehicle management using congestion-aware routing algorithm" *Journal of Ambient Intelligence and Humanized Computing* (2019) doi:10.1007/s12652-019-01523-8.
- [18] W. K. Saad, Y. Hashim and W. A. Jabbar, "Design and Implementation of Portable Smart Wireless Pedestrian Crossing Control System," in *IEEE Access*, vol. 8, pp. 106109-106120, 2020, doi: 10.1109/ACCESS.2020.3000014.
- [19] Pau, Giovanni, Tiziana Campisi, Antonino Canale, Alessandro Severino, Mario Collotta, and Giovanni Tesoriere. "Smart pedestrian crossing management at traffic light junctions through a fuzzy-based approach." *Future Internet* 10, no. 2 (2018): 15.
- [20] Aria, Muhammad "New fuzzy logic system for controlling multiple traffic intersections with dynamic phase selection and pedestrian crossing signal." *J. Eng. Sci. Technol* 14 (2019): 1974-1983.
- [21] Gerlough, Daniel L., and Andre Schuhl. "Use of Poisson Distribution in Highway Traffic. The Probability Theory Applied to Distribution of Vehicles on Two-Lane Highways." (1955).

# Computer Research Project Management

## Towards ontology based approach for Research Projects

Lassad Mejri<sup>1</sup>

Jouf University – Saudia Arabia  
College of Computer Science & Information  
Carthage University  
Faculty of Science in Bizerta, Tunisia

Henda Hajjami Ben Ghezala<sup>2</sup>, Raja Hanafi<sup>3</sup>

National School of Computer  
University of Manouba  
Tunisia

**Abstract**—Most research project managers, laboratories directors, young researchers at the beginning stage of thesis or professional research projects leaders are well effective at dealing with planned, scheduled events — they know how to function in conducting their research projects according to traditional knowledge areas of classical processes lied to time, cost, human resources, risk, stakeholders, and quality management. Unfortunately, they may have little specific training in selecting the best thematic of research. Indeed, they have no experience in identifying adequate research problems. Despite their motivation for the selected project and research thematic, they don't well master research problematic and how to deal with: Literature for the selected thematic of research: (Sources, Documents, reports and technical folders): List of problems encountered during the research theme conducting and how to make profit of the obtained solutions approaches for these kinds of research problems. - How to decide if this research theme and the list of connected problems are already resolved or not by any other research team. This paper aims to develop this idea and finally to propose ontology named "Onto-Research-Project" that formalizes all the domain knowledge of computer research projects. Our final goal is to propose an approach for historical research projects reusing. The output of this approach is a computer research project memory. In this way, we have to make use and to restructure the knowledge obtained from the research computer projects stored in the database "HAL-Archives-Nouvelles".

**Keywords**—Research projects; computer research project ontology; knowledge management; project memory

### I. INTRODUCTION

Research projects in general are much diversified. They occupied naturally many years of deeper studies and experimentations to make a valid proposal. They make use of many knowledge sources and experimented human resources. Research projects in the field of computer sciences and engineering require organized and methodological steps to achieve predefined goals. Indeed, these kinds of projects involve a conception phase which combines different reasoning modes, techniques and tools to design a final system which makes this kind of research projects more complex. Research projects in the domain of computer sciences and computer engineering often result in designing algorithms, models and approaches able to solve initial research problems. These multiple problems generally involve knowledge about different concepts, terms, languages, and vocabularies. In general [1], anthologies play now a major role in the

representation, organization and in the modeling of different and heterogeneous knowledge. Their main objective is to formalize the knowledge of a domain and thus add a semantic layer to computer systems and applications. In addition, the development of a new ontology makes it possible to explicitly represent the knowledge of a domain by means of a formal language, in order to be able to be manipulated automatically and shared easily.

Indeed, ontology consists of a set of concepts organized using hierarchical and specialized relationships representing a means of expression, sharing and reuse of knowledge, usable by all actors involved in the project. In computer engineering projects, construction methods and software techniques occupy an important place. Moreover, this domain makes use of many concepts, terms, languages, processes, models and methods of resolution. This fact involves the importance of using ontology to structure and to model all the concepts, the diverse knowledge that we would like to model.

In research projects, most research project managers, laboratories directors, young researchers at the beginning stage of thesis or professional research projects leaders are well effective at dealing with planned, scheduled events—they know how to function in conducting their research projects according to traditional knowledge areas of classical processes lied to time, cost, human resources (research teams), risk, stakeholders, and quality management. Unfortunately, they may have little specific training in how to select the best thematic of research. Indeed, they have no experience in identifying adequate research problems. Despite their motivation for the selected project and the selected research thematic they don't master well research problematic and how to deal with.

This paper aimed at elaborating an ontology based approach to give a helpful tool dedicated to researchers in the domain of computer sciences and engineering. This approach makes use of ontology of the domain to generate an aid at many levels:

- To help young researchers to select their adequate research theme.
- To help them to identify the adequate research problems.
- To give an aid in literature phase of research.

- To look for different research suggestions and/or solutions proposed by researchers in historical research projects similar to the new project.

Our paper is organized as follows. After the introduction, Section 2 consists of the state of the art which is composed of two sub-sections: In the first Sub-section, we will describe both the main related works of project memory approaches and a discussion study.

In the second sub-section the ontology elaborating methodologies are reviewed and finally a comparative study between these methodologies is discussed. Section 3 presents the modeling phase which consists in models description and giving finally our domain ontology for research projects. Section 4 consists of a proposal of an approach based on this ontology. Finally Section 5 is assigned to the conclusion and opens future works.

## II. STATE OF THE ART

The state-of-the-art consists essentially of two parts: The first one focuses on project memory concepts and their utility for the knowledge capitalization purposes. The second one reveals a state of the art on the methods of ontological elaboration and a comparative study of the available methodologies. In the following, we introduce the major works in the literature associated with the project memory concepts.

### A. Computer Project Memory

The concept of "computer project memory" is not famous in literature compared with the general known concept of "Project Memory" or "Corporate memory". We try here to introduce a research study to underline the concept of "Computer Project Memory". Indeed, for the past 20 years, computers have literally invaded businesses. They have developed many computer services [2] in order to manage, conduct, support and follow computer projects.

In the context of managing a computer project, there are constraints inherent to the information system of a company.

At the first, we could underline the increased user requirements, in particular as regards ergonomics.

Secondly, we could refer to the additional difficulties brought about by computer technologies.

Finally, a computer project is characterized by an intrinsic difficulty since this type of project is related to a software complexity [3].

Hence, it is essential to refer to a method of project management. This method helps designers better conduct this type of project stage by stage and use well-defined modeling tools [4].

In addition, purely computer projects are quite varied in view of the diversity of their sub-domains; Such as databases, smart systems, design resources, and software engineering. Hence, there is a major interest to restructure the knowledge of the computer domain by the construction of a "computer project memory".

1) *Concept of project memory*: Let us now, looking for the term of project memory in general and not essentially lied to computer projects.

According to [5], a "project memory" is a very limited part of a capitalization exercise of a whole range of diverse experiences in the business. This memory aims at the traceability and the re-use of similar projects. It consists essentially of two components:

- The problem-solving context.
- The method of resolution.

In [6] the "project memory" was considered as a technique that approximates the meeting often done at the end of the project because it seeks to determine the same knowledge and lessons learned during the project. Furthermore, the "project memory" is established throughout the implementation of the project and not at the end.

According to [7] "project memory" can be defined as a memory of project knowledge. It is an appropriation of the knowledge acquired over time of the activity of the company. The development of project memory is a procedure whose implementation requires some basic assumptions:

- The Project Memory is essentially formed and represented by database structure.
- The project memory is a tool for sharing accessibility based on the demand of this database.
- The project memory refers to the principle of community: "an individual effort at the service of the community".

According to [8] a project memory is the procedure that keeps track of actions performed in the arrangement of a project. It makes it possible to find the person responsible for a decision taken beforehand. This technique also allows the reuse of projects that are already realized in order to reduce the cost and the time.

According to [9] "a project memory" must contain in the first part the information describing the problem-solving and the decision-making. The second part represents the characteristics and the context of the said project.

Through these different definitions, we can consider "project memory" as the storage and the retention processes of the history during the realization of a given project. It therefore contains all the information, know-how, knowledge and skills that will be used by experts to achieve project goals.

2) *Synthesis of computer project memory concepts*: During our research study, we noticed that the researchers in memory projects domain based their research on two main directions:

Direction 1: Typologies of memories (classifications).

Direction 2: Project memory models.

a) *Typologies of memories (classifications)*: We present in the table below (Table I) a summary study of the

classifications of corporate memories given in literature. The Table I presents the kind of memory and the knowledge resources manipulated by each kind of organization memory. Corporate memory seems to be a solution for preserving and sharing knowledge that has come from different sources and fields. In addition, we notice that the «project memory» is almost present in all the classifications that we mentioned in Table I.

This shows us the importance and usefulness of this memory in the knowledge management.

TABLE I. SUMMARY OF THE CORPORATE MEMORY CLASSIFICATION

Classification	Type of Memory	manipulated data
<i>Marinella 's &amp; all classification [10]</i>	Documentary memory	Documents
	Memory based on case	Problems, solutions, experiences.
	Memory based on knowledge	Knowledge, text
	hybrid Memory	Knowledge, text, data, documents, ontology, annotations
	groupware Memory	Interventions, messages, mails
<i>Classification Of André [11]</i>	Semantics memory	knowledge, symbols, logical references
	Procedural memory	methods, strategies, structures, procedures
	Episodic memory	facts, episodes, events
<i>Classification Of Pominant [12]</i>	Project memory	Projects, experiences, tracks
	Organizational memory	Competencies, know-how
	Technical memory	experiences, papers
<i>Classification of Dieng et al [13]</i>	Memory of profession	Experiences, professions,
	Company memory	Document, know-how, know
	Individual memory	Contact information, judgment, historic...
	Project memory	Experiences, results, solutions
<i>Classification of Ben Sta [9]</i>	Long-term memory	long term information
	Short term memory	Short term information
<i>Classification of Bascans [14]</i>	Business memory	documents, tools, reference,
	Corporate memory	business, products, partnership
	Individual memory	statue, skills, know how
	Project memory	history, results, activities, experiences

Since a project is a unique process that consists of a set of coordinated and controlled activities, knowledge, information and experiences. The concept of “project memory” seems to be the best way to contribute efficiently to solve our research problem which consists to manage experiences and knowledge about past research projects in the way to resolve the new project.

*b) Project memory models:* Several project memory models are presented in the literature. Inspired from, we present our classification in (Table II). This classification is based on a set of criteria chosen by us:

- Decision making: this criterion permits to verify whether the proposed model takes into account the decision-making process in research project.
- Project context: is the set of elements characterizing the organization & environment factors of project. For each model proposed we will see if it guarantees the capitalization of the project context.
- Rationale design: is the problem solving process, this criterion checks if the model allows or not the capitalization of the logic design.
- Project characteristics: describes the set of elements: actors, materials, tools, processes and documents related to the project.
- Reuse: it expresses the possibility of reusing the project memory in future.
- Generic or specific: Checks if the model can be used for any type of project or it is simply specific to only one kind of project.

According to Bekhti [16], project memory is composed of two parts: the first one presents the design logic and the second presents the project context.

Harani [17] has proposed another generic model that is composed of three models (product model, process model and resource model). His proposal is structured on three levels: meta-model, specification and realization.

Labrousse [15] has proposed a model that is based on the integration of these concepts: product, process and resource. This model is defined by the roles played by these different concepts.

TABLE II. SUMMARY OF THE PROJECT MEMORY MODELS

Model	decision making	project context	design logic	project feature	reuse	generic / specific
<b>Labrousse [15]</b>	No	No	Yes	No	Yes	generic
<b>Bekhti [16]</b>	Yes	Yes	Yes	No	Yes	generic
<b>Harrani [17]</b>	No	No	Yes	No	Yes	generic
<b>Sta [9]</b>	No	Yes	Yes	No	Yes	generic

The set of models presented above could help to capitalize knowledge. This study allows us to note that:

- All the models are well-versed in the notion of reusing; they are generic models that could be profitable for all types of projects.
- The design logic is the most important component in the model. Effectively during the project leading, project team affronts many problems according to the design phase. So, all the models favor the capitalization of the design logic.
- No models allow the capitalization of project characteristics and subsequently they do not favor the documentation.
- Despite its importance in conducting projects, decision making process seems to be neglected by these models.
- Finally, we observe the absence of a model which guarantees the capitalization of all these elements at the same time: project context, project characteristics and design logic.

In the way to characterize correctly a computer research project and to organize and to structure the concept of computer project in general, it is very important at this stage to elaborate domain ontology of computer research project. Thus, we need first to have an idea about methodologies used to elaborate a useful ontology.

#### B. *Ontology Construction Methodologies (State-of-the-Art)*

In ontology engineering, the choice of methods, techniques and tools for the ontology construction process is an important step. Indeed, several methodological approaches have been proposed [18] to guide this process. We can distinguish four main categories of ontology development approaches:

- **Ontology construction approaches from zero:** For these methodologies, the sources of knowledge used for ontology construction are given by the domain experts [18]. Knowledge engineers are based on specific knowledge acquisition techniques such as brainstorming meetings, interview of experts, discussion, and knowledge extraction techniques, etc.
- **Text-based construction approaches:** This kind of methodology consists essentially of exploiting the textual resources [19] such as the projects documents and the lessons learned reports. They are generally applied for the construction of domain ontology.
- **Approaches based on the reuse of already existing ontology:** These approaches consist in exploiting the entire or a part of the knowledge contained in already developed ontology [20].
- **Crowd sourcing based approaches:** These approaches provide the outsourcing and the exploiting of tasks that are already performed by employees [18]. Knowledge engineers based their knowledge extraction on the direct observation of the tasks execution done effectively by employees. The essential goal is to formalize employees' experiences.

In our research work, we will be interested in the approach of building ontology from zero. Indeed, the construction of the proposed ontology follows an autonomous approach which is not based on any existing ontology or the updating of any other already constructed ontology.

Moreover, the knowledge and skills defining the essential components of the proposed ontology did not come from textual resources but from the deeper analysis of the domain of computer research projects.

For all the reasons mentioned above, we found ourselves obliged to adapt the construction approaches from zero to develop our domain ontology. In the following, we introduce the major works in the literature associated with this kind of approach.

*1) Description of the main approaches from zero:* Several works in the literature are oriented towards this type of approach in what follows we have discussed some proposals.

*a) Two-steps Methodology:* As its name indicates, this methodology is composed of two steps: 1) The knowledge organization and 2) the knowledge acquisition and reuse that allow the users collaboratively exploiting the knowledge [16]. In the beginning, a Core Reference Ontology (CRO) describing the generic concepts and relations according to the formalized requirements is identified. After, a Domain Specific Ontology (DSO) is specialized. Only two steps are not enough to describe a complete construction processes. In fact, this methodology is neither documented nor evaluated.

*b) On-To-Knowledge Methodology (OTKM)[16]:* It is a methodology based on acquired experiences of business activities. It is composed of four stages from identification, to documentation [21]. The stages are given implicitly and not explicitly [18]. The activities are few detailed (just a general description of the steps is given and no precision in the choice of components).

*c) The Methodology Proposed by Fox and al [16]:* This methodology is used in the context of the TOVE project (Toronto Virtual Enterprise). The application of this methodology is motivated by problems which are formulated under form of informal questions that ontology should answer. This methodology has made it possible to develop complex projects in the field of business but remains limited because neither the different stages nor the techniques used are precisely described [22]. This methodology is adapted only to informal knowledge description.

*d) The Method Proposed by Noy [16]:* This methodology is an iterative construction method that includes seven stages. Although this methodology is precise and well detailed, it is still incomplete. Indeed, no formalization and evaluation step is given in the process of construction. In addition, the description of the stages and the activities seems complicated and requires being a domain expert to achieve the ontology elaborating processes.

*e) The Meth-Ontology:* It is the most widely used methodology in literature [16]. It is the adopted construction approach for many anthologies in different fields. In fact, this method is highly-precise [27]. Meth-ontology can be applied

in all areas, thanks to its flexibility. In fact, it can be applied in scratch or text approach.

In order to adopt an approach to construct our ontology, we will propose a comparative study between the methods already mentioned in the previous sub-section.

2) *Comparative study of ontology construction methodologies*: This comparative study is based on four criteria: these four criteria are selected in accordance with domain experts:

- **Process step**: this criterion informs on the way in which the construction process is defined: detailed, little detailed, or very detailed.
- **Level of precision**: the precision in the choice of the terms, relations and classes during the construction stages. This criterion differs from one method to another.
- **Application domain**: It serves to know in which domain this method has been applied.
- **Type of activity**: each process of construction is composed of a set of tasks or activities. Here, we have tried to determine the type of activity. Indeed, we can have a support activities, documentation, evaluation activities, etc.

This comparative study results in the choice of the “Meth-ontology” as a methodology for ontology elaboration. Indeed, “Meth-ontology” is the most precise of all the previous methodologies. In addition, this methodology offers several types of activities and among these activities we mention project management.

The main orientation of this research study is to propose ontology in the field of research computer projects and particularly in project management domain. Since “Meth-ontology” has a project management activity as an essential activity [16], and it permits to develop the ontology progressively by iterations, we have decided to use this methodology to build the proposed ontology.

It is in this context that we have proposed ontology for the domain of research computer projects. This methodology is incrementally elaborated:

- First we propose a modeling phase in which we elaborate a project model and a class project model. The model of a project defines the basic components of a project. The class model tries to target on the essential pillars of a class of projects. Our goal is to synthesize the characteristics and specific knowledge of a set of projects belonging to the same class: the same thematic of research unifying many different projects of research.
- Secondly, based on the previous models, we try to elaborate progressively the ontology of the domain of research computer projects. In this way, we elaborate first a kernel-ontology which represents the basic concepts known as essential to define a research project and we finalize our ontology step by step by

adding branches and more details to well describe the domain of computer projects involved in research areas. So, our approach is called incremental approach which is mainly characterized by multi-intervention, documentation and iteration. In the next section, we will describe both the process of modeling of knowledge involved in Research computer projects and building ontology.

### III. KNOWLEDGE MODELING PHASE

We will describe both the process of modeling Project and class of projects.

#### A. Model of a Research Project

A research project model ‘Fig. 1’ underlines three main components of the research project in the computer sphere:

- The project description is a textual description (Abstract / Keywords of the research project/ Title of the project).
- The project Characteristics enumerate all the items which characterize the conduction and the management of this research project such as (Time allowed for the project/ Cost estimated for the project/ Project steps / Project size/ Stakeholders involved/ Deliverables/ Constraints/Human resources/ Scope of project/...etc.).
- The project Rationale Design or Logic Design specifies all the problems and sub-problems encountered in the process of analysis, design, implementation and test involved in the project. This component is essential for the project because it focuses on logic problems, suggestions and solutions proposed by different actors implicated in the project phases and thus must be memorized for further reusing in the context of REX (Return of Experience). These main research problems are attached to specific research problems within a class of research theme. It is this component which could be exploited in knowledge capitalization. Effectively, all the knowledge involved in problem specification, suggestions proposed during problem solving process, and retained solutions are part of this component.

#### B. Model of a Class of Projects

A research class project model underlines three main components of the class of projects (Fig. 2) in the computer research sphere:

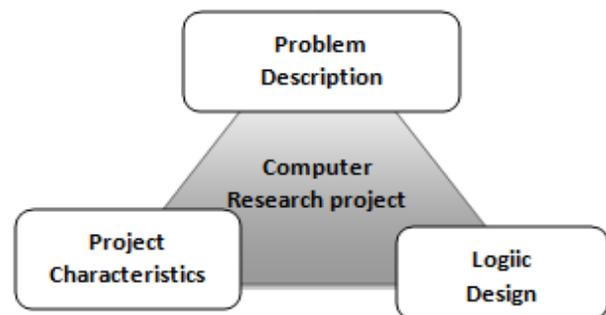


Fig. 1. Research Project Model.

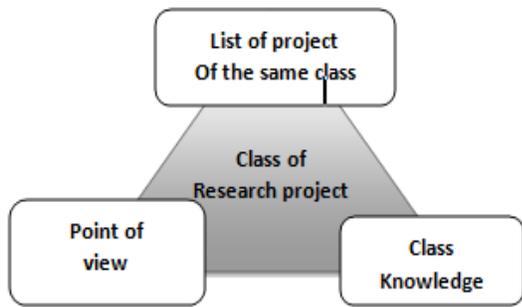


Fig. 2. Class Project Model.

- The List of projects is an extensive description of all the projects belonging to the same class and pre-classified by domain experts (experts in research computer projects area);
- The Class project Knowledge stores all the forms of knowledge which characterize the conduction and the management of this research project class such as (research thematic/ Scope of this class project/ Methodologies / Kinds of design architecture/ Kinds of research problematic/ Systems/ support documentation/Rex reports/ main solutions approaches/ Appropriate tools, etc.)
- The Point of view for class project specifies different viewpoints and different strategies to manipulate knowledge involved in a class of projects. This component gives different manners for exploiting the same knowledge in the class. The point of view is attached to one particular actor and differs from one actor to another according to the aimed goals.

### C. Model of Rationale Design

A rationale or logic design model underlines three main components of the project (Fig. 3) in the computer research sphere:

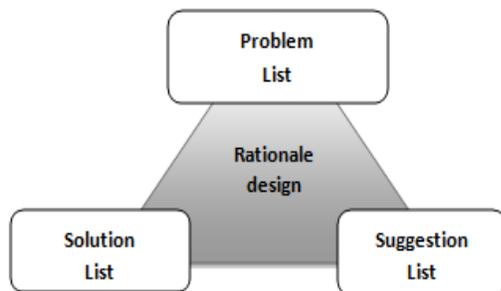


Fig. 3. Rationale Design Model.

- The List of problems is an extensive description of all the project research problems;
- The List of suggestions stores all the forms of suggestions introduced by researchers within the project area to solve the research questions or problems. The suggestion is a proposal to solve some research questions (research technique/ method of problem solving/ document/ tool/ algorithm/ strategy of solution/ issue of research/ etc.).

- The List of solutions specifies different solutions which could be adopted to solve a particular research problem.

### IV. PROPOSED DOMAIN ONTOLOGY: ONTO-RESEARCH COMPUTER-PROJECT

The proposal of a knowledge capitalization approach is the main goal of our current research study. This approach consists essentially of two processes:

- A knowledge formalization & acquisition process.
- A support decision for project management process.

The present paper is only concerned by the first process. It is composed of two phases: The phase of formalization and the phase of knowledge acquisition.

This process is relayed by the proposal of domain ontology which structures and organizes the great mass of the concepts and knowledge encapsulated in the proposed models.

#### A. Formalization Phase: Stages of Ontology Elaborating

In this paper, we proposed an ontological construction approach based on the methodology "Meth-ontology" which leads to a final version of our domain ontology. We will now describe in detail this approach, by applying carefully the methodology "Meth-ontology" which has been selected in the basis of a comparative study (i.e. Section II-B.2). Finally, we present a final version of the ontology (Fig. 10) with our proposed ontology validation approach.

The particularity of "Meth-ontology" is the possibility of the return on the steps preceding [25]. In what follows, inspired from "Meth-ontology", we will present the stages of the construction of our domain ontology:

- Step1: This step consists in building a glossary of terms containing all the domain knowledge that is useful and potentially usable for the construction of computer research domain ontology. This glossary includes concepts, instances, verbs and attributes. To do this step, we have met with domain specialists and experts to talk about computer projects. Fig. 4 gives a general idea on the knowledge areas recognized in PMBOK [26] reference as the essential rubrics to be considered in project management.
- Step2: In this step, we have built the first version of the ontology which presents the "classes' hierarchy": the hierarchy of concepts and terms obtained via the grouping, the categorization and the generalization of the different concepts studied (Fig. 5). This stage of modeling identifies three general Classes which are: the project description; the project characteristics; and the project logic design.
- Step 3: During this stage, we have created "relations between classes" by determining for each relation the type of relation and the classes to be connected (Fig. 6).
- Step 4: This step "instantiation of the ontology" consists in creating (individuals, instances) of the

classes of general concepts. Each complete instance is a new case: a project. To achieve this stage of instantiation (Fig. 7) we used the database "Archive Hal" of computer research projects named "HAL-Ouvertes".

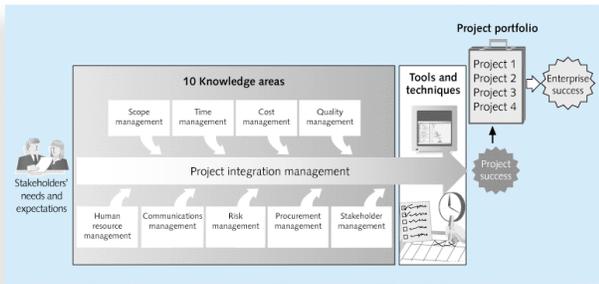


Fig. 4. Knowledge Areas of Project Management [26].

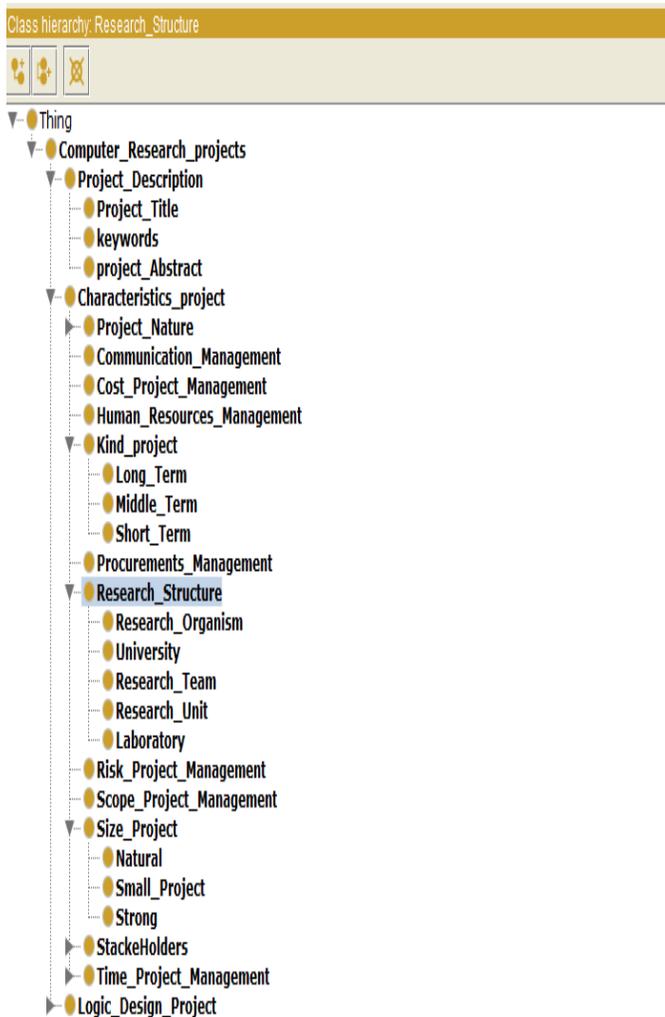


Fig. 5. Kernel Ontology: Class Hierarchy.

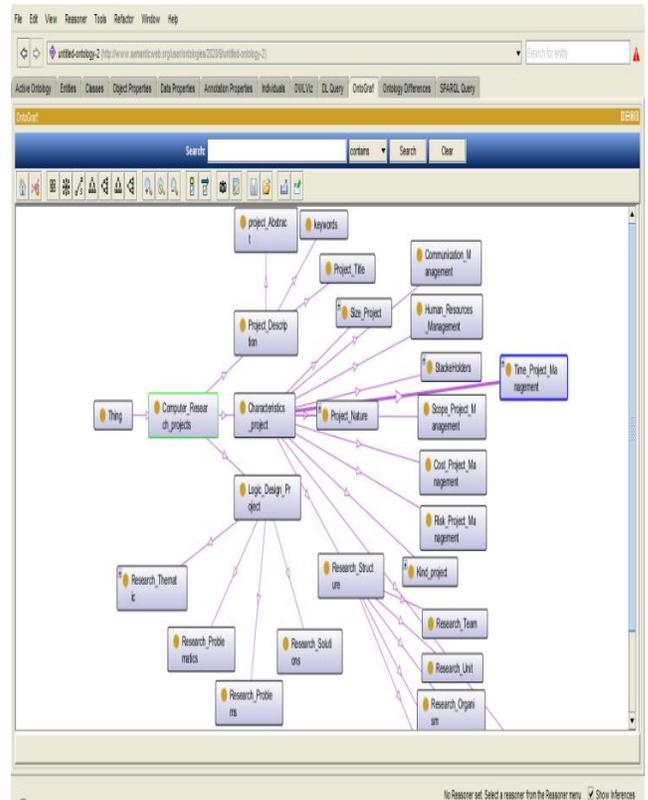


Fig. 6. Extract of Classes relations.

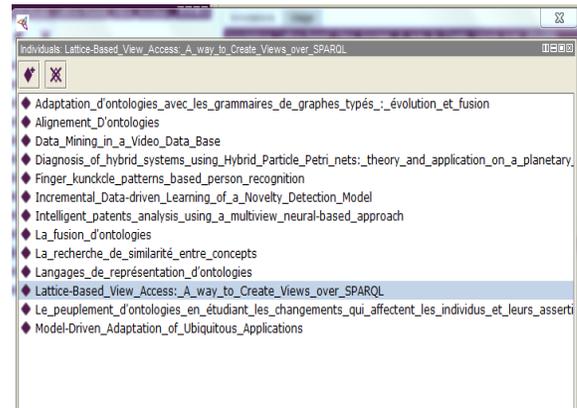


Fig. 7. Example of Individuals of Research Projects.

- Step 5: This step provides a detailed description of previously identified relationships, attribute concepts, and constants. We have used the research projects of the "Archive HAL" and the structure of documents to define some classes and some attributes (Fig. 8).
- Step 6: "Object properties". It concerns the description of formal properties, rules and axioms relating to the various elements of ontology. During this stage we will describe the set of properties and relations between the created individuals (Fig. 9).

Concepts	Detailed Description	Format of Concept
Project Description	An abstract of project which describes textually a project	String of characters
Project Title	A brief title identifying the project	String of characters
Keywords	The main keywords max of seven items	A list of 7 strings
Project Characteristics	A set of project main attributes lied to PM knowledge areas	A List of Characteristics
Project Nature	Class of a project	Item belonging to [professional/Undergraduate/PostGraduate/Industrial/Research]
Communication Management	Aspects related to Communication Area of PM	[Communication Tools/Communication Methods/Communication Actors/...]
Cost Management	Aspects related to Communication Area of PM	[Earned Value/ Actual Cost/Planned Value/Cost Variance/Cost Performance Index/Schedule Variance/Budget At completion/Estimate To Complete/Revised Budget/...]
Time Management	Aspects related to Time Area of PM	[First Start/ First Finish/ Late Start/ Latest Finish/ Critical Path/ Task Durations/ Float Activity/ Activity definition/ Activity resources Estimation/Activities Scheduling/...]
Human Resources Management	Aspects related to HR Area of PM	Details and processes of Human Resources PM
Risk Management	Aspects related to Risk Area of PM	Details and processes of Risk PM
.....	...etc.....	...etc.....
Kind Project	Type of project	Item belonging to [Short term/Long Term/Medium Term]
Research Structure	Organization tutoring the project	[ Laboratory / University / Team Project/ Industrial Office / Research Organism / Research Unit / Association...]
Scope PM	The domain of Research	[Artificial Intelligence/ Data Science/ Data Mining/ Software Eng / Networks / Operating Systems / Design Methodologies/ Knowledge Eng/ Knowledge Management /Neural Networks..]
Size Project	The Width of project	[Small / Strong / Medium]
Deliverables Project	The Outputs attended for project	[Report / Folders / Product / service / Results/ Lessons learned Reports/ Recommendations/ Analyses]
Stakeholders	The actors of the project	[Sponsors/Customers/Users/Project Manager/ Project Team/ Providers/Coaches ...]
Project Manager	The chief of the project	String specifying the position/ responsibilities/role
Project Team	The team responsible of achieving project	List of members and assigned roles
...etc.....	...etc.....	...etc.....

Fig. 8. Glossary of Concepts.

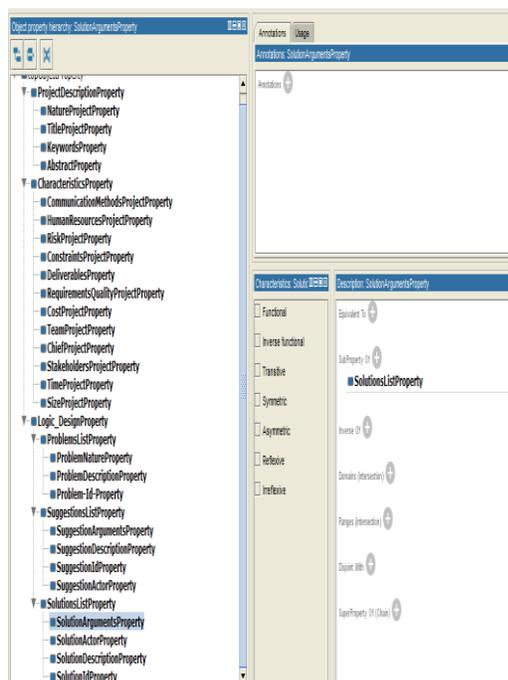


Fig. 9. Objects Properties.

- Step 7: This step concerns the detailed description of instances and relations between instances, classes and properties (Fig. 10).

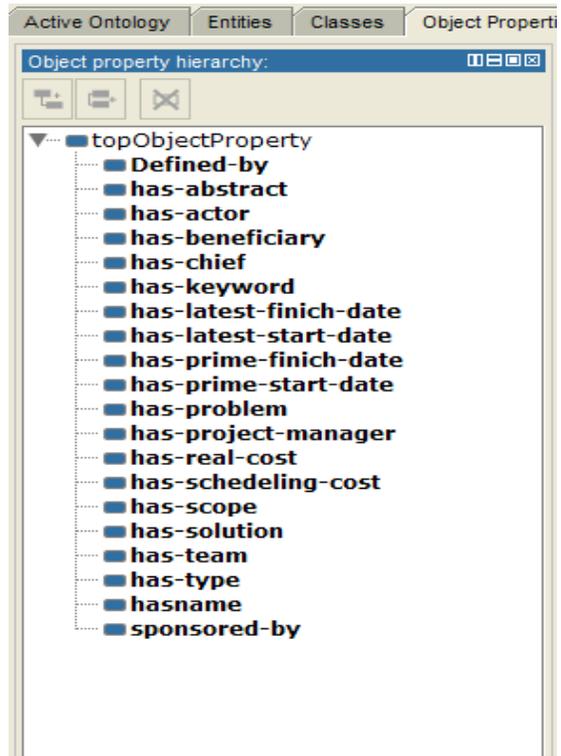


Fig. 10. Data Properties.

Validation ontology plays an important role during the creation and updating of ontology [27] to obtain a final and suitable ontology version (Fig. 11). This phase is done according two validation techniques: a structural and semantic validation [23], [28], [29], [30], [31], [32].

### B. Acquisition Phase

The phase of project knowledge acquisition is essentially the acquisition of knowledge related to projects already achieved and completed. The project manager or one of the members of the project team will instantiate the set of concepts already introduced in the proposed ontology. The knowledge management is a complex process which requires many strategies [24].

Indeed, the scope, the characteristics and the rationale design describing each project will be stored. The list of collected projects play a main role in the decision support phase after, since they will be used for decision-making concerning the new projects in question.

In order to validate finally our approach and to test the functionalities offered by the aimed decision support system, we will choose to work on a specific type of computer project called "research projects". The choice of this type of projects is argued firstly by the fact that I'm actually a tutor of a young researcher and I'm aware of the problems and difficulties that any researcher can encounter when carrying out his project. Then, tests and applications on this type of project always still valid for the other projects type.

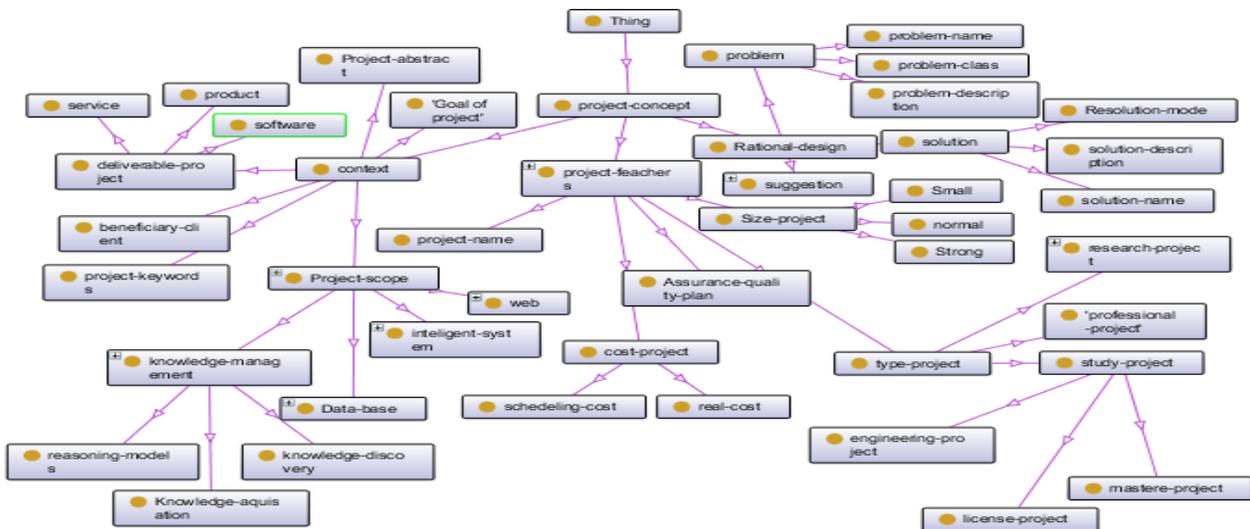


Fig. 11. Proposed Computer Domain Ontology Version.

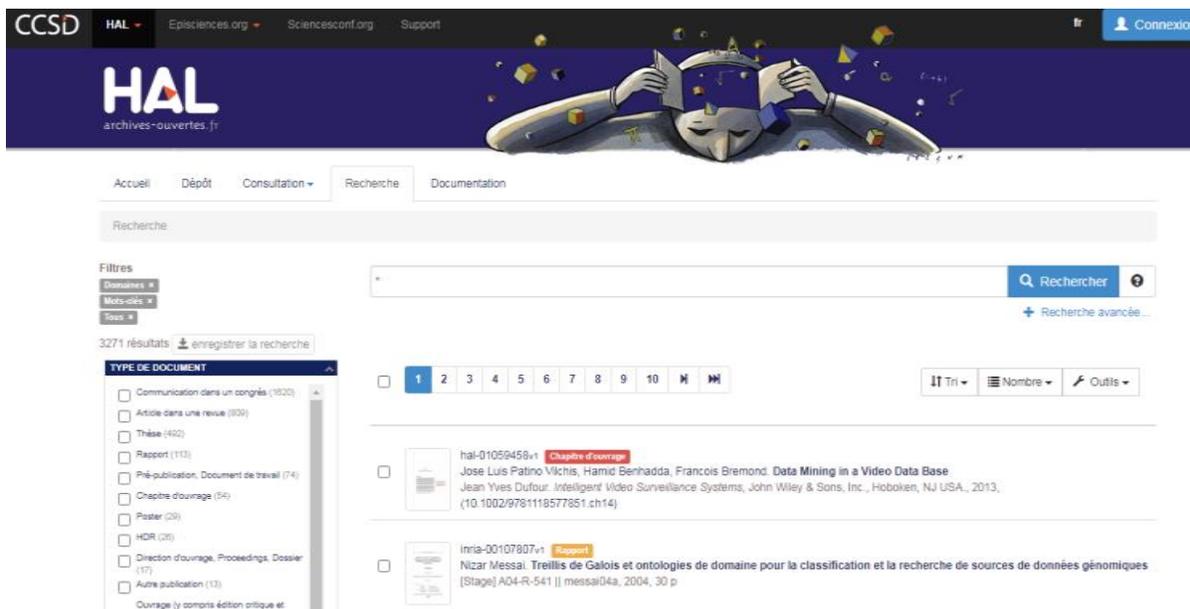


Fig. 12. Interface for Research Projects.

In this context we started with the construction of the knowledge base of the future system. This base is the results of an accumulation of projects published and validated in the Hal archive (almost 200 projects) structure (Fig. 12). We choose to work with 10 project scopes such as (ontology, database, big data, datamining, artificial intelligence, Networks, etc.).

#### V. TOWARDS A FUTURE SUPPORT DECISION APPROACH

This approach is essentially composed of two processes:

- Formalization and acquisition of knowledge process.
- Project management assistance process.

The First process was described above in the precedent section and results in modeling of knowledge involved in

research computer projects. This process is articulated essentially around the construction of the ontology of the domain of computer research projects concepts. The second process of assistance of project management is the object of this section and I will just introduce this process because it is yet in progress. We should give the general architecture of the target system (Fig. 13). This system aimed at supporting the decision making about research computer project. According to this goal, the project manager and the young researchers must be assisted by the system to make the convenient decision about their research topics. In the following, we will describe:

- The general description of the assistance process.
- The levels of help in decision making.
- The main modules of this system.

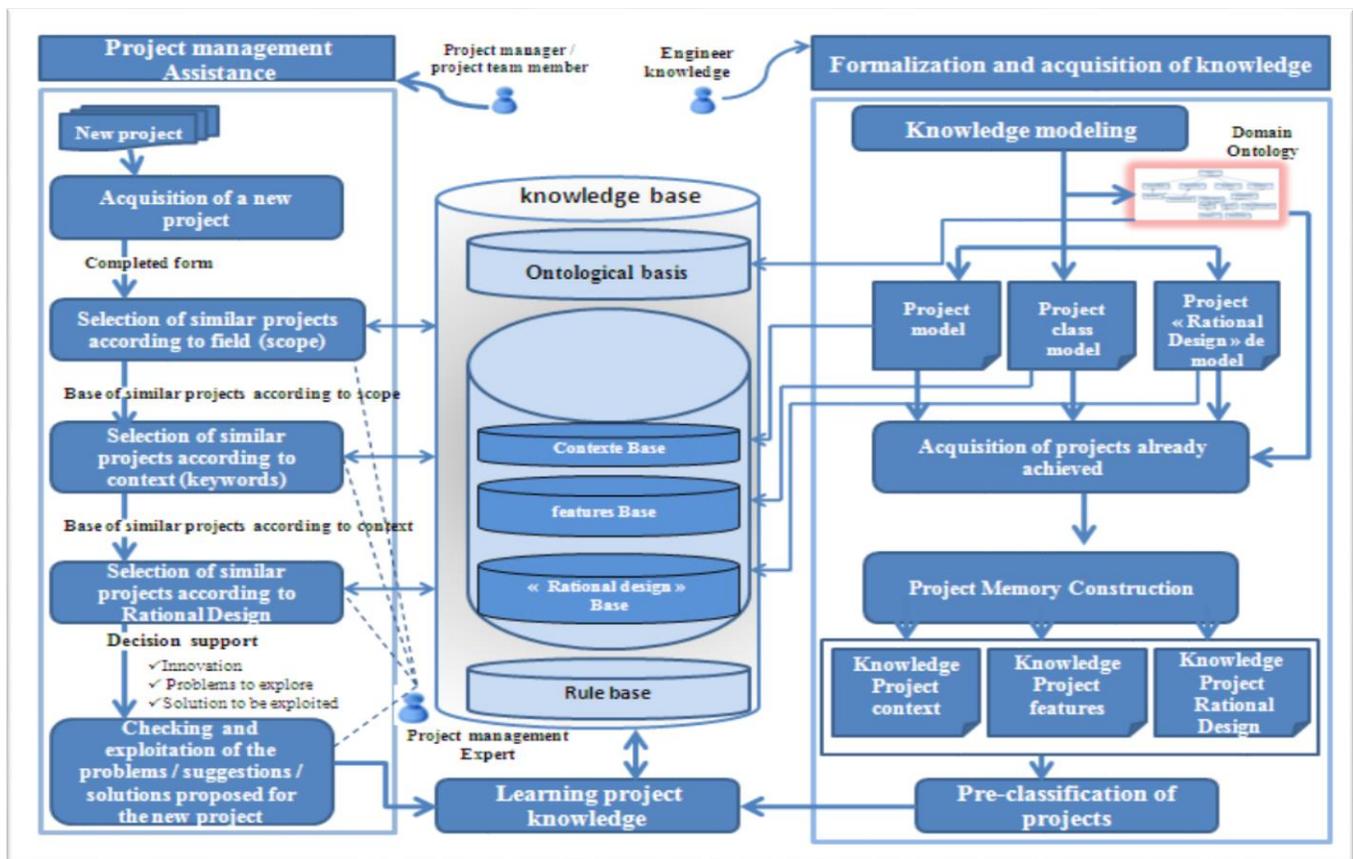


Fig. 13. Knowledge Capitalization Approach of Computer Research Project Memory.

A. General Description of the Assistance Process

This process begins with the acquisition of a new project and ends with the adding of this project, in the resolved form, to the project knowledge base. This process consists of four complementary sub-phases:

- Acquisition of a new project: The new project set by the project manager or the work team must be acquired as the first phase of the project management assistance process. In this situation, a form will be filled in containing all the characteristics defining this new project (context, characteristic, problems, Research theme, topics of research, actor ...).
- Selection of projects in the same scope: During this phase the list of projects belonging to the same project class will be displayed. The project manager (leader or member of the project team) must mention, from the beginning, the class (the scope) of the new project to be studied. Then, all the projects descriptions (characteristics, context and rationale design) of the class in question will be displayed. In this set of resulting projects, the rest of the manipulation and processing will be carried out. This phase of selection will reduce the workspace and search and will reduce the time of response.
- Selection of projects with the same context: this phase determine the set of projects that have the same

working context (according to project keywords ...). During the acquisition of new project the keywords will be introduced and they will be used to calculate the similarity between the keywords of new project and the list of keywords of the old memorized projects. Here a new sub-base of projects which have the same class and the same context will be created.

- Selection of projects according to rationale design: This phase consists of filtering, in the sub-base created in the previous phase. It consists of checking and exploiting of problems/suggestions and solutions. This phase consists of verifying and validating the suggestions and the solutions proposed in historical projects and thus to reuse them for the resolution of new projects. This phase is carried out by the project manager.
- Learning of the new project: When the project is treated according to proposed solutions for all the research questions and problems inherent to this project, it must be considered as a new project achieved successfully and then could be archived in the project base. This phase operates as a learning phase which permits to restructure the knowledge base by adding this project. The project hence added is considered as a new case able to be reused for the resolution of other future new projects.

### B. Levels of Help in Decision Making

In the literature, there are several approaches, tools and decision support systems. Inspired by the approaches of what we have studied and others that are in the literature, we decided to offer a guide to project leaders. The main objective of this guide is to automate our proposed approach and to offer help on several levels. The specificity of our decision support system is that it will:

- Offer a guide or help to the project manager during the realization of the project and not at the end.
- Help the project manager with multiple levels of help, from acquiring the new project to solving and learning phases and lessons learned.

In order to properly describe the future decision support system, we give, here, an outline of three levels of assistance:

- The first level of help: it is a help oriented service. It allows the enrichment, consultation, statistics, framing and contextualization of new projects to be processed.
- The second level of help: it is a help oriented decision making. This level presents the main help offered by the system considering that it will favor project manager decision. Indeed a project can be launched in the case where it is innovative (never already treated). So it will start from zero and it will be considered as an innovative project.
- The third level of help: it is considered as a help oriented decision support. This level of help is achievable if the problems underlined in the new project have already been treated in historical projects. In fact, the user will benefit from these kinds of projects by making profit of the method used in problem solving, the techniques of development and the strategies already adopted to deal with the project conducting. The issues and the research steps already used in historical projects can be profitable for the new project as well as the problem solutions, suggestions and even the obtained results. It is also useful to exploit the failed projects and inspired from untreatable problems to invoke new trends and new research deals. Success as well as failure signaled in historical projects should be of great interest for new projects.

### C. The Main Modules of the Assistance System

In this subsection, we will present the modules describing our proposed system and the application of involved levels of help in each module. Indeed, the system is defined by five modules: knowledge formalization module, acquisition module, project management assistance module, decision making module and learning module.

- Acquisition & formalisation modules

These two modules can be applied to two types of projects (new and historical) we choose to proceed by three steps: context acquisition, features acquisition and finally Rationale Design acquisition. This choice shows the specificity of the decision support approach. Indeed, each part will be handled

on a separate interface which facilitates access and management by different users.

The formalization of knowledge is done directly from the instantiation of the proposed domain ontology and the construction of a project memory.

- Project management assistance module

This module is the main module of the system. In this module, three levels of decision support are combined:

- The first level of decision support: selection of projects of the same class of the new project acquired. This selection is done thanks to a simple classification algorithm and requires that the achieved projects must be pre-classified (by project management expert).
- The second level of help is to determine the list of projects that have the same context. A similarity calculation algorithm will be applied to select projects that have a plausible similarity to the new project context. This level of help consists in selecting all the projects having similar keywords to the new project. The similarity rate adopted must be greater than or equal to 75%.
- The third level of help concerns the filtering of projects according to the proposed research problems contained in the new project.
- Decision making module

This module consists of making the final decision after the completion of the third level of filtering. Decision will be given automatically based on the result of the similarity calculation between the research problems of the new project and the set of research problems of the projects already selected from the knowledge base. In this situation, the user is concerned by one of three types of decision-making scenarios:

- First scenario of decision-making: in this situation, the similarity calculation rate is equal to zero. The user is informed that his project is an innovation and he must rely on his personal knowledge to solve his new project. In this situation the user can exploit the resulting information, knowledge and details in the first two levels of help. For example, he will see the list of problems encountered for projects in the same context. He can get an idea of the Rationale Design for this class of projects.
- Second scenario of decision-making: In this situation, projects that deal with the same type of problems are presented but they have not yet been solved (absence of the **solution**). The user can have an idea on the kinds of problems encountered for this type of research theme. In this case also the exploiting of the two other levels of help is possible.
- Third scenario of decision-making: In this case, the result of the similarity calculation shows that there are some projects that concern the same problems. In this situation, the user will solve the problems encountered

in his project based on suggestions and solutions of similar selected projects.

- Learning module

For this learning module two learning functions are to realize:

- The first function concerns newly resolved projects. Projects with their problems, their suggestions and their solutions will be added in the project knowledge base using a learning algorithm.
- The second function concerns the acquisition of rules to elaborate a classification rule base.

## VI. CONCLUSION AND FUTURE WORKS

Our paper has an essential objective which is to support young researchers and teams in the selection of their research project in the way to avoid ambiguity and redundancy in research projects. This support cannot be done only by selecting the convenient project but also by supporting the conducting of the selected project during its execution essentially in phases of literature and in important phases of analysis and conception. That is in this perspective, why our word aimed to develop a support system organized by many levels of help.

Naturally, our work necessitates to structure and to organize all the heterogeneous knowledge involved in computer projects in research fields. Thus, this important phase of knowledge modeling require to be well managed and processed. Then, when knowledge manipulated in the context of research computer project is collected, structured and well organized, an acquisition of a base of computer research projects is processed in the way to construct a project memory.

This paper is reserved to present the first process of knowledge modeling and acquisition. The models presented in this paper concern a model of computer research project, a model of projects' class and a model of project rationale design. All these models are of great benefits for knowledge structuring and organizing. After the modeling and the formalizing knowledge involved in the domain of computer research projects, the knowledge representation is a crucial mission. Thus, the ontology of the computer research projects domain was designed.

Validation ontology plays an important role during the creation and updating of ontology to obtain a final and suitable ontology version. This phase is done according two validation techniques: a structural and semantic validation. These two validation techniques are complementary to deal with an acceptable ontology. Evaluating ontology means checking and validating two aspects: structural aspect and semantic aspects. The validation of the structural aspect of ontology allows verifying the consistency and the coherence of a model to check. In this way, classes and sub-classes are verified according to criteria of consistency and coherence between them and to avoid redundancy.

The validation of the semantic aspects involves communication aspects between actors of different domains of

expertise. In this way, we proposed a validation approach based on two criteria:

- The first criterion: the Incremental validation of the ontology: the passage from one validation step to another results in an update [modification, deletion or addition] of the initial ontology.
- The second criterion: the Multi-intervention criteria: This approach is characterized by the intervention of several and different experts. Three experts are involved in the validation process:
  - The project management expert: He is an expert in the field of project management.
  - The project computer expert: He is an expert who masters all the concepts of computer projects.
  - The specialist in ontology engineering: this actor has a good command of all the tools and editors of the ontology.

Because the present paper was reserved to present the process of knowledge modeling, formalization and acquisition, different stages of ontology construction were given. We have also introduced here the general approach for exploiting ontology to construct a computer research project memory which could be after used by young researchers in computer science and computer engineering domains to help them to evaluate if their research themes and/or research problems proposed in their research projects are already treated by others before them or if they innovative.

Even, if their research projects are already treated, the approach introduced in this paper seems to help them to exploit the solutions and/or suggestions and issues and techniques proposed within the rationale design of historical projects archived to launch new issues or new approaches for solving the same problems or to process new problems. Although the approach seems interesting in the articulation of stages and main ideas and concepts involved, it still needs to be validated experimentally by its application on ontology of domain and on real research projects such the examples of HAL archives.

Then we have to implement in the future the modules proposed in our approach to validate the proposal and by the means of machine learning techniques we have to construct a knowledge base able to be exploited in helping young researchers in decision process. We have to validate and test the base knowledge. However, this part of work still insufficient it's always necessary to design approaches and to organize knowledge before implementation and tests.

For future work, we will focus on developing a prototype system to evaluate the feasibility of the whole approach.

## REFERENCES

- [1] J.Gherasim, M.Harzallah , G. Berio and P. Kuntz , "Comparative analysis of methodologies and tools automatic ontology construction from textual resources", LABSTICC, UMR 3192 CNRS, January, (2014).
- [2] N.Matta, G.Ducellieret and H. Atifi, "Learning from design projects: how to keep track and learn from knowledge produced in daily activity", ICD, University of Technology of troyes ,france (2016).

- [3] E. Lauraine, "IT project management", Digital business space, June (2017).
- [4] P. Collet, "Computer Project", University of Nice, France (2014).
- [5] Ch.Huang, W. liang, T.Tseng and R. Wong, "A rough set-based corporate memory for the case of ecotourism", Tourism Management Journal, Elsevier, Vol 47, pp. 22-33 April (2015).
- [6] F.Rauscher, N.Matta and H.Atifi, Hybrid System for Collaborative Knowledge Traceability An Application to Business Emails, In Proceedings of the 7th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management-Vol 3: KMIS, pp.260-267, Lisbon, Portugal,(2015).
- [7] J. : J.A.Duarte, "An Analysis Of The Recommended Knowledge For The Software Project Management Discipline", Thesis presented as part of the project management master's program, Polytech University, Madrid, June (2014).
- [8] L.Boubaker, L.Mellal, M.Djebabra, "Model DIK (Data - Information - Knowledge) Support tool for the development of project briefs", The Journal of Management Sciences 2010/3 (n ° 243-244), pp. 153-159. DOI 10.3917 / rsg.243.0153, (2010).
- [9] H.BenSta, "Contribution of the conceptual modeling to knowledge engineering management: application in the framework of the project memory", thesis Lille 1, (2006).
- [10] V.Marinela, L.Anica, I.Anica, "Organizational Memory: an Approach from Knowledge Management and Quality Management of Organizational Learning Perspectives", Amfiteatru Economic 11(26):473-481, June (2009).
- [11] A. André, "Organizational memory breaks with individual memory", Communication and organization [Online], 24 | 2004, posted online 19 December 2012, accessed on 01 October (2016).
- [12] J.Pomian, "Corporate memory, techniques & tools for knowledge management". Ed Sapientii, (1996).
- [13] R.Dieng, O. Corby, A.Giboin and M.Ribiere, "Methods and Tools for Corporate Knowledge Management",RR-3485,INRIA.inria-00073203, (1998).
- [14] J.Bascans, M.Chevalier, P.Gennero and Ch.Soul'e-Dupuy, "Adaptive organizational memory for automatic classification for information capitalization". 33rd Computer Congress of Organizations and Information and Decision Systems (INFORSID 2015), May (2015).
- [15] M.Labrousse, "Proposing a Unified Conceptual Model for the dynamic management of Corporate Knowledge", thesis of the central school of nantes specialty mechanical engineering, 13 July (2004).
- [16] S.Bekhti, "DYPKM: A Dynamic Process for Defining and Reusing Project Memory", Human Machine Interface [cs.HC], Troyes University of Technology, (2003).
- [17] Y.Harani, "A Multi-model Approach for the Capitalization of Knowledge in the Field of Design", thesis of the INPG, specialty in Industrial Engineering, November (1997).
- [18] F.Rauscher, N.Matta and H.Atifi, "Hybrid System for Collaborative Knowledge Traceability An Application to Business Emails", Second IFIP WG 12.6 International Workshop, AI4KM 2014, Warsaw, Poland, September 7–10, (2014).
- [19] A.Amarir, El.Benlahmer and L.Elhoussine, "The Methods of Building ontology from text", Conference Paper, The second day on Information Technologies and Modeling TIM'14, May (2014).
- [20] E.G.Caldorala, A.M.Rinaldi, "An Approach to Ontology Integration for Ontology Reuse" Conference Paper, IEEE 17th International Conference on Information Reuse and Integration, At Pittsburgh, Pennsylvania, USA, July (2016).
- [21] K. Drame, "Contribution to Ontology Construction And Information Retrieval: Application To Tthe Medical Field," thesis, Bordeaux University, France. ffnNT : 2014BORD0444 (2014).
- [22] J.Gherasim, M.Harzallah , G. Berio and P. Kuntz , "Comparative Analysis of Methodologies and Tools Automatic Ontology Construction From Textual Resources, LABSTICC, UMR 3192 CNRS, 8 Jan (2014).
- [23] B.Menaouera , S.Khalissab , B.Abdelbaki , T.Abdelhamid "Towards a new approach of support innovation guided by knowledge management: Application on FERTIA, 4th International Conference on Leadership, Technology, Innovation and Business Management, Procedia - Social and Behavioral Sciences 210, 260 – 269, (2015).
- [24] A.Amarir, El.Benlahmer and L.el houssine, "The methods of building ontology from text", Conference Paper, The second day on Information Technologies and Modeling TIM'14, May (2014).
- [25] M.Richard, X.Aimé, M.Krebs and J.Charlet, "LOVMI: Towards an Interactive Method For The Validation of Ontologies", INSERM UMRS 1142, LIMICS, F-75006, Paris, France ,IC, (2015).
- [26] <https://www.pmi.org/pmbok-guide-standards>, 2021 Project Management Institute, Inc.(2021).
- [27] G.Michael "Ontology Validation as Dialogue", 4.0 International (CC BY 4.0), eur-ws.org/Vol-2518/paper-WINKS3.pdf, (2019).
- [28] A.Yunianta et al, Methodology for Ontology Development on Data Integration (OntoDI), (IJACSA) International Journal of Advanced Computer Science and Applications, 2019.
- [29] S.Tartir,S.Amit,I.Arpinar and Young, "Ontological Evaluation and Validation, From Book Theory and Applications of Ontology" Computer Applications (pp.115-130) , (2010).
- [30] B.A.Asma, M.Silveira, C.Pruski, "An approach for content validation of an ontology by a system based on questions answers", CR SANTEC - Centre de Recherche Public Henri Tudor ,July (2013).
- [31] G.Leila,M.aya and D.faiza," Generation of A Questionnaire From A Domain Ontology,Conference paper, (2017).
- [32] G.Alex, B.P.Chavez and M.Davy,"Methodology to Design Ontologies from Organizational Models: Application to Creativity Workshops", 14 décembre 2020.

# Clustering of Association Rules for Big Datasets using Hadoop MapReduce

Salahadin A. Moahmmed<sup>1</sup>, Mohamed A. Alasow<sup>2</sup>, El-Sayed M. El-Alfy<sup>3</sup>

Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

**Abstract**—Mining association rules is essential in the discovery of knowledge hidden in datasets. There are many efficient association rule mining algorithms. However, they may suffer from generating large number of rules when applied to big datasets. Large number of rules makes knowledge discovery a daunting task because too many rules are difficult to understand, interpret or visualize. To reduce the number of discovered rules, researchers proposed approaches, such as rules pruning, summarizing, or clustering. For the flourishing field of big data and Internet-of-Things (IoT), more effective solutions are crucial to cope with the rapid evolution of data. In this paper, we are proposing a novel parallel association rule clustering approach which is based on Hadoop MapReduce. We ran many experiments to study the performance of the proposed approach, and promising results have been demonstrated, e.g. the lowest scaleup was 77%.

**Keywords**—Internet of Things; big data mining; clustering; association rules; Hadoop

## I. INTRODUCTION

Big data, business intelligence and Internet of Things (IoT) are among the fastest growing areas shaping the future, that attracted increasing attention of researchers and developers in the recent years. Many use cases have been envisioned to improve life quality and productivity through bridging the gap between physical and digital worlds, e.g. smart cities, smart homes, smart grids, smart meters, smart healthcare devices, wearable devices, smart poultry and animal farming, smart agriculture, and connected cars. As more physical entities are connected, an increasing volume of operational and management data is generated, making data mining and business analytics more crucial to turn this ocean of data into actionable insights generating values [1–5].

A branch of data mining and analytics is extracting association rules to discover patterns and regularities of frequent items in a dataset [6]. It was initially applied for transactional data analysis in point-of-sale systems in supermarkets to find items frequently purchased together (same basket) and predict the purchase of some items based on the observed frequency of others. A typical association rule takes the form  $\alpha \rightarrow \beta$ , where both  $\alpha$  and  $\beta$  are itemsets and  $\alpha \cap \beta = \emptyset$ .  $\alpha$  is known as the rule antecedent and  $\beta$  is the rule consequent. Each rule has a support which is the same as the support of  $\alpha \cup \beta$ , i.e. the number (or percentage) of transactions containing  $\alpha \cup \beta$ . Each rule has also a confidence level expressing how likely a person purchasing  $\alpha$  will simultaneously purchase  $\beta$ , i.e. the conditional probability  $P(\beta|\alpha)$ . For example, an association rule can be  $\{\text{coffee, sugar}\} \rightarrow \{\text{tea}\}$  with 75% confidence. Later its application has grown to many other domains.

For example in healthcare, a rule can take various forms, such as  $\{\text{Medicine}\} \rightarrow \{\text{Medicine}\}$ ,  $\{\text{Disease}\} \rightarrow \{\text{Disease}\}$ ,  $\{\text{Medicine}\} \rightarrow \{\text{Disease}\}$ ,  $\{\text{Symptoms}\} \rightarrow \{\text{Disease}\}$ , etc. [7]. Association rules and frequent-pattern mining have become an attractive area of research to support decision making in a wide spectrum of applications such as information security [8], health informatics [9], airline information systems [10], social networks [11], and several others [12, 13]. Several algorithms have been proposed on different areas in the literature [14]. However, many approaches can suffer from the massive number of discovered rules or spurious relations even for a moderately sized dataset. This limitation can lead to further problems in decision making attempting to visualize or interpret these rules; reducing their utility in decision support [15]. Some efforts have been made in the literature to address this problem in different directions such as rule grouping or clustering, rules pruning, meta-rules and constraint based mining [14, 16–20].

Nowadays, we are in the era of Internet-of-Things (IoT) where huge amount of data is generated by commercial, industrial and consumer IoT devices. However, along with the proliferation of IoT technology, cyberattacks that are exploiting the vulnerabilities of these new systems are becoming very challenging. Also labeling and discovering installed IoT devices is becoming very difficult. Association rules discovered from data generated from IoT devices are essential in securing, labeling, and discovering IoT devices [1, 21–24]. The problem is with the huge number of association rules that are discovered from IoT data. Existing solutions of reducing association rules are limited to traditional datasets.

In this paper, we are proposing a Hadoop MapReduce based algorithm that clusters rules discovered from big datasets. The proposed approach is composed of two phases. In the first phase, it prunes rules based on their structure, and in the second phase, it clusters the rules that were not pruned in the previous phase. The remainder of the paper is structured as follows. Related work is briefly reviewed in Section II. The proposed approach is presented in Section III and experimental evaluation is discussed in Section IV. The paper concludes in Section V with highlights of the paper findings and some future research work.

## II. RELATED WORK

Researchers proposed several algorithms in the literature to extract frequent itemsets and association rules in various domains, e.g. [9, 25, 26]. Among the major problems in big data is scalability of existing approaches leading to large number of association rules generated which hinders their interpretations and consuming huge computational resources.

Several studies proposed algorithms to reduce the number of association rules. For instance, in [14] the authors presented two methods to remove redundant rules based on domain knowledge. The first one prunes rules by grouping them based on user-defined semantics, and the second one groups rules based on common items.

In [27], the researchers proposed pruning rules by using the idea of domain ontology, which enables association rules to generalize in the form of is-a hierarchy. They integrated that with user knowledge pertaining to data, as a post-processing step, to select more interesting rules. To identify and then remove redundant rules, Torvonin et al. [18] utilized a rule cover method and then Brijs et al. [28] used integer programming to maximize the redundancy reduction. However, the success of these techniques depends on domain knowledge of users to eliminate uninteresting rules. The algorithm proposed in [29] goes through two phases. In Phase 1, it puts rules with the same consequences in the same group, and in Phase 2 prunes rules from each group that has minimum effect on the group cover.

Another direction uses various subjective and objective measures to identify interesting rules to keep. The study in [30] used chi-square statistical test to evaluate the dependence of rule antecedent and consequent. To make pruning of the rules, a pre-specified threshold value is used. However, this method may fail to prune many rules due to data sparsity. In [31], an idea based on minimum improvement constraint is presented to perform pruning by measuring the confidence difference between a rule and its proper sub-rules. However, the selection of threshold value is critical and lower values can lead to missing many overlapping rules. Contrast sets containing the conjunction of meaningfully different attributes and values was employed in [32]. In 2005, a search algorithm, known as OPUS (Optimized Pruning for Unordered Search-spaces) [33], was used in [34] to anatomically discard insignificant rules.

In [35], another approach is proposed that goes through two phases. In the first phase, clusters of association rules are created using a version of k-means algorithm called Kmeans-Rules; and in the second phase meta-rules are extracted from each cluster using two algorithms, namely BSO-MR and HBSO-TS-MR. BSO-MR uses bees swarm optimization and HBSO-TS-MR uses tabu search. The meta rules select representative rules and prune the rest. In [36], the authors propose pruning rules using a method called dual scaling to provide semantic contextualization. The method first groups the rules using an algorithm called AKMS and then prunes rules from the groups that have certain number of items to reduce data dimensionality.

An adaptive local pruning graphical method is described by Chawla et al. [37]. The authors defined an association rule network as a weighted B-graph and presented an algorithm to generate it. From a set of association rules with a singleton in the consequent as a goal item. Moreover, they presented an algorithm for rule pruning by removing hypercycles and reverse hyperedges in the B-graph. Visualization based techniques such as parallel coordinate plots [38], matrix-based visualizations [39] are introduced as post-processing techniques to analyze the discovered association rules. These techniques help visualize the interrelations between association rule categories

in a great detail. Unfortunately, most visualization techniques cannot display large sets of rules.

Another methodology applies classification or clustering approaches to reduce the number of discovered association rules. For example, Liu et al. [40] proposed a framework integrating classification with association rule mining to focus on a subset of association rules. This approach is known as Classification Based on Associations (CBA) and is composed of two parts: a rule generator (CBA-RG) and a classifier builder (CBA-CB). The first part, CBA-RG, is based on apriori algorithm to discover association rules whereas the second part, CBA-CB, is a heuristic to select the best rule subset. Other approaches used post processing with agglomerative hierarchical clustering to produce more compact set of association rules [41, 42]. Recently, Bui-Thi et al. proposed another approach based on the idea of mining unexpected patterns to automatically detect beliefs and outliers [43].

All the above mentioned solutions are limited to traditional datasets and cannot handle data generated by billions of IoT devices. Pruning or clustering association rules generated from big data is essential for many IoT applications [1, 24]. For example, IoT devices will pose substantial security challenges, some of which are device vulnerabilities, misconfiguration and mismanagement [21]. Also a wide variety of IoT devices are getting connected to residential networks everyday. But most residents lack the knowledge of how to protect their devices from security threats [22, 23]. Another problem is labeling and discovering of IoT devices which is now done manually. This is impractical with the rate at which the IoT devices are getting installed. Association rules can reduce the security issues of IoT related services and they can be used to automate labeling and discovering IoT devices [21–23].

### III. PROPOSED METHODOLOGY

The layout for association rule mining is illustrated in Fig. 1. In this study, we extended the work in [20]. After data acquisition and preprocessing, association rule mining is conducted. The proposed framework is composed of four MapReduce algorithms. First, PPrune [20] is applied to reduce the number of ARs based on their structure. Afterwards, Create-ACM, Compute-lift, and Cluster-SAR cluster the association rules that were not pruned.

#### A. PPrune: Rule Structure based Pruning Algorithm

PPrune reduces the number of association rules based on the structure of the rules. The concept of structural rule cover is presented in [18] and is utilized in PPrune to focus on most general rules of the original set of rules. PPrune is implemented for Hadoop MapReduce.

Algorithm 1 shows the PPrune Mapper which works as follows. For a given set of rules  $R$ , the Map method of PPrune reads each  $r \in R$  and identifies its antecedent, and consequent,  $r$ .antecedent and  $r$ .consequent (lines 3 and 4). It then sorts  $r$ .antecedent and computes its size,  $r$ .antecedent.size, which is the number of items in  $r$ .antecedent (lines 5 and 6). Finally, it emits a tuple (key, value) where key =  $r$ .consequent and value =  $r$  and sends it to the reducer (Line 9).

Algorithm 2 shows the Reduce method of PPrune. This method takes the output of the PPrune Mapper in the form of

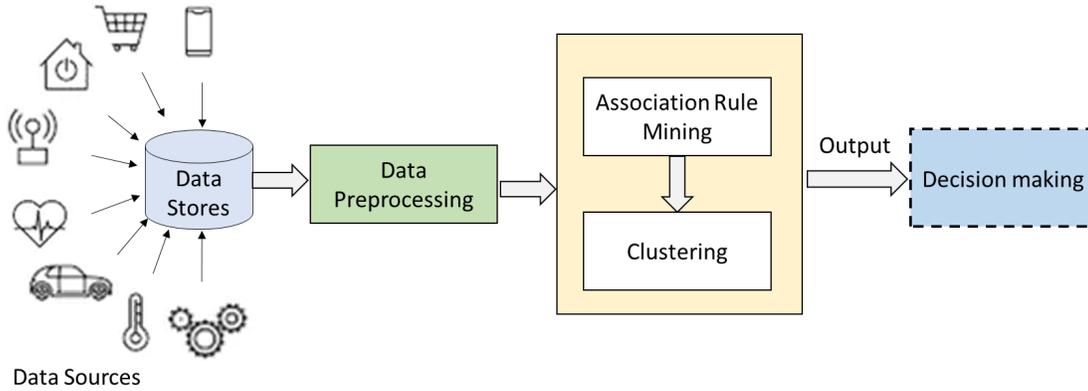


Fig. 1. Layout of Association Rule Mining.

---

**Algorithm 1** PPrune Mapper

---

```

1: Class MAPPER
2:   Method MAP(Key offset, Rule r)
3:     r.antecedent ← get-antecedent(r)
4:     r.consequent ← get-consequent(r)
5:     r.antecedent.size ← get-size(r.antecedent)
6:     r.antecedent ← sort(r.antecedent)
7:     k ← r.consequent
8:     v ← r
9:     Emit(k, v)
10:  End Method
11: End Class

```

---

(*k*, *v*) where the key *k* is rule consequent and the value *v* is a set of strong association rules having the same consequent. The Reduce method then generates a set of general rules *G* as output. It passes through two phases. First, it groups each *r* in *v* that has the same *r*.consequent and *r*.antecedent.size and forms a sub-partition,  $S[r.\text{antecedent.size}]$  (lines 3 to 7 in the pseudo code). After it puts each rule in one of the sub-partitions of *S*, it deletes the empty sub-partitions of *S* by resizing and re-indexing *S* (Line 8). In the second phase, reducer prunes covered rules. At Line 9, it initializes the set of general rules *G* to null. In following lines 10 to 18, the reducer loops through each sub-partition of *S*. For each rule in a sub-partition, if a rule belongs to the first sub-partition,  $S[1]$ , or is not a superset of any of the rules in *G*, then it adds the rule to *G*. Otherwise, the rule is pruned. Finally, the reducer emits the key *k* and the value *G* (Line 19).

**B. Lift-based Rules Clustering Approach**

This approach consists of the remaining three MapReduce algorithms introduced in the previous section, namely, Create-ACM, Compute lift, and Cluster-SAR. The number of ARs is further reduced by clustering ARs which were not pruned by PPrune. The clustering is based on an interest measure of AR known as lift [44], which is defined for rule  $A \rightarrow C$  as,

$$\text{lift}(A \rightarrow C) = \frac{\text{support}(A \cup C)}{\text{support}(A)\text{support}(C)} \quad (1)$$

---

**Algorithm 2** PPrune Reducer

---

```

1: Class REDUCER
2:   Method REDUCE(Key k, Value v)
3:     for each r ∈ v do
4:       s = r.antecedent.size
5:       ra = r.antecedent
6:        $S[s] \leftarrow ra$ 
7:     end for
8:     S ← Re-index(S)
9:     G ← ∅
10:    for i = 1; i ≤ |S|; i++ do
11:      for each r ∈  $S[i]$  do
12:        if i == 1 then
13:          G ← G ∪ r
14:        else if !Cover(G, r) then
15:          G ← G ∪ r
16:        end if
17:      end for
18:    end for
19:    Emit(k, G)
20:  End Method
21: End Class

```

---

It measures the correlation between the rule antecedent and consequent. A lift of value one indicates no correlation between the antecedent and consequent (i.e. independent); and a value much higher than one shows strong positive correlation. The proposed clustering approach is based on the assumption that rules with antecedents that are highly correlated with the same set of consequents are similar and thus should be clustered together [44]. Unlike the existing clustering approaches, this approach clusters antecedents containing itemsets which are rarely occurring together.

To perform the clustering efficiently, we created a 2-dimensional array (a matrix), *M*. The size of *M* is  $|A|$  by  $|C|$ , where  $|A|$  is the number of distinct antecedents and  $|C|$  is the number of distinct consequents of all the strong association rules that are going to be clustered. The element  $m_{i,j}$  of *M* contains the lift value of the rule  $A_i \rightarrow C_j$ , where  $A_i$  is the antecedent which corresponds to the  $i^{\text{th}}$  row of *M* and  $C_j$  is consequent which corresponds to the  $j^{\text{th}}$  column of *M*. An

element of  $M$  which does not belong to a strong association rule is assigned to a lift value of 1.

The distance between antecedents  $A_i$  and  $A_j$  is defined as:

$$dist(A_i, A_j) = \sqrt{\sum_{k=1}^{|C|} |m_{i,k} - m_{j,k}|} \quad (2)$$

To cluster antecedents into a set of  $K$  groups, namely  $G = G_1, G_2, \dots, G_K$ , we use  $K$ -means algorithm and minimize the within-cluster sum of squares,  $\sum_{i=1}^K \sum_{A_j \in G_i} dist(A_j, \mu_i)$ , where  $\mu_i$  is the centroid of  $G_i$ .

1) *Create-ACM mapreduce algorithm*: This algorithm takes as input strong association rules and initializes two 1-dimensional arrays called RHS and LHS, and a 2-dimensional array called ACM. LHS is indexed by the distinct antecedents of the strong association rules whereas RHS is indexed by the distinct consequents of the strong association rules. Let  $A = \{A_1, A_2, \dots, A_{|A|}\}$  be the set of all distinct antecedents and  $C = \{C_1, C_2, \dots, C_{|C|}\}$  be the set of all distinct consequents in the strong association rules, where  $|A|$  is the number of distinct antecedents and  $|C|$  the number of distinct consequents. The size of ACM is  $|A| \times |C|$ . Its rows are indexed by the members of  $A$  and its columns are indexed by the members of  $C$ . Let  $m_{i,j}$  be an element of ACM indexed by  $A_i$  and  $C_j$  and corresponds to the rule  $A_i \rightarrow C_j$ .

---

**Algorithm 3** Create-ACM Mapper

---

```
1: Class MAPPER
2:   Global: LHS, RHS
3:   Method MAP(Key offset, Rule r)
4:      $k \leftarrow$  get-antecedent(r)
5:      $v \leftarrow$  get-consequent(r)
6:     LHS  $\leftarrow$  AddLHS(k)
7:     RHS  $\leftarrow$  AddRHS(v)
8:     Emit(k, v)
9:   End Method
10: End Class
```

---

The Create-ACM Mapper extracts the antecedent and the consequent of each rule and emits them to the reducer function. It also initializes two global arrays called LHS and RHS. The size of LHS is  $|A|$  and the size of RHS is  $|C|$ . The elements of LHS and RHS are initially set to 0. The map function of the *Create-ACM* algorithm is depicted in Algorithm 3. At lines 4 and 5, the function extracts the antecedent and consequent of a rule. It then adds the consequent of a rule to RHS and the antecedent to LHS, lines 6 and 7. At Line 8, the function emits the antecedent and consequent of a rule to the reducer.

The Create-ACM Reducer creates ACM array as depicted in Algorithm 4. The reducer takes an antecedent and all its consequents from the Mapper as input. It also uses global lists LHS and RHS initialized by the reducer. At Line 4, the reducer uses a function called ACM-Init to create a row of ACM which contains  $|C|$  elements which are all initialized to -1. The row corresponds to one of the antecedents and each of its elements corresponds to one of the  $|C|$  consequents. Each element in a row correspond to a rule. At lines 5 to 7, each element of ACM which corresponds to a strong rule is set to 0. At last, the

Reducer emits the current antecedent with its corresponding ACM row, Line 8.

---

**Algorithm 4** Create-ACM Reducer

---

```
1: Class REDUCER
2:   Global: LHS, RHS, ACM
3:   Method REDUCE(Key k, Value v)
4:     ACM-Init(k, RHS, ACM)
5:     for each  $x \in v$  do
6:       ACM[k,x] = 0
7:     end for
8:     Emit(k, ACM[k])
9:   End Method
10: End Class
```

---

---

**Algorithm 5** Compute-Lift Mapper

---

```
1: Class MAPPER
2:   Global: TXN-count, LHS, RHS, ACM
3:   Method MAP(Key k, Value v,)
4:     TXN-count++
5:      $R \leftarrow$  generate-rules(v)
6:     for each  $r \in R$  do
7:        $c \leftarrow$  r.consequent
8:        $a \leftarrow$  r.antecedent
9:       update(LHS, a)
10:      update(RHS, c)
11:      if Exists(ACM, a, c) then
12:        Emit(a, c)
13:      end if
14:    end for
15:   End Method
16: End Class
```

---

2) *Compute-Lift mapreduce algorithm*: This algorithm takes as input transactions and gives as output the lift values of the strong association rules. It uses the three global arrays (TXN-count, LHS, RHS) and ACM to compute the lift values. The Compute-Lift Mapper is depicted in Algorithm 5. It counts the number of input transactions at Line 4 then generates all the possible rules from a transaction at Line 5. At lines 7 and 8, it extracts the antecedent and consequent of each rule generated at Line 5. If the antecedent is in LHS, then the corresponding element in LHS is incremented by 1, Line 9. Also if the consequent is in RHS, then the corresponding element in RHS is incremented by 1, Line 10. At last, the map function emits the current antecedent and consequent if they have a corresponding element in ACM, Lines 11 to 13.

The Compute-Lift reducer is shown in Algorithm 6. It takes an antecedent and all its consequents. It also uses the global variables TXN-count, ACM, LHS and RHS. This function receives from the mapper, an antecedent and all its consequents and checks the corresponding ACM element if it belongs to a strong association rule, Line 6. If it belongs to a strong association rule, then the count of that element is incremented by 1, Line 7. At last, the reducer computes the lift values using the Compute-lifts function and emits the antecedent and the corresponding lift values, Line 12.

3) *AR Clustering algorithm: Cluster-SAR*: This algorithm takes as input the rows of the 2-dimensional array ACM and

---

**Algorithm 6** Compute-Lift Reducer

---

```
1: Class REDUCER
2:   Global: TXN-count, LHS, RHS, ACM
3:   Method REDUCE(Key  $k$ , Value  $v$ )
4:      $a \leftarrow k$ 
5:     for each  $c \in v$  do
6:       if  $ACM[a,c] \geq 0$  then
7:          $ACM[a,c]++$ 
8:       end if
9:     end for
10:     $k \leftarrow a$ 
11:     $v \leftarrow \text{Compute-lifts}(ACM, \text{count}, LHS, RHS, a, c)$ 
12:    Emit( $k, v$ );
13:  End Method
14: End Class
```

---

returns as output the cluster of each strong association rule. Let us refer to each row of ACM as a sample. As explained above, each sample corresponds to a distinct antecedent and each element of a sample corresponds to a distinct consequent. Each element  $m_{i,j}$  of ACM contains the lift value of the rule  $A_i \rightarrow C_j$ .

---

**Algorithm 7** Cluster-SAR Mapper

---

```
1: Class MAPPER
2:   Global: centroid
3:   Method MAP(Key  $k$ , Value  $v$ )
4:     Init(index, minDistance)
5:     for  $i = 0; i < k; i++$  do
6:       distance  $\leftarrow$  EuclideanDistance( $v$ , centroid[ $i$ ])
7:       if  $dis \leq \text{MinDistance}$  then
8:         minDistance  $\leftarrow$  distance
9:         index =  $i$ 
10:      end if
11:    end for
12:     $k \leftarrow$  index
13:     $v \leftarrow \text{to\_string}(v)$ 
14:    Emit( $k, v$ )
15:  End Method
16: End Class
```

---

Cluster-SAR uses  $K$  (a pre-specified value) and global variable called centroid, which is initialized to random values. The algorithm is a slight modification of the one proposed in [44]. The Mapper of this algorithm is depicted in Algorithm 7. At Line 4, the function initializes the local variable index to -1 and the MinDistance to the highest real number. For each sample it reads, the mapper computes the distance of the sample from each of the  $K$  centroids. It associates each sample with the index of the closest centroid, Lines 5 to 11. At last, the mapper emits each centroid with its corresponding samples at Line 14.

The Cluster-SAR reducer is shown in Algorithm 8. It computes the new centroids. It takes as input each centroid and associated samples, then counts and computes the sum of the corresponding elements in its corresponding samples, lines 5 and 6. It then computes the average of the samples to generate the new centroids, Line 8.

---

**Algorithm 8** Cluster-SAR Reducer

---

```
1: Class REDUCER
2:   Method REDUCE(Key  $k$ , Value  $v$ )
3:     Init(SumV2, count)
4:     for each  $x \in v$  do
5:       count ++
6:       ComputeSum(SumV2,  $x$ )
7:     end for
8:     centroids  $\leftarrow$  ComputeCentroids(SumV2, count);
9:      $v \leftarrow \text{to\_string}(\text{centroids})$ ;
10:    Emit( $k, v$ );
11:  End Method
12: End Class
```

---

## IV. EVALUATION

We conducted a number of experiments to evaluate the performance of the proposed algorithms. In this section, we begin with a description of the experimental settings, datasets and evaluation metrics. We then describe the work conducted and discuss the obtained results and their analysis.

### A. Workspace Settings and Datasets

Hadoop 2.81 was used for the experiments. We used a hadoop cluster of three nodes; one was configured as a master node and the other two as slaves. We created four data nodes, each two in a machine. Python and Java were used to implement the proposed algorithms. The datasets used in the experiments were Chess, Mushroom, T10I4D100K, AllElectronics and Webdocs. We chose these datasets because they are publicly available benchmark datasets with different characteristics and frequently used in related work. A summary description of these datasets is shown in Table I including dataset name, notation, number of items, number of transactions, average number of items per transaction, and number of association rules for each dataset. In order to have larger datasets, we replicated each dataset to have four sizes: 1GB, 2GB, 3GB and 4GB; we will refer to each one of them as  $Di-j$ , where  $i \in 1, 2, 3, 4, 5$  denotes the dataset and  $j \in 1, 2, 3, 4$  denotes the sizes in GB.

### B. Evaluation Metrics

The proposed algorithms were evaluated using four performance measures, namely elapsed time, speedup, scaleup, and sizeup. Elapsed time is the difference between the completion time of job and its submission time. In short, it measures the duration of time a job took to be processed. Speedup compares the elapsed time of a single node to that of  $n$  nodes to complete the same job. It is defined as  $T_1/T_n$ , where  $T_1$  and  $T_n$  are the elapsed times of one and  $n$  nodes to complete the same job, respectively. Scaleup compares the elapsed time of a single node to complete a workload to that of  $n$  nodes to complete  $n$  times the original workload. It is defined as  $T_1/T_{n,n}$  where  $T_1$  is the elapsed time of one node and  $T_{n,n}$  is that of  $n$  nodes. Sizeup is defined as  $T_n/T_1$  and measures the scalability of a system. It compares the elapsed time to complete a single workload ( $T_1$ ) to the elapsed time of completing  $n$  times the original workload ( $T_n$ ).

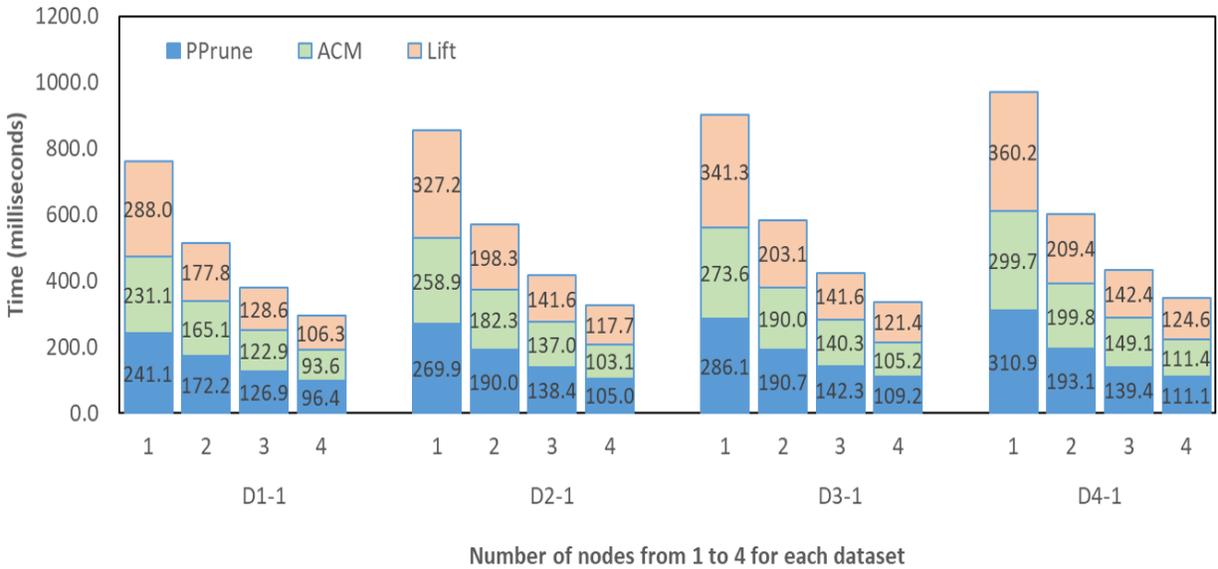


Fig. 2. Elapsed Time for each Algorithm (PPrune, Create-ACM, and Compute-Lift) for various Datasets and Number of Nodes.

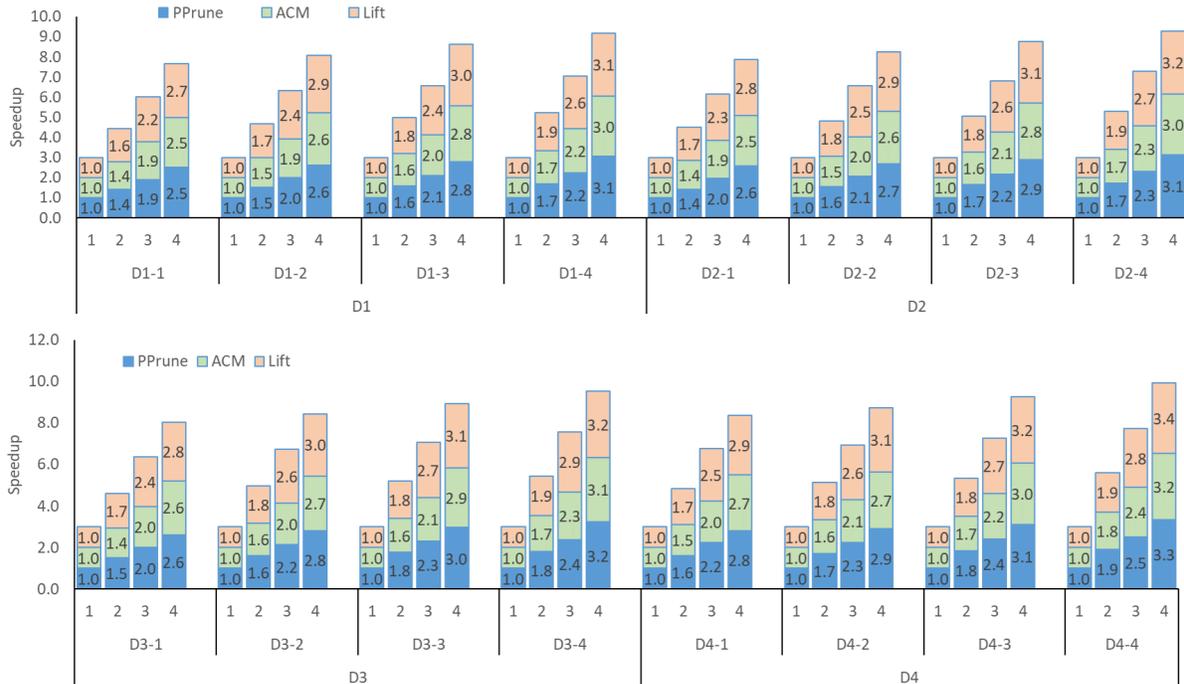


Fig. 3. Speedup for each Algorithm (PPrune, Create-ACM, Lift) for various Datasets and Number of Nodes.

TABLE I. EXPERIMENTAL DATASETS (EACH IS REPLICATED TO GENERATE LARGER DATASETS OF SIZE 1GB, 2GB, 3GB AND 4GB)

Dataset	Notation	Size (KB)	Items	Trans	Avg. Items/Trans	Rules
AllElectronics	D1	1	5	9	2.6	52
Chess	D2	335	75	3196	37	108061
Mushroom	D3	558	119	8124	23	111790
T10I4D100K	D4	3928	870	100000	10	5608
Webdocs	D5	1480	5,267,656	1,692,082	61	1,231,984

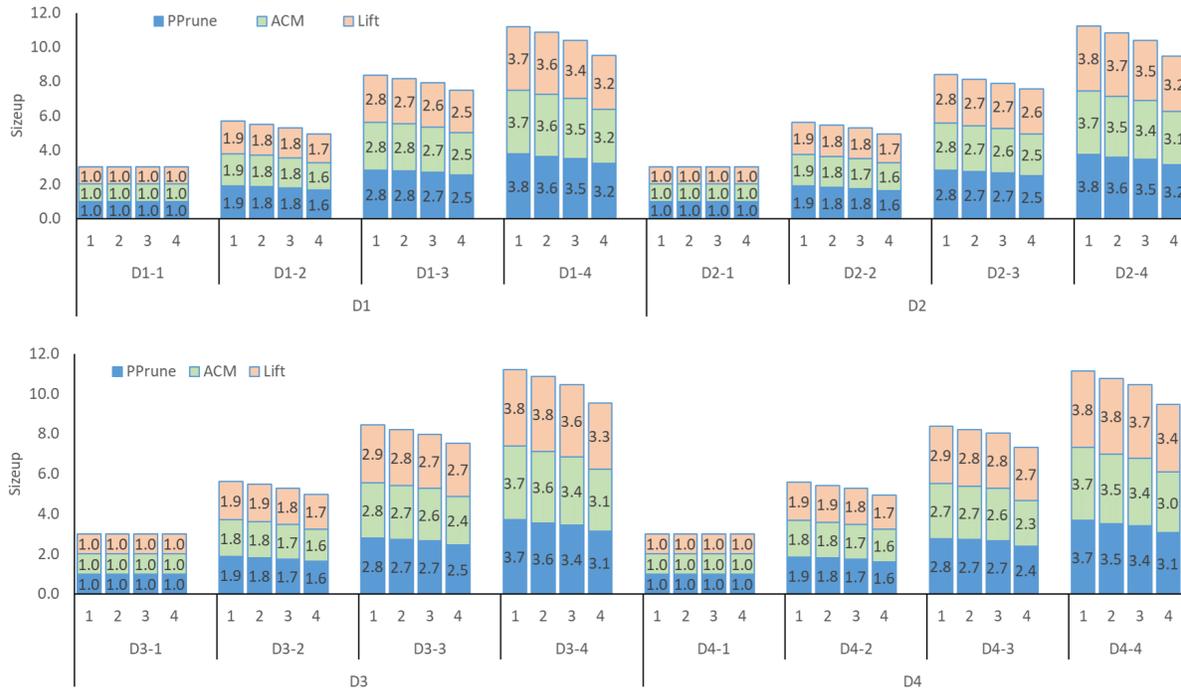


Fig. 4. Sizeup for each Algorithm (PPrune, Create-ACM, Lift) for various Datasets and Number of Nodes.



Fig. 5. Scaleup for each Algorithm (PPrune, Create-ACM, Lift) for various Datasets and Number of Nodes.

### C. Results

The performance of a MapReduce algorithm is significantly affected by the percentage of communication cost to that of I/O and CPU costs. The higher is the percentage of communication

cost in comparison to the I/O and CPU costs the less efficient is the MapReduce algorithm. To study the performance of the proposed MapReduce algorithms, we experimented using the datasets D1-1, D2-1, D3-1, and D4-1 with different number of data nodes (from one to four). Fig. 2 shows the results

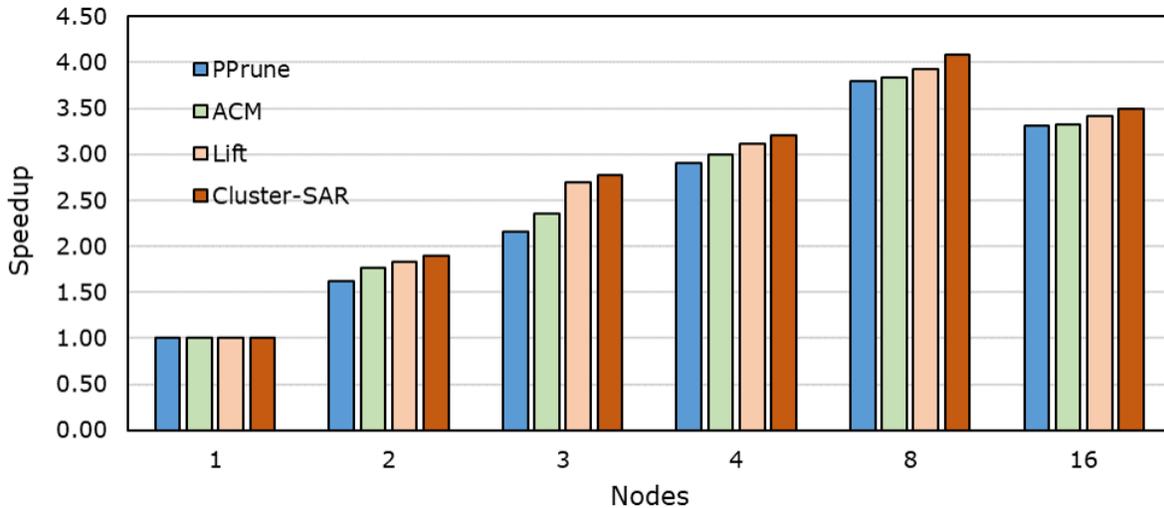


Fig. 6. Speedup of the Proposed Algorithms. Dataset used: Webdoc.

for the elapsed time for each algorithm (PPrune, Create-ACM, and Compute-Lift). As the number of nodes decreases, the elapsed time increases because more items in a node requires more elapsed time. As the number of nodes increases, less number of items is assigned per node, hence the elapsed time decreases. Moreover, the elapsed time increases with the number of items in a dataset; that is why D4-1 and D3-1 required more processing time than D1-1 and D2-1.

To study the remaining three measures, namely, scaleup, sizeup, and speedup, we performed three other sets of experiments. The result are shown in Fig. 3 for the speedup of PPrune, Create-ACM, and Compute-Lift. For  $p$  number of nodes, the ideal speed up is  $p$ . In our experiments, the worst speedup 1.6 for 2 nodes, 2.2 for three nodes and 2.7 for four nodes. The lowest speedup gained was when experimented with D1 and the best speedup was gained when experimented with D4. This is because D1 has few items compared to D4. Fewer elements results in shorter and fewer association rules, hence less CPU time. That is why the communication cost compared to the CPU cost was more when processing D1 than D4.

The second set of experiments was done to study the sizeup of PPrune, Create-ACM, and Compute-Lift. The results are shown in Fig. 4. The ideal sizeup is  $n$  when the size of the workload increases  $n$  times. The worst speedup was 3.1 for 4 nodes and the best was 3.4. The lowest speedup was attained with D1 and the best speedup was attained with D4. This is because D1 has few items compared to D4. Fewer elements result in shorter and fewer association rules, hence less CPU time. That is why the communication cost, compared to the CPU cost, was more when processing D1 than D4.

The third set of experiments was done to study the scaleup of PPrune, Create-ACM, and Compute-Lift. The results are shown in Fig. 5. The ideal scaleup is 1 when the size of the workload increases  $n$  times. In our experiments, the scaleups ranged between 0.78 and 0.84 when the number of nodes was 4. Again, the lowest scaleup was with D1 and the best

scaleup was with D4. This is because of the same reason that we discussed before, which is the number of items in D1 and D4.

Though we have replicated each dataset many times, the resulting number of rules was the same as the original dataset. Therefore, the number of rules was small. To experiment with a huge number of rules, we used the Webdoc dataset. We minimized the minimum support so that we can generate a huge number of rules from the dataset. Some attributes of the dataset are shown in Table I. We added another physical machine (with Intel i7-8750H Processor) and created up to 16 data nodes and then tested the proposed MapReduce algorithms. The performance of each algorithm is shown in Fig. 6. As expected, as the number of data nodes increased, the efficiency decreased since it is the ratio  $Speedup/p$ , where  $p$  is the number of processors. Also, when the number of data nodes used exceeded 8, the speedup decreased. This is because the percentage of the communication cost was too high compared to the CPU and I/O costs. The main reason for the high communication cost is the size of the Webdoc dataset, 1.48 GB, which is very small for a Hadoop machine with more than four data nodes. In general, the speedup of a Hadoop cluster with many nodes improves with bigger datasets.

## V. CONCLUSIONS

With the increasing size of datasets, the number of association rules mined by traditional approaches is growing exponential making them difficult to visualize or interpret. As a solution for this problem, researchers proposed pruning, grouping and clustering algorithms. The advent of big data technology motivates more research to be conducted in this field. This paper presented a novel approach for clustering huge number of association rules. The proposed MapReduce-based algorithms reduce the number of association rules by first pruning them based on rule structure and then clustering them based on lift value. To study the performance of the proposed algorithms, we used four measures, namely, elapsed

time, speedup, sizeup, and scaleup. We experimented using five benchmark datasets of which two are synthetic. We did all the experiments in a hadoop cluster and the results showed that the proposed algorithms are efficient. For example, the lowest scaleup achieved was 77%.

For future work, further experiments with more nodes and bigger datasets need to be conducted. The proposed algorithms can also be extended to relax the number of items in the consequent of a rule. Also different clustering algorithms and visualization tools can be employed to improve the efficiency of the proposed algorithms.

#### ACKNOWLEDGMENT

The authors would like to thank King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia, for the support during this work.

#### REFERENCES

- [1] C. Tsai, C. Lai, M. Chiang, and L. T. Yang, "Data mining for internet of things: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 77–97, 2014.
- [2] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.
- [3] T.-M. Choi, H. K. Chan, and X. Yue, "Recent development in big data analytics for business operations and risk management," *IEEE Transactions on Cybernetics*, vol. 47, no. 1, pp. 81–92, 2016.
- [4] E. Siow, T. Tiropanis, and W. Hall, "Analytics for the internet of things: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, p. 74, 2018.
- [5] Y. Cheng, K. Chen, H. Sun, Y. Zhang, and F. Tao, "Data and knowledge mining with big data towards smart production," *Journal of Industrial Information Integration*, vol. 9, pp. 1–13, 2018.
- [6] M.-S. Chen, J. Han, and P. S. Yu, "Data mining: an overview from a database perspective," *IEEE Transactions on Knowledge and Data Engineering*, vol. 8, no. 6, pp. 866–883, 1996.
- [7] K. Lakshmi and G. Vadivu, "Extracting association rules from medical health records using multi-criteria decision analysis," *Procedia computer science*, vol. 115, pp. 290–295, 2017.
- [8] 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.
- [9] W. Altaf, M. Shahbaz, and A. Guergachi, "Applications of association rule mining in health informatics: a survey," *Artificial Intelligence Review*, vol. 47, no. 3, pp. 313–340, 2017.
- [10] F. J. V. Martín, J. L. C. Sequera, and M. A. N. Huerga, "Using data mining techniques to discover patterns in an airline's flight hours assignments," *International Journal of Data Warehousing and Mining (IJDWM)*, vol. 13, no. 2, pp. 45–62, 2017.
- [11] H. Si, J. Zhou, Z. Chen, J. Wan, N. N. Xiong, W. Zhang, and A. V. Vasilakos, "Association rules mining among interests and applications for users on social networks," *IEEE Access*, vol. 7, pp. 116 014–116 026, 2019.
- [12] P. Fournier-Viger, J. C.-W. Lin, B. Vo, T. T. Chi, J. Zhang, and H. B. Le, "A survey of itemset mining," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 7, no. 4, p. e1207, 2017.
- [13] V. S. Kireev, A. I. Guseva, P. V. Bochkaryov, I. A. Kuznetsov, and S. A. Filippov, "Association rules mining for predictive analytics in iot cloud system," in *Biologically Inspired Cognitive Architectures Meeting*. Springer, 2018, pp. 107–112.
- [14] A. An, S. M. Khan, and X. Huang, "Objective and subjective algorithms for grouping association rules," in *Proc. 3rd IEEE International Conference on Data Mining (ICDM'03)*, vol. 3, 2003, p. 477.
- [15] R. Agrawal, T. Imieliński, and A. Swami, "Mining association rules between sets of items in large databases," *ACM SIGMOD Record*, vol. 22, no. 2, pp. 207–216, 1993.
- [16] S. Chawla, J. G. Davis, and G. Pandey, "On local pruning of association rules using directed hypergraphs," in *ICDE*, vol. 4, 2004, pp. 832–841.
- [17] A. Berrado and G. C. Runger, "Using metarules to organize and group discovered association rules," *Data Mining and Knowledge Discovery*, vol. 14, no. 3, pp. 409–431, 2007.
- [18] H. Toivonen, M. Klemettinen, P. Ronkainen, K. Hatanen, and H. Mannila, "Pruning and grouping discovered association rules," in *ECML'95 MLnet Workshop on Statistics, Machine Learning, and Knowledge Discovery in Databases*, April 1995, pp. 47–52.
- [19] B. Lent, A. Swami, and J. Widom, "Clustering association rules," in *Proceedings 13th International Conference on Data Engineering*, 1997, pp. 220–231.
- [20] M. A. Alasow, S. A. Mohammed, and E.-S. M. El-Alfy, "Parallel association rules pruning algorithm on hadoop mapreduce," in *International Conference on Advanced Communication and Networking*. Springer, 2019, pp. 117–130.
- [21] X. Feng, Q. Li, H. Wang, and L. Sun, "Acquisitional rule-based engine for discovering internet-of-thing devices," in *Proceedings of the 27th USENIX Conference on Security Symposium*, ser. SEC'18, 2018, pp. 327–341.
- [22] N. Hashimoto, S. Ozawa, T. Ban, J. Nakazato, and J. Shimamura, "A darknet traffic analysis for iot malwares using association rule learning," *Procedia Computer Science*, vol. 144, pp. 118 – 123, 2018.
- [23] R. Kumar, X. Zhang, R. Khan, and A. Sharif, "Research on data mining of permission-induced risk for android iot devices," *Applied Sciences*, vol. 9, p. 277, 01 2019.
- [24] Z. Wang, W. Liang, Y. Zhang, J. Wang, J. Tao, C. Chen, H. Yan, and T. Men, "Data mining in iot era: a method based on improved frequent items mining algorithm," in *Proc. 5th International Conference on Big Data and Information Analytics (BigDIA)*, 2019.
- [25] P. Sunhare, R. R. Chowdhary, and M. K. Chattopadhyay, "Internet of things and data mining: An applications oriented survey," *Journal of King Saud University-Computer and Information Sciences*, 2020.
- [26] W. Xiao and J. Hu, "Sweclat: a frequent itemset mining algorithm over streaming data using spark streaming," *The Journal of Supercomputing*, vol. 76, no. 10, pp. 7619–7634, 2020.
- [27] C. Marinica, F. Guillet, and H. Briand, "Post-processing of discovered association rules using ontologies," in *Data*

- Mining Workshops, 2008. ICDMW'08. IEEE International Conference on.* IEEE, 2008, pp. 126–133.
- [28] T. Brijs, K. Vanhoof, and G. Wets, “Reducing redundancy in characteristic rule discovery by using ip-techniques,” *Intelligent Data Analysis Journal*, vol. 4, pp. 200–0, 2000.
- [29] S. Kannan and R. Bhaskaran, “Association rule pruning based on interestingness measures with clustering,” *International Journal of Computer Science Issues*, vol. 6, 12 2009.
- [30] B. Liu, W. Hsu, and Y. Ma, “Pruning and summarizing the discovered associations,” in *Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining.* ACM, 1999, pp. 125–134.
- [31] R. J. Bayardo, R. Agrawal, and D. Gunopulos, “Constraint-based rule mining in large, dense databases,” *Data Mining and Knowledge Discovery*, vol. 4, no. 2-3, pp. 217–240, 2000.
- [32] S. D. Bay and M. J. Pazzani, “Detecting group differences: Mining contrast sets,” *Data mining and knowledge discovery*, vol. 5, no. 3, pp. 213–246, 2001.
- [33] G. I. Webb, “Opus: An efficient admissible algorithm for unordered search,” *Journal of Artificial Intelligence Research*, vol. 3, pp. 431–465, 1995.
- [34] S. Huang and G. I. Webb, “Discarding insignificant rules during impact rule discovery in large, dense databases,” in *Proc. SIAM International Conference on Data Mining*, 2005, pp. 541–545.
- [35] Y. Djenouri, H. Drias, and A. Bendjoudi, “Pruning irrelevant association rules using knowledge mining,” *International Journal of Business Intelligence and Data Mining*, vol. 9, p. 112, 01 2014.
- [36] L. A. Fernandes and A. C. B. García, “Association rule visualization and pruning through response-style data organization and clustering,” in *Lecture Notes in Artificial Intelligence (LNAI)*, vol. 7637, 2012, pp. 71–80.
- [37] S. Chawla and J. Davis, “On local pruning of association rules using directed hypergraphs,” in *Proc. 20th IEEE International Conference on Data Engineering (ICDE'04)*, 2003.
- [38] L. Yang, “Visualizing frequent itemsets, association rules, and sequential patterns in parallel coordinates,” in *International Conference on Computational Science and Its Applications.* Springer, 2003, pp. 21–30.
- [39] M. Hahsler and R. Karpienko, “Visualizing association rules in hierarchical groups,” *Journal of Business Economics*, vol. 87, no. 3, pp. 317–335, 2017.
- [40] B. L. W. H. Y. Ma and B. Liu, “Integrating classification and association rule mining,” in *Proc 4th International Conference on Knowledge Discovery and Data Mining*, 1998.
- [41] A. Strehl, G. K. Gupta, and J. Ghosh, “Distance based clustering of association rules,” in *Proceedings ANNIE*, vol. 9, 1999, pp. 759–764.
- [42] J. Mattiev and B. Kavšek, “Cmac: Clustering class association rules to form a compact and meaningful associative classifier,” in *Proc. International Conference on Machine Learning, Optimization, and Data Science.* Springer, 2020, pp. 372–384.
- [43] D. Bui-Thi, P. Meysman, and K. Laukens, “Clustering association rules to build beliefs and discover unexpected patterns,” *Applied Intelligence*, pp. 1–12, 2020.
- [44] M. Hahsler, “Grouping association rules using lift,” in *Proc 11th INFORMS Workshop on Data Mining and Decision Analytics (DMDA'16)*, 2016.

# Recent Advancement in Speech Recognition for Bangla: A Survey

Sadia Sultana<sup>1</sup>, M. Shahidur Rahman<sup>2</sup>, M. Zafar Iqbal<sup>3</sup>  
Dept. of Computer Science and Engineering  
Shahjalal University of Science and Technology Sylhet, Bangladesh

**Abstract**—This paper presents a brief study of remarkable works done for the development of Automatic Speech Recognition (ASR) system for Bangla language. It discusses information of available speech corpora for this language and reports major contributions made in this research paradigm in the last decade. Some important design issues to develop a speech recognizer are: levels of recognition, vocabulary size, speaker dependency and approaches for classifications; these have been defined in this paper in the order of complexity of speech recognition. It also highlights on some challenges which are very important to resolve in this exciting research field. Different studies carried out on last decade for Bangla speech recognition have been shortly reviewed in a chronological order. It was found that selection of classification model and training dataset play important roles in speech recognition.

**Keywords**—Bangla ASR; Bangla speech corpora; speaker dependency; vocabulary size; classification approaches; challenges

## I. INTRODUCTION

There are several important applications of a speech recognition system. It is used to develop chat-bots in smartphones and gadgets. For customer service in call centers, speech recognition systems are used for automated replies. ASR systems are widely used in automated machines to detect voice commands. Speech recognizer also can be used in detecting crime planned over phone calls and also for detection of hate speech delivery. A study shows that for English language more than 10% of searches are made by voice and most of them are done using smartphones [2]. This number will increase day by day. The first paper on Speech Recognition was published in 1950. Since then researches on Speech technology have achieved remarkable advancement over the last few decades, major advancement was started in 1980's with introduction of Hidden Markov Model (HMM) for Speech Recognition. The main objective of all research is to build an ASR (Automatic Speech Recognition) system which can operate for large vocabulary continuous speech for different languages.

Bangla language is spoken by more than 228 million people all over the world [1]. People from West Bengal, Tripura, Assam, Barak Valley, Andaman, Nicobar Islands, and diaspora living in various countries speak in Bangla Language. It is the national language of Bangladesh and official language of the states of West Bengal. As Bangla language has a large number of speaker groups, a successful ASR (Automatic Speech Recognition) system for this language will benefit lots of people. Research on Bangla ASR came into focus in the 90's. Recognition of Bangla speech has been started since around 2000. In 2002 A. Karim et al. presented a method for Spoken Letters Recognition in Bangla [3]. In the same year,

K. Roy et al. presented the Bangla speech recognition system using Artificial neural networks [4]. In 2003, M.R. Hassan presented a phoneme recognition system using Artificial neural network [5] and K.J. Rahman presented a continuous speech recognition system using ANN in 2003 [6]. Recently, Google presented a functional speech recognizer and voice search service (SpeechTexter and Google Assistant) for Bangla and other languages. But, these available for only android devices. The aim of this paper is to summarise all important works done recently on the development of Bangla ASR to facilitate the researchers working in this filed. Fig. 1 shows the diagram of a common ASR system. The system takes voice signal  $x(n)$  as input. Then, after preprocessing, feature extractions are done to reduce dimensionality of the input vector while preserving the discriminating attributes for recognition. In the decoder, there are mainly three parts: acoustic models, pronunciation dictionary and language models. Acoustic model calculates the probability of observed acoustic signal  $(x_1...x_N)$  for the given word sequence  $(w_1...w_N)$ . Language model provides the probability of proposed word sequence which is  $Pr(w_1...w_N)$ . Pronunciation dictionary contains list of words with their phonetic transcriptions, and it propose valid words for a given context. The decoder combines inputs from all three parts and applies classification models to deliver the recognized text as output  $y(n)$ .

The rest of this paper contents are organized as follows. Related works are discussed in Section II, issues to consider for developing ASR are presented in Section III, challenges in developing a successful Bangla ASR are explained in Section IV, a list of available natural speech corpora are reported in Section V, recent advancement in last decade is discussed in Section VI, and discussion and conclusion of the this study is presented in Sections VII and VIII, respectively.

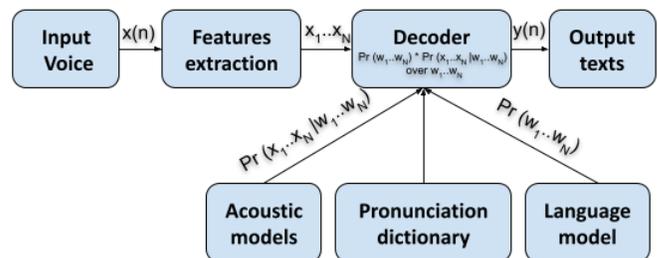


Fig. 1. Automatic Speech Recognition System.

## II. RELATED WORKS

In 2014, Sultana and Palit surveyed some common speech recognition techniques for Bangla language [7]. In 2020, Badhon et al. reviewed 15 research papers which worked on Bangla ASR. The study represented the datasets and detailed methodologies involved in those researches [8]. A few language specific surveys on ASR have been conducted for other languages by the researchers. For example, a group of researchers have represented speech recognition techniques for Chinese language [9]. Few studies have been done on Speech Recognition for Indian Languages [10][11][12]. Lima et al. have studied the Speech Recognition components for Portuguese language [13]. A literature review on Arabic speech recognition was done by Al-Anzi and AbuZeina [14]. In 2006, Ronzhin et al. studied all methods and models used for Russian speech recognition [15]. The target of such reviews is to represent a useful summary of overall works done on a language specific Speech recognition.

## III. ISSUES TO CONSIDER FOR ASR

There are some important research concerns that need to be considered when developing a speech recognition system. The application, development complexity, recognition efficiency of the system depend on a few things like utterance type, vocabulary size, speaker dependency and pattern matching approaches [16]. These factors are discussed briefly in the following sections in increasing order of recognition complexity of the system.

### A. Levels of Speech Recognition

The early stage of Speech recognition started with phoneme recognition from recorded speech [17]. Speech recognition systems can be developed to recognize: isolated words, connected words, continuous speech, or spontaneous speech. **Isolated words** are uttered separately with sufficient pause between them. For **connected words**, single words are recorded together but still there are pauses between them. In **continuous speech**, words are connected and there is overlapping between the words. This means deliberate pauses are not added after each word while recording. The **spontaneous speech** recognition system processes natural speech which is characterized by pauses, silence, disfluencies, etc. This type of recognition is most difficult as they require additional methods to process the speech.

### B. Vocabulary Size

The requirements for the vocabulary size of training dataset depend on the target applications of recognition systems. Some applications require as small vocabulary as a few words whereas some other requires millions of words to train the system. **Small-size vocabulary** dataset comprises only few to hundreds of words. It is used only when the system needs to recognize a fixed small number of digits or other spoken words. For example, digits dialing and access control. Usually contains 2 to 10 hours of recorded speech. Dataset for **medium-size vocabulary** contains thousands of words. This may contain 10 to 100 hours of recorded speech. This kind of datasets are used to recognize under-resourced languages. **Large-size vocabulary** contains millions of words. Large

vocabulary recognition systems are used in real-life speech recognition e.g. class lecture transcription. The speech corpora contains more than 100 hours of recordings involving a large number of speakers.

### C. Speaker Dependency

For speech recognition, features are collected from speakers' voice and the classification model is trained for these features. The system can be classified depending on the number of speakers they are able to identify successfully. **Speaker-dependant** voice recognition technique identifies different acoustic features of a single voice. These kinds of systems are easier to develop but they do not perform well for unknown speakers. **Speaker-independent** speech recognition systems comprises a large collection of speech from several speakers. Features are calculated for this large size data and recognition is performed by searching the best matching for existing data. **Speaker-adaptive** systems collects features from user samples to enrich the training data. The system adapts to the best suited features for speech recognition collected from users, in this way the error rate is reduced and the system also performs independent of speakers.

### D. Different Approaches of Speech Recognition

The approaches used to classify speech are categorized as follows [18]:

**Acoustic-phonetic approach:** This type of approach focuses on the nature of the speech. Speech features of phonetic units are detected with help of spectral analysis. For example, accent features of vowels and diphthongs analysis, considering the formants and energy of the signals, etc. The target is to discover the acoustic features of the sounds and apply those features to recognise continuous speech. Prior to the recognition this involves few steps which are features extraction, segmenting the feature contours and labelling the segments.

**Pattern recognition approach:** involves two steps - pattern training and pattern matching. By applying appropriate statistical methods patterns are extracted from speech units which are probably smaller than a word or a single word are stored in the database. A training algorithm is applied for this stored dataset and direct comparison is done between unknown speech segments and trained patterns during the recognition.

**Artificial intelligence approach:** This approach is considered as a mimic of our human brain which actually solves the problems based on its previous learning experiences. The problem solving strategy always follows the steps: learning, reasoning and perception. Typically this type of speech recognition system is based on neural networks (NN). Actually it combines the ideas taken from both the acoustic-phonetic approach and pattern recognition approach. Input signals are segmented and the acoustic parameters for these segments are calculated. The system is trained for these parameters and pattern matching is done for recognition. The pattern recognition task can be supervised or unsupervised. For supervised pattern recognition example input patterns are provided to the system as a predefined class. For unsupervised systems there are no example patterns, these systems are learn-based. Recent researches focus on speech recognition based on DNN, RNN, hybrid of HMM-DNN approaches.

### E. Performance Analysis

For word recognition systems, raw accuracy rate was used in many studies. For continuous speech recognition, Word error rate (WER) and Word recognition rate (WRR) most commonly used performance measure of the systems. Word error rate can be computed as [19]:  $WER = S+D+I/N$ ; where, S = number of substitutions, D = number of the deletions, I = number of the insertions, N = number of words in the reference. Word recognition rate (WRR) is defined as:  $WRR = 1 - WER$ . Reference word sequence and recognized word sequence may have different length and order, to skip this problem the recognized words are first aligned with the reference word then the error rate is calculated.

## IV. CHALLENGES IN DEVELOPING BANGLA ASR

Inherently Bangla language has some distinct features like different phonemic systems, presence of long and short vowels, frequent use of consonant clusters, variation in stress and intonation, etc. Building an efficient and successful Speech Recogniser for continuous speech in Bangla language is a challenging task for the researchers. There are some well-established APIs available for English language like SAPI, SIRI, IBM Watson API, etc. Researchers face few challenges when developing a speech recognizer for Bangla based on a successful API developed for other languages, e.g. English. The reasons are discussed below.

### A. Different Phonemes

Bangla Language consists of 14 vowels (7 natural, 7 nasal) and 29 consonants [20]. Number of phonemes and phonemic features differ from language to language. For example, Bangla and English language have their distinct phonemic systems [21]. One speciality of Bangla phonemes is that it has 7 nasalised vowels. There also exist two more long vowels /i:/ and /u:/.

### B. Speech Patterns

There are some basic differences in the speech pattern of Bangla with that of English and other languages. Bangla is said to be bound stress as for Bangla language stress is high at initial and becomes low at the end of speech [22]. Whereas, English is said to be stress-timed for different stress patterns.

### C. Difference in Accents

There is a noticeable difference of accents from region to region, it is true especially for different districts of Bangladesh. Sylhet, Dhaka, Comilla and other districts have their own dialects. The same word may be pronounced differently for different areas. This is a big challenge to build a common ASR system for all. For example, পাতা /-pata/ (English:leaf) is pronounced as ফাতা /-fata/ by many people from Sylhet.

### D. Insufficient Dataset

Still, Bangla is considered to be a low resource language [23]. That means, for the Bangla language, very low resources are public for research purposes. Nowadays almost all the research of Computational Linguistics are concentrating on Machine Learning-based models. A large training dataset is

the key point of getting a highly accurate model for DNN. We only have a few annotated dataset available for Bangla speech recognition.

### E. Homophones

There are a number of words which sound alike, but have different spellings, and meanings. For example, the words 'শব'- (English: dead body) 'সব' (English: all) both are pronounced as /ʃob/. Another example is, 'বিশ' (English: twenty) vs 'বিষ' (English :poison)both pronounced as /biʃ/. For the same phonetic representation, these problems cannot be resolved at the acoustic or phonetic levels. A higher level of language analysis is required to do this. To solve these kinds of problems we need a well defined language model and pronunciation dictionary. Unfortunately, still there is a lack of such well defined models for Bangla continuous speech.

### F. Spoken vs Written Words

Sometimes spoken language is not the same as the written language. For example, /bol/ (Englis: ball) and /bolo/ (English: speak) both have the same spelling 'বল'। Another example is /ʃabdʰan/ 'সবধান'where 'স'is pronounced as 'শ'. Again, a well-defined language model is required to solve this kind of problems.

### G. Consonant Clusters

Frequent use of consonant clusters in Bangla speech has made it difficult for word boundary detection. One example is the Bangla word 'চক্কর'(/tʃokkɔr/), in such cases most of the time the boundary is detected wrongly before the word ends, e.g. 'চক' and 'কর'it considers it as two words. This degrades the performance accuracy for the overall systems.

### H. Mismatched Environment

The background sound in many circumstances is an uncontrollable variable. For example, the level of background noise in streets of Bangladesh is not as same as those in other developed countries. It is a challenge to build an ASR system which will work efficiently on noisy environments.

### I. Unit Selection

Bangla words are pronounced syllable-wise and said to be rhythmic. We know there are different units of speech i.e. syllables, demi-syllables, diphones, phoneme. Bangla and English have different syllable structures [24]. The same pronunciation model can not be applied to both language. Sometimes it also becomes hard to decide which unit to select to implement an efficient boundary detection method. Syllable segmentation is a challenging task, still researchers are working on it.

## V. AVAILABLE SPEECH CORPORA FOR BANGLA

There are two standard forms of Bangla language. One is spoken in West Bengal of India and another form is the official language of Bangladesh. Researchers of both Bangladesh and West Bengal are contributing equally to enrich resources in this filed. For Bangla, there are a limited number of publicly available speech corpora. For Kolkata standard, (West Bengal), the first Bangla speech corpus was developed by Center

for Development of Advanced Computing (CDAC), Kolkata [25] in 2005. It is a collection of speech corpora for three East Indian Languages: Bangla, Assamese and Manipuri. It consists of 32 hours of continuous Bangla speech data. A read speech corpus named SHRUTI was released by IIT, Kharagpur in 2011 which contains 7383 unique Bangla sentences with 49 phonemes [26][27][28]. IARPA (Intelligence Advanced Research Projects Activity) Babel program developed a speech corpus which contains approximately 215 hours of Bengali conversational and scripted telephone speech collected in 2011 and 2012 along with corresponding transcripts [29]. According to a report published in 2014 [30] the Linguistic Data Consortium for Indian Languages (LDC-IL) collected 138 hours of Bangla continuous speech recorded over microphone and telephone line [31]. Technology Development for Indian Languages Program (TDIL) released a speech corpus which contains the more than 43000 audio files of Bangla words spoken by 1000 native speakers of West Bengal [32]. Recently European Language Resources Association (ELRA) published a Bangla (Bengali) Speech Corpora which contains a total of 70 hours of continuous speech recordings [33].

For Bangladeshi Bangla, in 2010 Bangladeshi researchers Firoj Alam et al. developed three speech corpora CRBLP for three different purposes [34]. The Corpus for acoustic analysis contains 262 sentences, the Diphone corpus contains 4335 sentences and the Continuous speech corpus contains 10895 sentences collected from nine categories of data. In the next year Murtoza et al. developed a phonetically balanced Bangla speech corpus which has 2 millions sentences with 47 millions biphones [35]. Khan et al. created a connected word speech corpus in 2018 containing 62 hours of recordings collected from more than 100 speakers [36]. Khan and Sobhan constructed another speech corpus for isolated words in the same year which has total 375 hours of recordings collected from 150 speakers [37]. OpenSLR's 'Large Bengali ASR training dataset' was recently published by Google in 2018, the dataset contains 229 hours of continuous speech for Bangladeshi Bangla [38]. There were 323 males and 182 females in total of 505 speakers who participated in the recording of 217902 utterances. In 2020 Ahmed et al developed an annotated speech corpus of 960 hours of speech collected from publicly available audio and text data [24]. The authors of this corpus also proposed an algorithm to automatically generate transcription from existing audio sources. At Shahjalal University, the NLP research team has developed a speech corpus subak.ko which contains 241 hours of recorded speech with 38,470 unique words which is yet to be published [39]. Table I represents the summary information of these mentioned corpora.

## VI. RECENT ADVANCEMENT IN LAST DECADE

Researches done for developing Bangla ASR have made a moderate progress since 2009. In 2009, Ghulam Muhammad et al. developed an HMM-based speaker independent Bangla digit recognizer [40] which used their own dataset of 10000 words recorded from 50 males and 50 females. The correction rate is above 80% for the system. An Artificial neural network (ANN) and Linear predictive coding (LPC) based ASR has been proposed by Anup Kumar et al. [41] in the same year. Multilayer perceptron (MLP) approach was followed to design the ANN model and LPC coder was used to extract the coefficients. It was able to discriminate four different words uttered

by 2 males and 2 females. In the next year, a Bangla phoneme classifier was built by Kotwal et al. [42]. It used hybrid features of Mel-frequency cepstral coefficients (MFCCs); and the phoneme probability was derived from the MFCCs and acoustic features using Multi-layer neural network (MLN). It obtained an accuracy rate of 68.90% using HMM classifier. The dataset contained 4000 sentences uttered by 40 male speakers. In the study [43] carried out by Mahedi Hasan et al., the researchers focused on triphone HMM-based classifier for word recognition. The system could recognize continuous speech using a speech corpus of 4000 sentences spoken by 40 males at the accuracy rate was above 80%. Mel-frequency cepstral coefficients MFCC38 and MFCC39 were extracted as features for classifications. In 2011, Firoze et al. [44] proposed a word recognition system which used spectral features and fuzzy logic classifier. The system was trained for a small dataset of 50 words spoken by a male and a female. The reported accuracy was 80%. An ASR method based on context sensitive triphone acoustic models was represented by Hassan et al. for continuous speech recognition. in 2011 [45]. It applied Multilayer neural network (MLN) to extract phoneme probabilities and triphone HMM for classification. It obtained accuracy of 93.71% using the same dataset from [42]. At about the same time a study was carried out by Sultana et al. [46] that applied a rule-based approach using Microsoft speech API (SAPI). The obtained accuracy was 74.81% for 270 Bangla unique words for this system. Akkas Ali et al. [47] presented a Bangla word recognizer in 2013 which used MFCC, LPC features and a hybrid of Gaussian mixture model (GMM) and Dynamic time warping (DTW) for classification. A group of researchers applied Back-propagation Neural Network for Bangla digit recognition [48]. Perceived recognition accuracy for the speaker-dependent system was 96.33% and speaker-independent system was 92%, respectively. The sample size of the dataset was limited to 300 words taken from 10 male speakers. A speaker-dependent neural network-based speech recognizer for this language was built in 2014 using MFCC features [49]. It employed feed-forward with back-propagation algorithm for classification and the perceived accuracy was 60%. A study carried out by Mahtab Ahmed and his team in 2015 claimed accuracy of 94% which employed Deep Belief Network (DBN) to classify recorded Bangla digits [50]. Seven layers of RBMs were considered for designing DBN and speech features were collected from MFCCs. Another study [51] applied semantic Modular time-delay neural network (MTDNN) for Bangla isolated word recognition. They conducted recurrent time delay structure to obtain dynamic long term memory. In total of 525 words were used to obtain an accuracy of 82%. In 2016, Nahid et al. [52] developed an automatic Bangla real number recognizer using the API CMU Sphinx 4 which was designed based on HMM. They used their own dataset 3207 sentences were taken from male speakers where feature extraction was done using MFCCs and accuracy of the system was 85%. In 2016, Mukherjee et al. [53] developed a Bangla character recognition system REARC (Record Extract Approximate Reduce Classify). Their database consisted of 3150 Bangla vowel phonemes retrieved from the voices of 18 females and 27 males. They considered MFCCs for feature extraction and the recognition rate was reported as 98.22%. Another study was published in the same year [54] which utilized Back-propagation neural network (BPNN) to classify Bangla digits using a dataset of

TABLE I. AVAILABLE SPEECH CORPORA FOR BANGLA

Year	Corpus Name	Size of dataset	No. of Speakers
2005	CDAC, Kolkata	32 hours of continuous speech	Not known
2010	CRBLP	13.50 hours of continuous speech	4 males, 4 females
2011	Phonetically balanced corpus	1.18 hours of continuous speech	One female
2011	SHRUTI	21.64 hours of continuous speech	26 males, 8 females
2012	IARPA-babel103b-v0.4b	215 hours of continuous speech	Not known
2014	LDC-IL	138 hours of continuous speech	240 males, 236 females
2014	TDIL	43000 audio files of isolated words	1000 native speakers
2018	OpenSLR's 'Large Bengali ASR training dataset'	229 hours of continuous speech	323 males, 182 females
2018	Bangla connected word speech corpus	62 hours continuous speech	50 males, 50 females
2018	Bangla isolated word speech corpus	375 hours of connected words	50 males, 50 females
2019	ELRA-U-S 0031	70 hours of continuous speech	Not known
2020	Bangla Speech Corpus from Publicly Available Audio & Text	960 hours of continuous speech	268 males, 251 females
2020	Subak.ko	241 hours of continuous speech	33 males, 28 females

300 connected digits. The system was tested against three different set-ups and the obtained accuracies were 88.84%, 98.46%, 82.31% for the experiments. It also represents some contrastive analysis of different digit recognition rates. In 2017, the famous "Google Voice Search" [55] added Bangla language to their system which was a turning point for Bangla ASR. The system employed attention-based encoder-decoder architectures such as Listen, Attend, and Spell (LAS) and n-gram based model for context detection [56]. Nahid et al. presented their study [57] for Bangla real number recognition using the dataset of their previous experiment [52]. The new experiment employed double layered Long short-term memory (LSTM) of an Recurrent neural network (RNN) approach to recognize individual Bengla words and achieved word detection error rate of 13.2% and phoneme detection error rate of 28.7%. A Bangla phoneme recognition system READ (Record Extract Approximate Distinguish) was developed by the researchers of West Bengal [58] in 2017. A group of 12 males and 8 females volunteered to develop the dataset of 1400 phonemes for the system. The overall recognition accuracy of the system was 98.36%. In 2018, a voice search system [59] for Bangla search engine Pipilika [60] was proposed. The system experimented two approaches and obtained word error rate of 3.96% and 5.30% for (GMM-HMM) based model and (DNN-HMM) based model, respectively. The dataset consisted of 500 words obtained from 43 male speakers and 7 female speakers. Rahman et al. developed a Bangla speech classifier [61] based on DTW-assisted Support vector machine (SVM) which can detect words in accuracy of 86.08%. MFCC features were obtained from a dataset of 260 words recorded from 52 speakers. Mukherjee, Phadikar and Roy presented an ensemble learning based Bangla phoneme recognition system which used LPCC-2 features for classification [62]. The system was tested on a dataset of 3710 Bangla vowel phonemes and obtained 99.06% recognition accuracy. 32 males and 21 females volunteered to build the dataset. A lexicon-free Bangla speech recognition system [63] was proposed in 2019 by Hasan et al. The model was trained for open-source Bangla speech corpus published by Google Inc. [38]. Two Connectionist temporal classification-based (CTC) experiments were carried out and the obtained WERs are 39.61% and 27.89% for the setups. A Bangla voice command detector [64] was developed by Gupta et al. in 2019. This digital personal assistant could execute a task by recognizing Bangla command. It employed the cross-

correlation technique to compare the energy of a given command with a pre-recorded signal. Five speakers volunteered to build a dataset of 240 audio files for 12 voice commands recorded in Bangla. The system perceived accuracies 83%, 83% and 75% for noiseless, moderate and noisy environments respectively. Another voice command recognition system was developed in 2020 [65] by Sadeq et al. The model used a hybrid of CTC and Attention mechanism in the end-to-end architecture with an RNN based language model. The system was trained for Bangla corpus released by Google [38]. For testing, a corpus containing 28973 sentences recorded from 34 male and 22 female speakers was built. Overall WER of the system for two different setups were 27.2% and 26.9%.

## VII. DISCUSSION

The study reveals that a good number of researches have been done in the field of developing Bangla ASR in the last decade. A large number of studies concentrated on developing a successful word recognition system for Bangla. Since, nowadays researchers are more interested doing NLP researches using the end-to-end systems, there is a growing attention to develop a continuous speech recognition system for Bangla based on this type of model. From the Table II, it is seen that the most commonly used features are MFC coefficients and the recent trend of using classifier is focused on ANN based models. Considering the size of the corpus the largest speech corpus for Bangla is the "Bangla Speech Corpus from Publicly Available Audio & Text", though publicly available largest natural corpus for this language is Google's "Large Bengali ASR training dataset". Considering, the training dataset and accuracy level Google's voice API is performing the best for Bangla speech recognition to date. The system uses n-gram language model which has the problem with synonyms and rigidity. It is evident that using a larger dataset in newer ML-based models improving the overall recognition rate of the system. Though, lots of works have been done related to Bangla ASR still we need to develop efficient language model and pronunciation model to be used for this purpose.

## VIII. CONCLUSION

In this paper, a study has been presented covering all the relevant researches done for Bangla ASR. A short summary of 24 research papers has been reported to address major

TABLE II. RECENT WORKS DONE ON BANGLA SPEECH RECOGNITION

Year	Author	Dataset	Unit	Input features/method	Approaches	Accuracy
2009	Muhammad et al.	10K digits	Digits	MFCC	HMM	> 84%
2009	Paul et al.	4 words	Isolated words	LPC	ANN	not mentioned
2010	Kotwal et al.	4K sentences	Phonemes	MFCC,Energy	HMM	>47%
2010	Hasan et al.	4K sentences	Connected words	MFCC38,MFCC39	Triphone HMM	>86%
2011	Firoze et al.	50 words	Isolated words	Energy, frequency	Fuzzy logic	80%
2011	Hassan et al.	4K sentences	Continuous speech	Phoneme probabilities	HMM	93.71%
2012	Sultana et al.	396 words	Connected words	xml grammar	SAPI	78%
2013	Akkas Ali et al.	1K words	Isolated words	MFCC, LPC, and DTW	GMM	>50%
2013	Hossain et al.	300 samples	Digits	F1, F2, MFCC	BPN	>92%
2014	Barua et al.	8 utterances	Continuous speech	MFCC	ANN	60%
2015	Ahmed et al.	840 words	Isolated words	MFCC	DBN	94%
2015	Ali Khan et al.	525 words	Isolated words	MFCC	MTDNN	82.66%
2016	Nahid et al.	3207 sentences	Real numbers	MFCC	CMU Sphinx-HMM	85%
2016	Mukherjee et al.	3150 phonemes	Continuous speech	MFCC	MLP	98.22%
2016	Ahammad et al.	300 digits	Digits	MFCC	BPN	98.46%
2017	Google Voice Search	217902 utterances	Continuous speech	LAS model	LSTM	WER 5.6%
2017	Nahid et al.	2000 words	Real numbers	MFCC	RNN, LSTM	WER 13.2%
2017	Mukherjee et al.	1400 phonemes	Phonemes	MFCC	MLP	98.35%
2018	Saurav et al.	500 words	Isolated words	MFCC	GMM-HMM(Kaldi)	WER 3.96%
2018	Rahman et al.	260 words	Isolated words	DTW	SVM	86.08%
2018	Mukherjee et al.	3710 vowels	Phonemes	LPCC-2	Ensemble Learning	99.06%
2019	Hasan et al.	OpenSLR's dataset	Continuous speech	Improved MFCC	CTC	WER 27.89%
2019	Gupta et al.	240 voice commands	Continuous speech	Energy	Cross-correlation	>75%
2020	Sadeq et al.	28973 sentences	Continuous speech	Labeled LDA	Hybrid CTC-Attention mechanism	>WER 12.8%

advancement in this filed. A detailed list of available speech corpora for this language also have been presented. Some challenges regarding the development of a successful and efficient Bangla ASR also have been discussed. The study found that the recent trend focuses on the ML-based approaches for classification. Introducing larger datasets for Bangla natural speech is improving the performance of ASR systems. This study may provide some important research insight for the researchers in this filed.

#### REFERENCES

- [1] Wikipedia. Bangali Language; 2021. Available from: [https://en.wikipedia.org/wiki/Bengali\\_language](https://en.wikipedia.org/wiki/Bengali_language).
- [2] TheNewStack. Bangali Language; 2021. Available from: <https://thenewstack.io/speech-recognition-getting-smarterstate-art-speech-recognition>.
- [3] Rezaul Karim AHM, Rahman MS, Iqbal MZ. Recognition of Spoken Letters in Bangla. In: In proceedings of the 5th ICCIT conference. ICCIT; 2002. p. 1–5.
- [4] Roy K, Das D, Ali MG. Development of the speech recognition system using artificial neural network. In: Proc. 5th international conference on computer and information technology (ICCIT02); 2002. p. 118–122.
- [5] Hassan MR, Nath B, Bhuiyan MA. Bengali phoneme recognition: a new approach. In: Proc. 6th international conference on computer and information technology (ICCIT03); 2003.
- [6] Rahman KJ, Hossain MA, Das D, Islam AZMT, Ali DMG. Continuous Bangla Speech Recognition System. In: Proc. 6th Int. Conf. on Computer and Information Technology (ICCIT03); 2003. p. 1–5.
- [7] Sultana R, Palit R. A survey on Bengali speech-to-text recognition techniques. In: 2014 9th International Forum on Strategic Technology (IFOST); 2014.
- [8] Badhon SSI, Rahaman MH, Rupon FR, Abujar S. State of art Research in Bengali Speech Recognition. In: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCN-T). IEEE; 2020. p. 1–6.
- [9] Fu SW, Lee C, Clubb OL. A survey on Chinese speech recognition. Communications of COLIPS. 1996;6(1):1–17.
- [10] Besacier L, Barnard E, Karpov A, Schultz T. Automatic speech recognition for under-resourced languages: A survey. Speech communication. 2014;56:85–100.
- [11] Hemakumar G, Punitha P. Speech recognition technology: a survey on Indian languages. International Journal of Information Science and Intelligent System. 2013;2(4):1–38.
- [12] Kurian C. A survey on speech recognition in Indian languages. International Journal of Computer Science and Information Technologies. 2014;5(5):6169–6175.
- [13] de Lima TA, Da Costa-Abreu M. A survey on automatic speech recognition systems for Portuguese language and its variations. Computer Speech & Language. 2020;62:101055.
- [14] Al-Anzi F, AbuZeina D. Literature survey of Arabic speech recognition. In: 2018 International Conference on Computing Sciences and Engineering (ICCSE). IEEE; 2018. p. 1–6.
- [15] Ronzhin AL, Yusupov RM, Li IV, Leontieva AB. Survey of russian speech recognition systems. In: Proc. of 11th International Conference SPECOM; 2006. p. 54–60.
- [16] Saksamudre SK, Shrishrimal P, Deshmukh R. A review on different approaches for speech recognition system. International Journal of Computer Applications. 2015;115(22).
- [17] Ostendorf M, Roukos S. A stochastic segment model for phoneme-based continuous speech recognition. IEEE Transactions on Acoustics, Speech, and Signal Processing. 1989;37(12):1857–1869.
- [18] Singh AP, Nath R, Kumar S. A Survey: Speech Recognition Approaches and Techniques. In: 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON). IEEE; 2018. p. 1–4.
- [19] Gaikwad SK, Gawali BW, Yannawar P. A review on speech recognition technique. International Journal of Computer Applications. 2010;10(3):16–24.
- [20] Wikipedia. Bengali phonology; 2011. Available from: [https://en.wikipedia.org/wiki/Bengali\\_phonology](https://en.wikipedia.org/wiki/Bengali_phonology).
- [21] Barman B. A contrastive analysis of English and Bangla phonemics. Dhaka University Journal of Linguistics. 2009;2(4):19–42.
- [22] Mandal SKD, Gupta B, Datta AK. Word boundary detection based on suprasegmental features: A case study on Bangla speech. International Journal of Speech Technology. 2007;9(1-2):17–28.
- [23] Bhattacharjee A, Hasan T, Samin K, Rahman MS, Iqbal A, Shahriyar R. BanglaBERT: Combating Embedding Barrier for Low-Resource Language Understanding. arXiv preprint arXiv:210100204. 2021;.
- [24] Ahmed S, Sadeq N, Shubha SS, Islam MN, Adnan MA, Islam MZ. Preparation of Bangla Speech Corpus from Publicly Available Audio & Text. In: Proceedings of The 12th Language Resources and Evaluation Conference; 2020. p. 6586–6592.

- [25] C-DAC. Annotated Speech Corpora for 3 East Indian Languages viz. Bangla, Assamese and Manipuri; 2005. Available from: [https://www.cdac.in/index.aspx?id=mc\\_ilm\\_Speech\\_Corpora](https://www.cdac.in/index.aspx?id=mc_ilm_Speech_Corpora).
- [26] Das B, Mandal S, Mitra P. SHRUTI Bengali Continuous ASR Speech Corpus; 2011. Available from: [https://cse.iitkgp.ac.in/~pabitra/shruti\\_corpus.html](https://cse.iitkgp.ac.in/~pabitra/shruti_corpus.html).
- [27] Das B, Mandal S, Mitra P. Bengali speech corpus for continuous automatic speech recognition system. In: 2011 International conference on speech database and assessments (Oriental COCOSDA). IEEE; 2011. p. 51–55.
- [28] Mandal S, Das B, Mitra P, Basu A. Developing Bengali speech corpus for phone recognizer using optimum text selection technique. In: 2011 International Conference on Asian Language Processing. IEEE; 2011. p. 268–271.
- [29] IARPA. IARPA Babel Bengali Language Pack IARPA-babel103b-v0.4b; 2016. Available from: <https://catalog.ldc.upenn.edu/LDC2016S08>.
- [30] Kandagal AP, Udayashankara V. Speech Corpus Development for Speaker Independent Speech Recognition for Indian Languages. *Grenze International Journal of Computer Theory and Engineering*. 2017;3(4).
- [31] LDCIL. Bengali Raw Speech Corpus; 2014. Available from: <https://data.ldcil.org/bengali-raw-speech-corpus>.
- [32] TDIL. Bengali Speech Data – ASR; 2018. Available from: [http://tdil-dc.in/index.php?option=com\\_download&task=showresourceDetails&toolid=2000&lang=en](http://tdil-dc.in/index.php?option=com_download&task=showresourceDetails&toolid=2000&lang=en).
- [33] ELRA. ELRA-U-S 0031; 2018. Available from: [http://universal.elra.info/product\\_info.php?cPath=37\\_39&products\\_id=1669](http://universal.elra.info/product_info.php?cPath=37_39&products_id=1669).
- [34] Alam F, Habib S, Sultana DA, Khan M. Development of annotated Bangla speech corpora. 2010;.
- [35] Murtoza S, Alam F, Sultana R, Chowdhur S, Khan M. Phonetically balanced Bangla speech corpus. In: Proc. Conference on Human Language Technology for Development 2011; 2011. p. 87–93.
- [36] Khan MF, Sobhan MA. Creation of Connected Word Speech Corpus for Bangla Speech Recognition Systems. *Asian Journal of Research in Computer Science*. 2018; p. 1–6.
- [37] Khan MF, Sobhan MA. Construction of large scale isolated word speech corpus in Bangla. *Global Journal of Computer Science and Technology*. 2018;.
- [38] Kjartansson O, Sarin S, Pipatsrisawat K, Jansche M, Ha L. Crowd-Sourced Speech Corpora for Javanese, Sundanese, Sinhala, Nepali, and Bangladeshi Bengali. 2018;.
- [39] Subakko. Speech to Text; 2019. Available from: <https://stt.sustbanglaresearch.org/>.
- [40] Muhammad G, Alotaibi YA, Huda MN. Automatic speech recognition for Bangla digits. In: 2009 12th International Conference on Computers and Information Technology. IEEE; 2009. p. 379–383.
- [41] Paul AK, Das D, Kamal MM. Bangla speech recognition system using LPC and ANN. In: 2009 Seventh International Conference on Advances in Pattern Recognition. IEEE; 2009. p. 171–174.
- [42] Kotwal MRA, Hossain MS, Hassan F, Muhammad G, Huda MN, Rahman CM. Bangla phoneme recognition using hybrid features. In: International Conference on Electrical & Computer Engineering (ICECE 2010). IEEE; 2010. p. 718–721.
- [43] Hasan MM, Hassan F, Islam GMM, Banik M, Kotwal MRA, Rahman SMM, et al. Bangla triphone hmm based word recognition. In: 2010 IEEE Asia Pacific Conference on Circuits and Systems. IEEE; 2010. p. 883–886.
- [44] Firoze A, Arifin MS, Quadir R, Rahman RM. Bangla Isolated Word Speech Recognition. In: ICEIS (2); 2011. p. 73–82.
- [45] Hassan F, Kotwal MRA, Muhammad G, Huda MN. MLN-based Bangla ASR using context sensitive triphone HMM. *International Journal of Speech Technology*. 2011;14(3):183–191.
- [46] Sultana S, Akhand M, Das PK, Rahman MH. Bangla Speech-to-Text conversion using SAPI. In: 2012 International Conference on Computer and Communication Engineering (ICCC). IEEE; 2012. p. 385–390.
- [47] Ali MA, Hossain M, Bhuiyan MN, et al. Automatic speech recognition technique for Bangla words. *International Journal of Advanced Science and Technology*. 2013;50.
- [48] Hossain M, Rahman M, Prodhan UK, Khan M, et al. Implementation of back-propagation neural network for isolated Bangla speech recognition. arXiv preprint arXiv:13083785. 2013;.
- [49] Barua P, Ahmad K, Khan AAS, Sanaullah M. Neural network based recognition of speech using MFCC features. In: 2014 international conference on informatics, electronics & vision (ICIEV). IEEE; 2014. p. 1–6.
- [50] Ahmed M, Shill PC, Islam K, Mollah MAS, Akhand M. Acoustic modeling using deep belief network for Bangla speech recognition. In: 2015 18th International Conference on Computer and Information Technology (ICCIT). IEEE; 2015. p. 306–311.
- [51] Khan MYA, Hossain SM, Hoque MM. Isolated Bangla word recognition and speaker detection by semantic modular time delay neural network (MTDNN). In: 2015 18th International Conference on Computer and Information Technology (ICCIT). IEEE; 2015. p. 560–565.
- [52] Nahid MMH, Islam MA, Islam MS. A noble approach for recognizing bangla real number automatically using cmu sphinx4. In: 2016 5th International Conference on Informatics, Electronics and Vision (ICIEV). IEEE; 2016. p. 844–849.
- [53] Mukherjee H, Phadikar S, Rakshit P, Roy K. REARC-A Bangla phoneme recognizer. In: 2016 International Conference on Accessibility to Digital World (ICADW). IEEE; 2016. p. 177–180.
- [54] Ahammad K, Rahman MM. Connected bangla speech recognition using artificial neural network. *International Journal of Computer Applications*. 2016;149(9):38–41.
- [55] Inc G. Google Voice Search; 2011. Available from: <https://voice.google.com/about>.
- [56] Chiu CC, Sainath TN, Wu Y, Prabhavalkar R, Nguyen P, Chen Z, et al. State-of-the-art speech recognition with sequence-to-sequence models. In: 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE; 2018. p. 4774–4778.
- [57] Nahid MMH, Purkaystha B, Islam MS. Bengali speech recognition: A double layered LSTM-RNN approach. In: 2017 20th International Conference of Computer and Information Technology (ICCIT). IEEE; 2017. p. 1–6.
- [58] Mukherjee H, Halder C, Phadikar S, Roy K. READ—a Bangla phoneme recognition system. In: Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications. Springer; 2017. p. 599–607.
- [59] Saurav JR, Amin S, Kibria S, Rahman MS. Bangla speech recognition for voice search. In: 2018 international conference on Bangla speech and language processing (ICBSLP). IEEE; 2018. p. 1–4.
- [60] of Science SU, Technology. Pipilika; 2013. Available from: <https://pipilika.com/>.
- [61] Rahman MM, Dipta DR, Hasan MM. Dynamic time warping assisted svm classifier for bangla speech recognition. In: 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2). IEEE; 2018. p. 1–6.
- [62] Mukherjee H, Phadikar S, Roy K. An ensemble learning-based Bangla phoneme recognition system using LPCC-2 features. In: *Intelligent Engineering Informatics*. Springer; 2018. p. 61–69.
- [63] Hasan MM, Islam MA, Kibria S, Rahman MS. Towards Lexicon-free Bangla Automatic Speech Recognition System. In: 2019 International Conference on Bangla Speech and Language Processing (ICBSLP). IEEE; 2019. p. 1–6.
- [64] Gupta D, Hossain E, Hossain MS, Andersson K, Hossain S. A digital personal assistant using bangla voice command recognition and face detection. In: 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON). IEEE; 2019. p. 116–121.
- [65] Sadeq N, Ahmed S, Shubha SS, Islam MN, Adnan MA. Bangla Voice Command Recognition in end-to-end System Using Topic Modeling based Contextual Rescoring. In: ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE; 2020. p. 7894–7898.

# Intrusion Detection using Deep Learning Long Short-term Memory with Wrapper Feature Selection Method

Sana Al Azwari<sup>1</sup>, Hamza Turabieh<sup>2</sup>

Department of Information Technology, Taif University, Taif, Saudi Arabia

**Abstract**—Recently, many companies move to use cloud computing systems to enhance their performance and productivity. Using these cloud computing systems allows the execution of applications, data, and infrastructures on cloud platforms (i.e., online), which increase the number of attacks on such systems. As a resulting, building robust Intrusion detection systems (IDS) is needed. The main goal of IDS is to detect normal and abnormal network traffic. In this paper, we propose a hybrid approach between an Enhanced Binary Genetic Algorithms (EBGA) as a wrapper feature selection (FS) algorithm and Long Short-Term Memory (LSTM). A novel injection method to prevent premature convergence of the GA is proposed in this paper. An intelligent k-means algorithm is employed to examine the solution distribution in the search space. Once 80% of the solutions belong to one cluster, an injection method (i.e., add new solutions) is used to redistribute the solutions over the search space. EBGA will reduce the search space as a preprocessing step, while LSTM works as a binary classification method. UNSW-NB15, a real-world public dataset, is used in this work to evaluate the proposed system. The obtained results show the ability of feature selection method to enhance the overall performance of LSTM.

**Keywords**—Intrusion detection; feature selection; long short-term memory; binary genetic algorithm

## I. INTRODUCTION

With the exponential growth rates of volumes of data, both structured and unstructured, that are generated from a variety of sources, the need to provide protection and privacy becomes a challenging issue for intrusion detection systems (IDSs) in this big data environment. Intrusions are suspicious and unauthorized activities on a computer or network that threaten the security of these systems. IDSs are very crucial to ensure network and information security. These systems can be devices or software that monitor systems or networks for malicious activities or violations of security policies.

Intrusion detection systems detects unusual attacks based on two methods; signature-based detection and anomaly detection. In signature-based detection, IDS analyzes system activities to find patterns that are similar to previously detected and stored patterns in a database. Intrusion detection using an anomaly detection method which relies on machine learning to build models of patterns of normal behavior on the system or the network (i.e., cloud computing systems) to detect patterns of unusual behavior. Fig. 1 presents the main architecture for IDS for cloud computing systems.

There are many algorithms have been proposed to build a robust IDS based on machine learning and soft computing methods. Network traffic data is a high dimensional one, many

papers investigated the ability of employing FS algorithms to enhance the overall performance of IDS [1]. For example, Almomani [2] applied four types of FS algorithms, namely, genetic algorithm (GA), particle swarm optimization (PSO), firefly optimization (FFA), and grey wolf optimizer (GWO). Almomani used two classifiers: Support Vector Machine (SVM) and decision tree (J48) to build a robust IDS. Thakkar and Lohiya [3] applied seven ML classifiers (i.e., Neural Networks (NN), Decision Tree (DT), Logistic Regression (LR), Support Vector Machine (SVM), k-nearest neighbours (kNN), Random Forest (RF), and Naïve Bayes (NB)) to build an intelligent IDS. Zhu et al. [4] introduced a multi-objective method for FS for building a robust IDS inside cloud computing systems.

Many contributions in the literature focus on traditional machine learning methods for IDS. However, these methods have high cost in terms of training time when working with big data sets. To overcome this issue, deep learning approach is used for effective learning mechanism in reducing the training time and increasing the accuracy of the obtained results from the IDS. Moreover, the main contribution of this work is to introduce a robust wrapper feature selection that is able to reduce the high dimensionality of the dataset.

This paper is organized as follow: Section II presents the related works of IDS. Section III presents the proposed method used in this paper (i.e., EBGA and LSTM). Section IV presents the data set used in this paper. Section V presents the obtained results and analysis. Finally, Section VI presents the conclusion and future works of this paper.

## II. RELATED WORK

The literature shows a number of traditional machine learning approaches methods have been proposed for intrusion detection systems which include Support Vector Machine, K-Nearest Neighbors, Decision Trees, Random Forests, Linear Regression, Naive Bayes, Artificial Neural Networks. Recently, deep learning-based approaches has emerged to overcome the challenges of developing an accurate high-detection rate IDSs. State of the art deep learning approaches that have been used for IDS include Deep Neural Networks (DNNs) [5], Deep Belief Networks (DBNs), Restricted Boltzmann Machines (RBMs), autoencoders and hybrid methods. For example, Zhao et al. [6], proposed an intrusion detection method based on deep belief networks and probabilistic neural network. The KDD CUP 99 data set was used for testing the performance of the proposed method. The result shows that their proposed method performs better than traditional

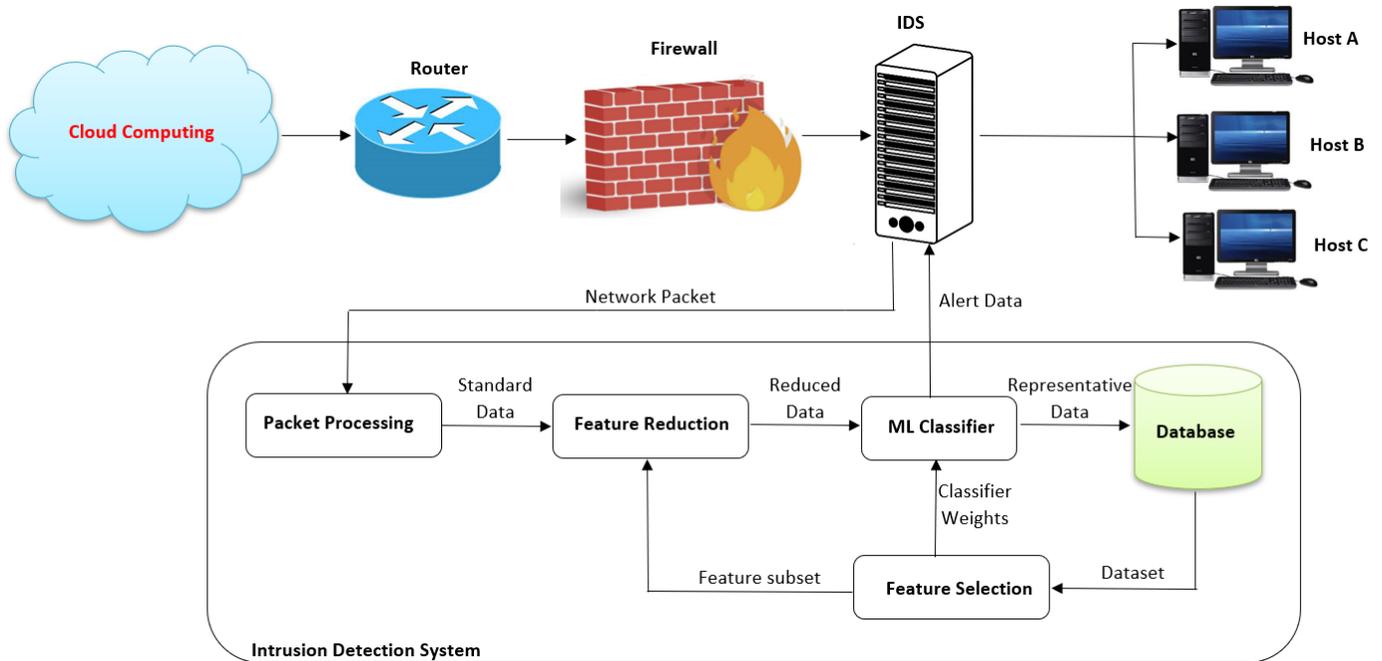


Fig. 1. IDS Architecture in a Cloud Computing.

machine learning techniques with accuracy of 99.1%, precision of 93.25% and FAR of 0.615%.

In [7] Erfani et al. presented a hybrid approach for IDS by combining DBNs with a linear one-class SVM and was applied using several data sets. Their experimental results show that their proposed model is scalable and computationally efficient and when compared to an autoencoder it executes 3 times faster in the training phase and 1000 times faster in the testing phase.

In [8], the authors proposed an approach for IDS based on deep learning using self-taught learning on NSL-KDD, a benchmark data set, with only six features selected out from the forty one features of the data set. results of their experiments and comparisons with other machine learning algorithms; Naive Bayes, SVM and Decision Tree show that using deep learning algorithm is promising as it performs better than the other algorithms with higher accuracy rate and lower false positive rate.

Javaid et al. [5] proposed a network intrusion detection system based on deep learning approach. They used self-taught learning technique (STL) on NSL-KDD benchmark data set. They compared the performance of their approach with the soft-max regression (SMR). their results show that the proposed approach outperforms SMR with accuracy rate more than 98%.

In [9] proposed an approach for network traffic identification using Artificial Neural Networks (ANN) and Stacked AutoEncoder (SAE) based on Deep learning using a real data set of TCP data collected from an internal network. Results of their work show that their proposed approach can classify any flow data to a predefined protocol with accuracy enough to be applied in real applications.

Yin et al. [10] compared the performance of their IDS which is based on recurrent neural network, a deep learning approach, with a number of traditional machine learning techniques. Results from their experiments on NSL-KDD benchmark data set show that the proposed system outperforms traditional machine learning methods in both binary and multi-class classification with high accuracy.

The above work studied the emergence of deep learning in the performance of IDS. However, to date, A few number of existing studies in the literature have addressed the integration of deep learning approaches and Big Data for improving the performance of IDSs. Faker and Dogdu [11] integrated Big Data and deep learning approach to enhance the performance of intrusion detection system using three classifiers to classify attacks in both binary and multi-class classification; Deep Feed-Forward Neural Network (DNN), Random forest and Gradient Boosting Tree (GBT) on UNSW-NB15 and CICIDS2017 data sets. on UNSW-NB15, DNN gives high accuracy results in both binary and multi-class classification of 99.19% and 97.04%, respectively with low prediction times. However, on CICIDS2017, GBT achieved the best accuracy, of 99.99%, in binary classification. Researches in [12] suggested the implementation of Deep Neural Network model (DNN) for IDS to detect and classify unforeseen and unpredictable cyberattacks. They provide a comprehensive evaluation of experiments of DNN and other traditional machine learning models using various benchmark IDS data sets such as KDDCup99, NSL-KDD, UNSW-NB15, Kyoto, WSN-DS and CICIDS2017. Their proposed model exceeded in performance the other classical machine learning classifiers. A recent work by [13] addressed the detection of intrusions through the use of deep learning in big data environment. They proposed a hybrid deep learning model based on convolutional neural network (CNN) and a weight-dropped, long short-term memory net-

work (WDLSTM). CNN is used to extract features from IDS big data and WDLSTM network for learning dependencies among the extracted features to solve the overfitting problem. Their experimental results show a good performance with 97.1% accuracy.

### III. PROPOSED METHOD

#### A. Enhanced Binary Genetic Algorithm

One of the most population evolutionary algorithms that mimics the nature selection is Genetic Algorithm (GA) [14]. GA is a population-based algorithm, where the best solution obtained after a predefined number of iterations. In simple, GA starts by generating a set of solutions called population. All these solutions are evaluated based on a fitness function. A set of genetic operations (i.e., selection, crossover, and mutation) are applied on the population at each iteration. This process is repeated iteratively until stop condition is met and return the best solution [15]. Fig. 2 explores the standard GA algorithm.

```

Given:
-nP: base population size.
-nI: number of iterations.
-rC: rate of crossover.
-rM: rate of mutation.
Generate initial population of size nP.
Evaluate initial population according to the fitness function.
While (current_iteration ≤ nI)
//Breed rC × nP new solutions.
Select two parent solutions from current population.
Form offspring's solutions via crossover.
IF(rand(0.0, 1.0) < rM)
Mutate the offspring's solutions.
end IF
Evaluate each child solution according to the fitness function.
Add offspring's to population.
//population size is now MaxPop=nP × (1+rC).
Remove the rC × nP least-fit solutions from population.
end While
Output the global best solution
    
```

Fig. 2. Standard Genetic Algorithm.

To enhance the performance of GA, we proposed a novel injection method based on solution distribution in the search space. At each iteration, we examined the solution distribution using intelligent k-means clustering algorithm, if 80% of the solutions located in one cluster, we redistribute the solution by injecting the population with new solutions to redistribute the solutions over the search space and prevent the premature convergence. This enhancement will enhance the exploration process of GA. Fig. 3 explores the flow chart of enhanced GA.

#### B. Long Short-Term Memory (LSTM) Networks

A deep learning method (i.e., CNN-LSTM) is employed to detect intrusions. Fig. 4 explores the main structure of CNN-LSTM. In simple, LSTM uses an internal memory to memorise the temporal sequence of the input feature vectors.

LSTM maps the input  $i$  (i.e., features) with output  $o$  (i.e., abnormal/normal packet), while forget  $f$  gate to memorize the store features. The hidden state  $h$  cell state  $c$  are used for

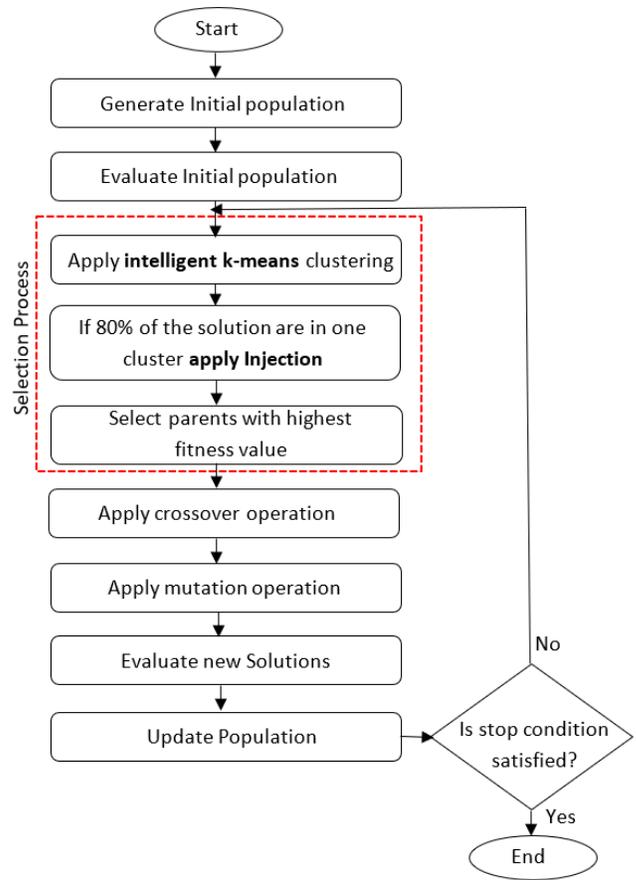


Fig. 3. Enhanced Genetic Algorithm.

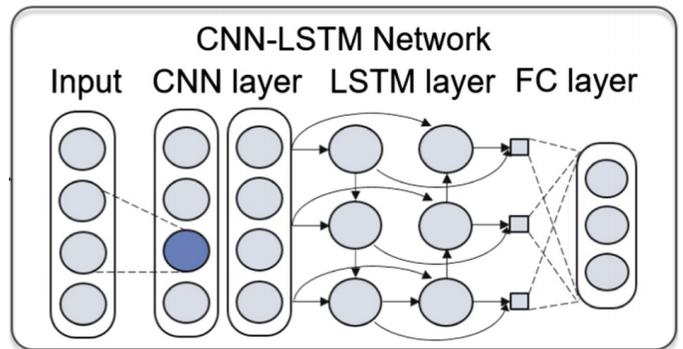


Fig. 4. The Main Structure of CNN-LSTM.

memorizing. All calculations of LSTM are shown in Eqs.(1, 2, and 3).

$$\begin{pmatrix} i \\ f \\ o \\ g \end{pmatrix} = \begin{pmatrix} \text{sigmoid} \\ \text{sigmoid} \\ \text{sigmoid} \\ \text{tanh} \end{pmatrix} w^t \begin{pmatrix} h_{t-1}^l \\ h_{t-1}^l \end{pmatrix} + \begin{pmatrix} b_i \\ b_f \\ b_o \\ b_g \end{pmatrix} \quad (1)$$

$$c_t = f_t \circ c_{t-1} + i_t \circ g \quad (2)$$

$$h_t = o_t \circ \sigma(c_t) \quad (3)$$

The calculation of fully connected layer and softmax process are shown in Eq. (4), and Eq.(5), respectively. In this work, we employed the softmax to classify the input user's role. While the output of the fully connected layer is presented by the softmax layer in a range [0,1].  $N_c$  refers to the number of rules, and  $L$  presents the activity class probability.

$$d_i^l = \sum_i \sigma(W_{ji}^{l-1}(h_i^{l-1}) + b_i^{l-1}) \quad (4)$$

$$P(c|d) = \underset{c \in C}{\operatorname{argmax}} \frac{\exp(d^{L-1}w^L)}{\sum_{k=1}^{N_c} (d^{L-1}w_k)} \quad (5)$$

### C. EBGA-LSTM

The proposed hybrid approach works by combining EBGA with LSTM. Here, EBGA works as a wrapper FS to remove the redundant/irrelevant data from the original dataset. while LSTM works as a binary classifier to detect normal and abnormal network traffic.

## IV. DATASET

This paper evaluates the proposed hybrid approach over a public intrusion data set called UNSW-NB1. The data set is generated using a tool called IXIA PerfectStorm by Moustafa et al. [16]. The data set has 9 different types of attacks. The data set has 49 features. In this work, only 44 features are used. Table I explores 44 features of the data set. Moreover, this data set has 9 different attacks as shown in Table II.

UNSW-NB data set is imbalanced data set. In this work, adaptive synthetic sampling method (ADASYN) is employed for solving class imbalance issue [17]. Table III explores the original and balanced data set. In this work, this data set is used as a binary classification problem to determine normal or abnormal attacks.

## V. RESULTS AND ANALYSIS

This section reports the validation of the proposed hybrid method (i.e., EBGA with LSTM) to detect intrusion in cloud computing systems. All experiments are employed based on cross-validation method with  $k$ fold=10. We implemented the proposed approach using MATLAB 2019b. We used six criteria to evaluate the proposed method which are: accuracy (see Eq.(6)), Specificity (see Eq.(7)), Precision (see Eq.(9)), Recall (see Eq.(10)), and F-Measure (see Eq.(11)).

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \quad (6)$$

$$Specificity = \frac{TN}{TN + FP} \quad (7)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (8)$$

$$Precision = \frac{TP}{TP + FP} \quad (9)$$

$$Recall = \frac{TP}{TP + FN} \quad (10)$$

$$F - Measure = \frac{2 \times (Recall \times Precision)}{Recall + Precision} \quad (11)$$

Fig. 5 explores the performance of the original GA and EBGA as wrapper feature selection algorithms. Here, we used kNN as an internal classifier for all FS methods. The performance of EBGA outperform the original one with accuracy equals 88.7475, while the performance of original GA was the worst with accuracy equals 87.523. It is obvious here, the EBGA select 18 features out of 43, while the original GA select 11 features. The obtained results here give us a good indication that our proposed feature selection algorithm can explore the search space better than the original one.

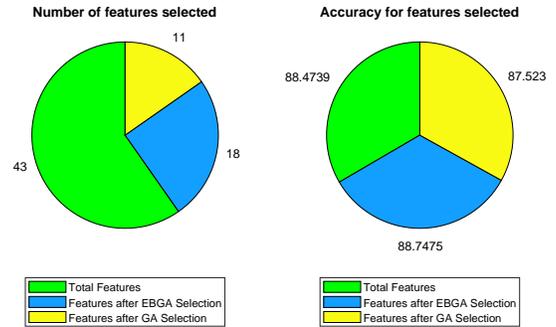


Fig. 5. Selected Features.

To perform a good analysis of the proposed approach, we simulated the proposed hybrid approach (i.e., EBGA with LSTM) with three settings; balanced data set with FS (i.e., EBGA), balanced data set without FS and Original data set without FS. Table IV explores the obtained results for three types of experiments. It is clear that the performance of feature selection improves the overall performance of LSTM compared to other experiments without feature selection. For example, the obtained results for testing data set show a good improvement (i.e., 6%) for the proposed method over balance data set. Fig. 6 explores the performance of LSTM in the training process. The classification error (i.e., RMSE) has a smooth convergence for balanced data with feature selection (i.e., blue line). Fig. 7 explores the loss convergence for the three experiments. It is clear that employing FS method helps LSTM to converge faster.

From the obtained results, we believe that the proposed method can enhance the overall performance of IDS inside cloud computing system.

TABLE I. FEATURES OF UNSW\_NB15 DATA SET.

Feature number	Feature Name	Type	Feature number	Feature Name	Type
1	id	Nominal	23	dtcpb	Integer
2	dur	Float	24	dwin	Integer
3	proto	Nominal	25	tcprrt	Float
4	service	Nominal	26	synack	Float
5	state	Nominal	27	ackdat	Float
6	spkts	Integer	28	smean	Integer
7	dpkts	Integer	29	dmean	Integer
8	sbytes	Integer	30	trans_depth	Integer
9	dbytes	Integer	31	response_body_len	Integer
10	rate	Integer	32	ct_srv_src	Integer
11	sttl	Integer	33	ct_state_ttl	Integer
12	dttl	Integer	34	ct_dst_ltm	Integer
13	sload	Float	35	ct_src_dport_ltm	Integer
14	dload	Float	36	ct_src_sport_ltm	Integer
15	sloss	Integer	37	ct_dst_src_ltm	Integer
16	dloss	Integer	38	is_ftp_login	Binary
17	sinpkt	Integer	39	ct_dtp_ltm	Integer
18	dinpkt	Integer	40	ct_src_ltm	Integer
19	sjit	Float	41	ct_srv_dst	Integer
20	djit	Float	42	ct_sm_ips_ports	Integer
21	swin	Integer	43	is_sm_ips_ports	Binary
22	stcpb	Integer	44	attack_cat	Nominal

TABLE II. PERCENTAGE OF ATTACKS IN UNSW-NB1 DATASET.

Attack type	Percentage%
Normal	87.94
Exploits	1.5
DoS	0.53
Backdoor	0.09
Analysis	0.09
Fuzzers	0.88
Generic	8.42
Reconnaissance	0.49
Shellcode	0.05
Worms	0.01

TABLE III. ORIGINAL AND BALANCED UNSW\_NB15 DATASET.

Dataset	Number of Normal	Number of Attacks	Total
Original Training	56000	119341	175341
Original Testing	37000	45332	82332
Balanced Training	119341	119341	238682
Balanced Testing	45332	45332	90664

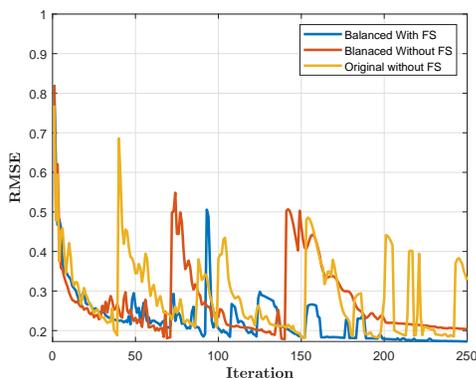


Fig. 6. LSTM Convergence for Original Training Data Set based on RMSE.

## VI. CONCLUSION AND FUTURE WORKS

This paper proposed a hybrid method between EBGa and LSTM to detect normal and abnormal network traffic.

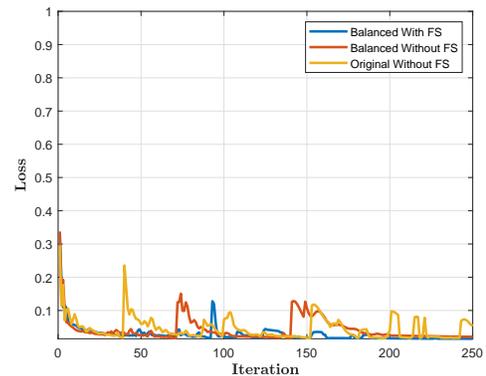


Fig. 7. LSTM Convergence for Original Training Data Set based on Loss.

EBGa works as a wrapper feature selection, while LSTM works as binary classifier. The proposed method employed as IDS for could computing system. We examined the proposed approach over a real public data set called UNSW-NB15. The original data set is imbalanced one. We handled the imbalanced data set using ADASYN method. The obtained results show the importance of feature selection method and its ability of enhancing the classification accuracy. In future work, different feature selection methods such as Harris Hawks Optimization (HHO), Gray Wolf Optimization (GWO), and Whale Optimization Algorithm (WOA) will be applied to reduce the search space and determine the most important features for IDS systems.

## REFERENCES

- [1] H. Alazzam, A. Sharieh, and K. E. Sabri, "A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer," *Expert Systems with Applications*, vol. 148, p. 113249, 2020. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0957417420300749>
- [2] O. Almomani, "A feature selection model for network intrusion detection system based on pso, gwo, ffa and ga algorithms," *Symmetry*, vol. 12, no. 6, p. 1046, 2020.

TABLE IV. COMPARISON BETWEEN DIFFERENT SETTING OVER THE BALANCED DATA SET.

	Balanced Data set with FS		Balanced Data set without FS		Original Data set without FS	
	Training	Testing	Training	Testing	Training	Testing
Accuracy	0.97	<b>0.91</b>	0.95	0.84	0.86	0.86
Sensitivity	0.95	<b>0.99</b>	0.94	0.84	0.96	0.88
Specificity	1.00	0.84	0.99	<b>0.85</b>	0.71	0.82
Precision	1.00	<b>0.88</b>	1.00	0.84	0.82	0.85
Recall	0.95	<b>0.99</b>	0.94	0.84	0.96	0.88
F-measure	0.98	<b>0.91</b>	0.97	0.86	0.89	0.87

- [3] A. Thakkar and R. Lohiya, "Attack classification using feature selection techniques: a comparative study," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2020.
- [4] Y. Zhu, J. Liang, J. Chen, and Z. Ming, "An improved nsga-iii algorithm for feature selection used in intrusion detection," *Knowledge-Based Systems*, vol. 116, pp. 74 – 85, 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0950705116304245>
- [5] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, 2016, pp. 21–26.
- [6] G. Zhao, C. Zhang, and L. Zheng, "Intrusion detection using deep belief network and probabilistic neural network," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 1. IEEE, 2017, pp. 639–642.
- [7] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, "High-dimensional and large-scale anomaly detection using a linear one-class svm with deep learning," *Pattern Recognition*, vol. 58, pp. 121–134, 2016.
- [8] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 2016, pp. 258–263.
- [9] Z. Wang, "The applications of deep learning on traffic identification," *BlackHat USA*, vol. 24, no. 11, pp. 1–10, 2015.
- [10] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *Ieee Access*, vol. 5, pp. 21 954–21 961, 2017.
- [11] O. Faker and E. Dogdu, "Intrusion detection using big data and deep learning techniques," in *Proceedings of the 2019 ACM Southeast Conference*, 2019, pp. 86–93.
- [12] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41 525–41 550, 2019.
- [13] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data environment," *Information Sciences*, vol. 513, pp. 386–396, 2020.
- [14] J. H. Holland, *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control and Artificial Intelligence*. Cambridge, MA, USA: MIT Press, 1992.
- [15] C.-L. Huang and C.-J. Wang, "A ga-based feature selection and parameters optimization for support vector machines," *Expert Systems with Applications*, vol. 31, no. 2, pp. 231 – 240, 2006. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0957417405002083>
- [16] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6.
- [17] Haibo He, Yang Bai, E. A. Garcia, and Shutao Li, "Adasyn: Adaptive synthetic sampling approach for imbalanced learning," in *2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, 2008, pp. 1322–1328.

# Evaluation of Collaborative Filtering for Recommender Systems

Maryam Al-Ghamdi<sup>1</sup>, Hanan Elazhary<sup>2</sup>, Aalaa Mojahed<sup>3</sup>

College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia<sup>1,2,3</sup>  
Computers and Systems Department Electronics Research Institute Cairo, Egypt<sup>2</sup>

**Abstract**—Recently, due to the increasing amount of data on the Internet along with the increase in products' purchasing via e-commerce websites, Recommender Systems (RS) play an important role in guiding customers to buy products they may prefer. Furthermore, these systems help the companies to advertise their products to the most potential customers, and therefore raise their revenues. Collaborative Filtering (CF) is the most popular RS approach. It is classified into memory-based and model-based filtering. Memory-based filtering is in turn classified into user-based and item-based. Several algorithms have been proposed for CF. In this paper, a comparison has been performed between different CF algorithms to assess their performance. Specifically, we evaluated K-Nearest Neighbor (KNN), Slope One, co-clustering and Non-negative Matrix Factorization (NMF) algorithms. KNN algorithm is representative of the memory-based CF approach (both user-based and item-based). The other three algorithms, on the other hand, are under the model-based CF approach. In our experiments, we used a popular MovieLens dataset based on six evaluation metrics. Our results reveal that the KNN algorithm for item-based CF outperformed all other algorithms examined in this paper.

**Keywords**—Co-clustering; collaborative filtering; KNN; NMF; recommender systems; slope one

## I. INTRODUCTION

Nowadays, most people tend to buy products from online websites and due to the huge amount of data available on the Internet, making the right decision to choose the most appropriate products has become more difficult. Thus, tools like Recommender Systems (RS) are very necessary to help them to make the right decisions.

RS can be defined as software tools and techniques that help the user in decision-making processes, such as what products to buy, what books to read, and what movies to watch [1]. Furthermore, these systems help the companies to raise their revenues. Amazon and eBay are examples of companies that strongly depend on RS to increase their sales and financial profits. RS can be generally classified into two main categories, Content-based Filtering (CBF), and Collaborative Filtering (CF) [1]. CBF is one of the simplest approaches in RS. It recommends to the users a list of items that are similar to the items they liked in the past. The system analyzes the item's textual information, such as item's descriptions and user's preferences, then finds the similar items to the ones they liked in the past. After that, CBF makes recommendations using some classification algorithms [2]. For example, the system recommends to the users books from the same genre of the books they already liked or recommends a product with a shape and color similar to what they liked before.

CF is the most popular recommender systems approach. It recommends items based on the user's past behavior as well as similar decisions made by other users. The first CF system that was proposed is Tapestry. It was developed by Goldberg et al. [3] in 1992. Tapestry is mainly developed to handle the problem of a huge stream of incoming documents via e-mail. They proposed a way to use CF, in addition to CBF, to filter documents coming from e-mails. Their simple idea of CF is that people help each other to filter these documents by recording their reactions to them. In this research, we focus on the CF approach only, since it is the most popular and generally more efficient in comparison to other approaches. The CF approach is categorized into memory-based and model-based [4]. In this paper, we evaluate and compare several algorithms under those two classes using a popular MovieLens dataset and based on six evaluation metrics.

The rest of this paper is structured as follows: Section II describes the different CF algorithms. Related work is summarized in Section IV. Evaluation metrics are presented in Section III. Section V discusses the research methodology that we adopted. Results are discussed in Section VI. Finally, a conclusion is provided in Section VII.

## II. COLLABORATIVE FILTERING

In this section we discuss the two classes of the collaborative filtering approach and the corresponding algorithms that we evaluate in this paper.

### A. Memory-based Approach

Memory-based or *neighborhood-based* approach uses user-item ratings matrix to generate the recommendations [5]. From this matrix, the system computes the similarities between users, or between items. Then, it saves computed similarity scores to a similarity matrix. There are several methods that have been used to calculate the similarities such as Euclidean, cosine, and mean squared distances.

The memory-based methods suffer from two main issues, which are sparsity and scalability [6]. In the sparsity case, it will be hard for the system to provide good recommendations due to the small number of items that each user rated. Scalability problem occurs when the numbers of users and items increase exceedingly. In such case, there will be a lot of information and it will be hard for the system to deal with it [6]. As previously noted, the memory-based approach is classified into user-based and item-based filtering [7].

a) User-based:

In the user-based approach, recommendations are made based on similar user preferences. K-Nearest Neighbor (KNN) is one of the algorithms that could be used in this approach. Equation (1) shows the prediction formula:

$$\hat{r}_{ui} = \mu_u + \frac{\sum_{v \in N_i^k(u)} sim(u, v) \cdot (r_{vi} - \mu_v)}{\sum_{v \in N_i^k(u)} sim(u, v)} \quad (1)$$

Where  $\hat{r}_{ui}$  is the predicted rating of user  $u$  for item  $i$ ,  $\mu_u$  is the mean of all ratings given by user  $u$  and  $sim(u, v)$  is the similarity value between users  $u$  and  $v$ . The value of  $sim(u, v)$  can be computed using cosine similarity measure as shown in the following equation:

$$sim(u, v) = \frac{\sum_{i \in I_{uv}} r_{ui} \cdot r_{vi}}{\sqrt{\sum_{i \in I_{uv}} r_{ui}^2} \cdot \sqrt{\sum_{i \in I_{uv}} r_{vi}^2}} \quad (2)$$

b) Item-based:

In the item-based approach, the system makes recommendations based on the similarities among items. KNN prediction formula for item-based CF is as follows:

$$\hat{r}_{ui} = \mu_i + \frac{\sum_{j \in N_i^k(i)} sim(i, j) \cdot (r_{uj} - \mu_j)}{\sum_{j \in N_i^k(i)} sim(i, j)} \quad (3)$$

Where  $\hat{r}_{ui}$  is the predicted rating of user  $u$  for item  $i$ ,  $\mu_i$  is the mean of all ratings given to item  $i$  and  $sim(i, j)$  is the similarity value between items  $i$  and  $j$ . The value of  $sim(i, j)$  can be computed using cosine similarity measure as follows:

$$sim(i, j) = \frac{\sum_{u \in U_{ij}} r_{ui} \cdot r_{uj}}{\sqrt{\sum_{u \in U_{ij}} r_{ui}^2} \cdot \sqrt{\sum_{u \in U_{ij}} r_{uj}^2}} \quad (4)$$

### B. Model-based Approach

To overcome the aforementioned issues of the memory-based approach, the model-based approach has been proposed. Model-based CF works by grouping different users into a small number of classes based on their ratings patterns. Many machine learning algorithms can be used to build such a model. In this research, we focused on three algorithms which are: Slope One, co-clustering, and NMF.

a) Slope one:

Lemire et al. [8] proposed a model-based CF algorithm called Slope One. One of strengths of this algorithm is that it takes into account two types of information, information about other users who rated the same item (similar to user-based), and information about other items that the same user rated before (similar to item-based).

We will illustrate the basis of the Slope One approach by an example. Suppose we have two users,  $A$  and  $B$ , and two items,  $i$  and  $j$  as shown in Table I. Item  $j$  is rated by both users ( $A$  and  $B$ ). User  $A$  gave it a rating of 2, while user  $B$  gave it a rating of 4. User  $A$  also gave item  $i$  a rating of 2.5. We notice that item  $i$  is rated more than  $j$  by  $2.5 - 2 = 0.5$ .

Now we can use this information to predict that user  $B$  will give item  $i$  a rating of  $4 + 0.5 = 4.5$ .

TABLE I. SLOPE ONE EXAMPLE.

	Item $i$	Item $j$
User $A$	2.5	2
User $B$	N/A	4

The process of the prediction is done by computing the average differences between the ratings of one item and another for users who rated both. The prediction formula for Slope One algorithm is as follows [8]:

$$\hat{r}_{ui} = \mu_u + \frac{1}{|R_i(u)|} \sum_{j \in R_i(u)} dev(i, j) \quad (5)$$

Where  $\hat{r}_{ui}$  is the predicted rating of user  $u$  for item  $i$ ,  $\mu_u$  is the mean of all ratings given by user  $u$  and  $R_i(u)$  is the set of items  $j$  rated by user  $u$  which also have at least one common user with item  $i$ .  $dev(i, j)$  is considered as the average difference between item  $i$ 's ratings ( $r_{ui}$ ) and item  $j$ 's ratings ( $r_{uj}$ ) as shown in the following equation [8]:

$$dev(i, j) = \frac{1}{|U_{ij}|} + \sum_{u \in U_{ij}} r_{ui} - r_{uj} \quad (6)$$

b) Co-clustering:

Clustering is a powerful technique in the data mining field that refers to the process of grouping objects in a way that similar objects will belong to the same group or cluster. There are various clustering methods that could be used based on the type of the data. In case of CF, the data is the user-item ratings matrix, so we need a way to cluster rows and columns. This process is called co-clustering. In this paper, we used co-clustering algorithm that has been proposed by George et al. in [9]. This algorithm is based on weighted co-clustering algorithm proposed in [10]. The idea is to compute the neighborhoods for the users and items via co-clustering and then make predictions according to the average ratings of the co-clusters while taking into consideration the users and items individual biases. The prediction formula is as the following:

$$\hat{r}_{ui} = \overline{C_{ui}} + (\mu_u - \overline{C_u}) + (\mu_i - \overline{C_i}) \quad (7)$$

Where  $\overline{C_{ui}}$  is the average rating of co-cluster  $C_{ui}$ , and  $\overline{C_u}$  is the average rating of  $u$ 's cluster,  $\overline{C_i}$  is the average rating of  $i$ 's cluster,  $\mu_u$  is user  $u$ 's average rating and  $\mu_i$  is item  $i$ 's average rating.

It is worth noting that if the user is new (not existing before) but the item is known, the prediction value  $\hat{r}_{ui}$  will be the average rating given to item  $i$ . If the item is unknown (new) but the user is known, the prediction value  $\hat{r}_{ui}$  will be the average rating given by user  $u$ . In case both the user and the item are unknown, the prediction value of  $\hat{r}_{ui}$  will be the global average of all the existing ratings.

c) *Non-negative matrix factorization (NMF):*

Matrix Factorization-based (MF-based) modeling is one of the CF approaches that are widely used in recent years. It is highly accurate and scalable in several cases [11]. MF-based models work by decomposing the user-item matrix into two low-rank matrices. The first one is user-features matrix and the other is item-features matrix. We can make any predictions by calculating the dot product of two lower dimensionality rectangular matrices.

Various matrix factorization algorithms have been proposed, such as Singular Value Decomposition (SVD), Probabilistic Matrix Factorization (PMF) and Non-negative Matrix Factorization (NMF). In this research, we focus on NMF as an example of the MF approach. In this algorithm, the prediction  $\hat{r}_{ui}$  is computed as follows:

$$\hat{r}_{ui} = q_i^T p_u \quad (8)$$

Where  $q_i$  is an item factors matrix and  $p_u$  is user factors matrix.

Different optimization algorithms could be used in MF-based models. The NMF algorithm uses Stochastic Gradient Descent (SGD) optimization algorithm. At each step of the SGD procedure, the factors (features)  $f$  of user  $u$  and item  $i$  are updated as follows:

$$p_{uf} \leftarrow p_{uf} \cdot \frac{\sum_{i \in I_u} q_{if} \cdot r_{ui}}{\sum_{i \in I_u} q_{if} \cdot \hat{r}_{ui} + \lambda_u |I_u| p_{uf}} \quad (9)$$

$$q_{if} \leftarrow q_{if} \cdot \frac{\sum_{u \in U_i} p_{uf} \cdot r_{ui}}{\sum_{u \in U_i} p_{uf} \cdot \hat{r}_{ui} + \lambda_i |U_i| q_{if}} \quad (10)$$

where  $\lambda_u$  and  $\lambda_i$  are regularization parameters.

### III. EVALUATION METRICS

Several metrics have been proposed to evaluate the performance of recommender system's algorithms. In addition to training time and testing time, examples of those metrics include Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), Fraction of Concordant Pairs (FCP), and coverage. In the following subsections, we will present each of the latter four metrics in details.

#### A. Mean Absolute Error (MAE)

MAE computes the average absolute difference between the observed and predicted ratings. The MAE is given by:

$$MAE = \frac{1}{|\hat{R}|} \sum_{\hat{r}_{ui} \in \hat{R}} |r_{ui} - \hat{r}_{ui}| \quad (11)$$

Where  $|\hat{R}|$  is the total number of predicted ratings,  $r_{ui}$  is the true rating value that user  $u$  gave to item  $i$  and  $\hat{r}_{ui}$  is the predicted rating value that user  $u$  gave to item  $i$ . A lower value of MAE means the predictions are more accurate and so the performance of the algorithm is better.

#### B. Root Mean Squared Error (RMSE)

RMSE is very similar to MAE, except that instead of summing the absolute values of the rating prediction errors, we sum their squares using the following formula:

$$RMSE = \sqrt{\frac{1}{|\hat{R}|} \sum_{\hat{r}_{ui} \in \hat{R}} (r_{ui} - \hat{r}_{ui})^2} \quad (12)$$

Where  $|\hat{R}|$  is the total number of predicted ratings,  $r_{ui}$  is the true rating value that user  $u$  gave to item  $i$  and  $\hat{r}_{ui}$  is the predicted rating value that user  $u$  gave to item  $i$ . A lower value of RMSE means the predictions are more accurate and so the algorithm's performance is better.

#### C. Fraction of Concordant Pairs (FCP)

One of the issues for MAE and RMSE is that they don't take into consideration rating scales that vary from one user to another [12]. Thus, in addition to MAE and RMSE, we have used FCP to evaluate the algorithms. It is calculated using equation 13 [12] such that a higher value of FCP means the algorithm is more accurate.

$$FCP = \frac{n_c}{n_c + n_d} \quad (13)$$

Where,

$$n_c = \sum | \{ (i, j) \mid r_{ui} > r_{uj} \text{ and } \hat{r}_{ui} > \hat{r}_{uj} \} | \quad (14)$$

$$n_d = \sum | \{ (i, j) \mid r_{ui} < r_{uj} \text{ and } \hat{r}_{ui} < \hat{r}_{uj} \} | \quad (15)$$

#### D. Coverage

Coverage refers to the percentage of items that the system was able to successfully recommend. It is computed using the following formula [13]:

$$Coverage = \frac{n_{pi}}{n_i} \quad (16)$$

Where  $n_i$  is the total number of items that the system predict and  $n_{pi}$  is the total number of items that were successfully predicted by the system.

### IV. RELATED WORK

This section discusses the research papers that compared different RS algorithms. Benin in [14] made a comparison of RS for crowdfunding projects. This study aims to compare different types of RS which are CBF, CF and hybrid RS, which combines both CBF and CF. The popular MovieLens-1M [15] dataset was used in the experiments. To evaluate the algorithms, they did both quantitative and qualitative analysis. The quantitative analysis relied on RMSE and MAE. The qualitative analysis, which is the analysis of the quality of the produced recommendations, was achieved via eyeballing-produced recommendations. However, evaluating the recommendations using this method is considered primitive and

imprecise since it may vary from one point of view to another. This study concluded that hybrid RS outperform CF and CBF.

Arsan et al. [16] made a comparison between user-based and item-based algorithms to observe their performance and accuracy. Since similarity measures play an important role in the user-based and item-based predictions accuracy, they applied various similarity measures, which are Euclidean distance, log likelihood ratio, Pearson correlation coefficient, Tanimoto coefficient, uncentered cosine, and Spearman correlation coefficient. The authors applied the algorithms to the MovieLens-100K dataset. MAE and RMSE were used to evaluate the algorithms' accuracy. Time spent to make the recommendations was also calculated. Based on their experiments, they concluded that item-based algorithms perform better than user-based algorithms.

Najafi et al. [17] assessed the item-based CF and the MF-based FunkSVD algorithms. The idea of their study is to compare the performance of these algorithms when the data is scaled. MovieLens 100k and MovieLens-1M were used. They used MAE and RMSE to evaluate the algorithms. Their results shows that the FunkSVD algorithm is more accurate than the item-based CF when the data is scaled.

Lemire et al. [8] proposed three algorithms which are Slope One, weighted Slope One and bi-polar Slope One. They compared their proposed algorithms with four other algorithms which are: bias from mean, adjusted cosine item-based (model-based), per user average and Pearson (memory-based) algorithms. Both EachMovie [18] and MovieLens datasets were used in their experiments. They tested the algorithms using the evaluation metric MAE. Their results showed that the proposed Slope One algorithms achieved comparable accuracy to the other selected algorithms.

George and Merugu [9] proposed a novel CF algorithm which is based on weighted co-clustering algorithm [10]. They compared their proposed algorithm with SVD, NMF, and classic correlation-based CF algorithms. The experiments were applied on MovieLens-100K dataset. The MAE was used to compute the prediction accuracy. Their results indicate that their proposed algorithm has a high accuracy with much lower computational cost in comparison to the other algorithms.

Our comparison is different from the above-discussed papers in many aspects. First, we made a comparison between memory-based (both user-based and item-based) KNN algorithms and model-based (NMF, Slope One, and co-clustering) algorithms. Besides, we evaluated these algorithms using six different metrics which are MAE, RMSE, FCP, coverage, training time and testing time.

## V. METHODOLOGY

This section discusses the methodology used to complete this research. Section V-A introduces the dataset used in the experiments and some of its statistical analysis results. Section V-B describes our experimental setup including hyperparameter tuning and used libraries.

### A. Dataset Exploration

We have used MovieLens-25M dataset [15], which is one of the most popular datasets used by researchers in the field

of CF. It describes a 5-star rating and tagging activity. It contains 62,423 movies, 25,000,095 ratings and 1,093,360 tag applications. However, in this research, we have focused on the CF algorithms, where only the ratings data are considered. The data were created by 162,541 users throughout 24 years and 10 months, from 9 January 1995 to 21 November 2019 and it was released on December 2019. In this dataset, the users are randomly selected and each user is represented merely by an Id [15]. Fig. 1 shows the ratings histogram for the MovieLens dataset. From the figure, we notice that 26.56% of the ratings are 4.0 and 19.59% are 3.0. This indicates that users tend to rate the movies they preferred. However, in our experiment, we haven't used the whole dataset because the memory-based filtering algorithms don't scale very well to such a big data size. So, we have randomly selected 100,000 ratings of 54,778 users on 10,271 movies with a sparsity of 99.9822%.

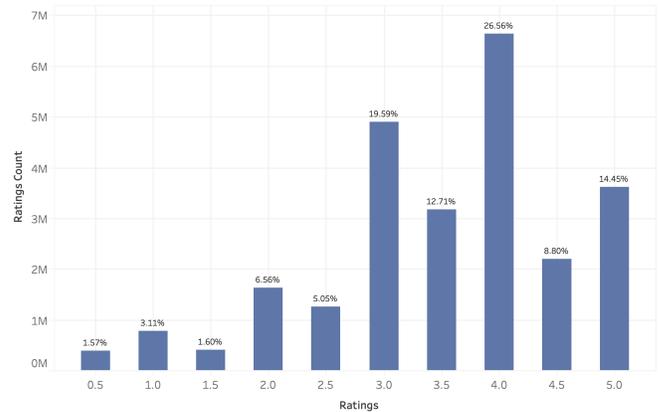


Fig. 1. Ratings Distribution for MovieLens Dataset.

### B. Experimental Setup

In this section, we discuss our experimental setup. First, in our experiment with the KNN algorithm, we selected cosine similarity measure to compute the similarities between users or items. Second, in order to achieve the highest machine learning predictive model performance, hyperparameter values need to be selected carefully. This is one of the important steps in building any machine learning model [19]. Table II shows the hyperparameters, the corresponding test values that we selected to optimize the algorithms' performance and the best values that we obtained. The test values were chosen with the help of the default values in the library [20] and values found in other studies in the related work.

Third, for training, we adopted K-fold cross validation, with k equals 5. In this method, the dataset is divided into K folds and the model is trained K times, each time on different K-1 folds, and then tested on the remaining fold. The average performance of the K results is then calculated. K-fold cross validation approach avoids overfitting to the particular division of the training and testing sets that may appear in the other approaches, which split the data into training and testing sets and run the algorithm once [1], [21].

The code used in this research was implemented mainly using Python. Surprise library was used, which is a Python

TABLE II. LIST OF HYPERPARAMETER VALUES

Method	Hyperparameter	Test values	Best value
KNN	k, number of neighbors	10, 20, 30	10
	n_cltr_u, number of user clusters	3, 5	3
Co-clustering	n_cltr_i, number of item clusters	3, 5	5
	n_factors, the number of factors	5, 10, 15	15
NMF	n_epochs, the number of iterations of SGD	15, 20, 25	20

Scikit library for CF [20]. In addition, Pandas [22] and Numpy [23] libraries were used. All the work is done using MacBook Pro with CPU 2.5 GHz Intel Core i5 and 16 GB RAM. It is worth noting that in order to visualize the dataset and our results in graphs, Tableau desktop software - professional edition, version 2020.3 was used.

## VI. RESULTS AND DISCUSSION

In this section, we will discuss the results of our experiments. As observed in Fig. 2, the item-based KNN CF algorithm outperformed all the other algorithms in terms of MAE, RMSE and FCP. It also took less training time compared to the others. This is at the expense of taking longer testing time in comparison to Slope One, NMF, and co-clustering algorithms. Regarding the user-based KNN algorithm, it's noticeable that it is less effective in terms of accuracy and speed; it was too slow in both training and testing. These results were expected since our dataset contains 10,271 movies only while the number of users is as large as 54,778. This surely has a significant effect in helping the item-based CF algorithm to work very well compared to others.

However, when we look at the coverage results, all the algorithms except co-clustering were not able to make predictions for all the testing dataset. Specifically, they were able to predict only about 57% of the dataset while co-clustering was able to predict 100% of it. The full results for all the algorithms are reported in Table III.

## VII. CONCLUSION

In this paper, we have performed a comparison between five different CF algorithms to assess their performance. The selected algorithms are KNN for user-based, KNN for item-based, Slope One, co-clustering, and NMF. The algorithms have been evaluated using six metrics which are MAE, RMSE, FCP, coverage, training time and testing time. Our results show that the KNN algorithm for item-based CF outperformed all other algorithms examined in this paper. It achieved the lowest error values and thus the highest accuracy. As future work, we plan to run the algorithms on a larger sample of the dataset to assess their scalability. In addition, we plan to consider more algorithms and more evaluation metrics.

## REFERENCES

[1] F. Ricci, L. Rokach, B. Shapira, and P. B. Kantor, *Recommender Systems Handbook*. Springer US, 2011. [Online]. Available: <http://dx.doi.org/10.1007/978-0-387-85820-3>

[2] X. Su and T. M. Khoshgoftaar, "A survey of collaborative filtering techniques," *Advances in Artificial Intelligence*, vol. 2009, pp. 1–19, 2009. [Online]. Available: <http://dx.doi.org/10.1155/2009/421425>

[3] D. Goldberg, D. Nichols, B. M. Oki, and D. Terry, "Using collaborative filtering to weave an information tapestry," *Communications of the ACM*, vol. 35, no. 12, pp. 61–70, 1992. [Online]. Available: <http://doi.acm.org/10.1145/138859.138867>

[4] L. E. Molina and S. Bhulai, "Recommendation system for netflix," 2018.

[5] M.-P. T. Do, D. Nguyen, and L. Nguyen, "Model-based approach for collaborative filtering," in *6th International Conference on Information Technology for Education*, Ho Chi Minh City, Vietnam, August 2010, pp. 217–228.

[6] S. Gong, H. Ye, and H. Tan, "Combining memory-based and model-based collaborative filtering in recommender system," in *2009 Pacific-Asia Conference on Circuits, Communications and Systems*, Chengdu, China, May 2009, pp. 690–693.

[7] X. Liang, Z. Xia, L. Pang, L. Zhang, and H. Zhang, "Measure prediction capability of data for collaborative filtering," *Knowledge and Information Systems*, vol. 49, no. 3, pp. 975–1004, 2016.

[8] D. Lemire and A. Maclachlan, "Slope one predictors for online rating-based collaborative filtering," *Proceedings of the 2005 SIAM International Conference on Data Mining, SDM 2005*, vol. 5, 2007.

[9] T. George and S. Merugu, "A scalable collaborative filtering framework based on co-clustering," in *Fifth IEEE International Conference on Data Mining (ICDM'05)*, November 2005, pp. 625–628.

[10] A. Banerjee, I. Dhillon, J. Ghosh, S. Merugu, and D. S. Modha, "A generalized maximum entropy approach to bregman co-clustering and matrix approximation," in *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '04. New York, NY, USA: Association for Computing Machinery, December 2004, pp. 509–514. [Online]. Available: <https://doi-org.sdl.idm.oclc.org/10.1145/1014052.1014111>

[11] X. Luo, M. Zhou, Y. Xia, and Q. Zhu, "An efficient non-negative matrix-factorization-based approach to collaborative filtering for recommender systems," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1273–1284, 2014.

[12] Y. Koren and J. Sill, "Collaborative filtering on ordinal user feedback," in *Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence*, ser. IJCAI '13. Beijing, China: AAAI Press, Jun 2013, pp. 3022–3026. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2540128.2540570>

[13] F. Hdioud, B. Frikh, and B. Ouhbi, "A comparison study of some algorithms in recommender systems," in *2012 colloquium in information science and technology*. IEEE, Oct 2012, pp. 130–135.

[14] A. C. Benin, "A comparison of recommender systems for crowdfunding projects," *Adriano Carmiel Benin*, July 2018.

[15] F. M. Harper and J. A. Konstan, "The movielens datasets: History and context," *ACM Trans. Interact. Intell. Syst.*, vol. 5, no. 4, pp. 19:1–19:19, 2015. [Online]. Available: <http://doi.acm.org/10.1145/2827872>

[16] T. Arsan, E. Köksal, and Z. Bozkus, "Comparison of collaborative filtering algorithms with various similarity measures for movie recommendation," *International Journal of Computer Science, Engineering and Applications (IJCSA)*, vol. 6, no. 3, pp. 1–20, 2016.

[17] Z. Salam Patrous and S. Najafi, "Evaluating prediction accuracy for collaborative filtering algorithms in recommender systems," *KTH Royal Institute of Technology*, 2016.

[18] P. McJones, "Eachmovie Collaborative Filtering Dataset, DEC Systems Research Center," <http://www.research.compaq.com/src/eachmovie/>, 1997.

[19] J. Gaudillo, J. J. R. Rodriguez, A. Nazareno, L. Baltazar, J. Vilela, R. Bulalacao, M. Domingo, and J. Albia, "Machine learning approach to single nucleotide polymorphism-based asthma prediction," *PLOS ONE*, vol. 14, p. e0225574, 2019.

TABLE III. RESULTS.

Metric	KNN (User-based)	KNN (Item-based)	Slope One	Co-clustering	NMF
MAE	0.8891	0.8191	0.8934	0.8934	0.8940
RMSE	1.1513	1.0446	1.1575	1.1437	1.1365
FCP	0.4883	0.5202	0.4928	0.5097	0.5138
Coverage	57.07%	57.07%	57.07%	100%	57.07%
Training Time (in sec)	196.2037	3.8485	4.3010	13.7191	4.8723
Testing Time (in sec)	1.5243	0.3690	0.3147	0.2202	0.3043

- [20] N. Hug, "Surprise: A python library for recommender systems," *Journal of Open Source Software*, vol. 5, no. 52, p. 2174, 2020. [Online]. Available: <https://doi.org/10.21105/joss.02174>
- [21] K. Falk, *Practical recommender systems*. Shelter Island, NY: Manning Publications, 2019.
- [22] T. pandas development team, "pandas-dev/pandas: pandas," 2020. [Online]. Available: <https://doi.org/10.5281/zenodo.3509134>
- [23] C. R. Harris, K. J. Millman, S. J. van der Walt, R. Gommers, P. Virtanen, D. Cournapeau, E. Wieser, J. Taylor, S. Berg, N. J. Smith, R. Kern, M. Picus, S. Hoyer, M. H. van Kerkwijk, M. Brett, A. Haldane, J. F. del R'io, M. Wiebe, P. Peterson, P. G'erald-Marchant, K. Sheppard, T. Reddy, W. Weckesser, H. Abbasi, C. Gohlke, and T. E. Oliphant, "Array programming with NumPy," *Nature*, vol. 585, no. 7825, pp. 357–362, 2020. [Online]. Available: <https://doi.org/10.1038/s41586-020-2649-2>

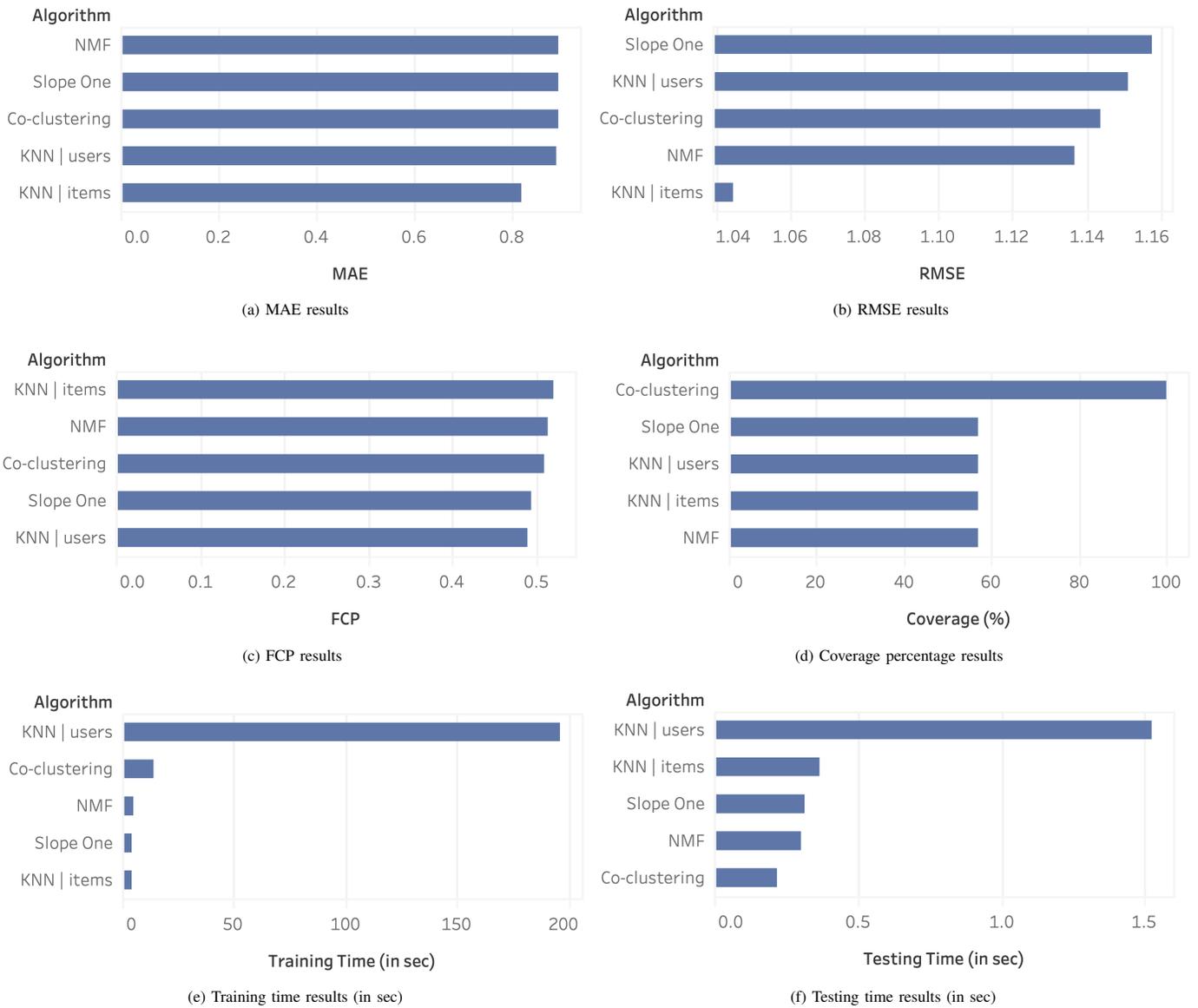


Fig. 2. Results for all Algorithms.

# Deployment and Migration of Virtualized Services with Joint Optimization of Backhaul Bandwidth and Load Balancing in Mobile Edge-Cloud Environments

Tarik Chanyour\*<sup>1</sup>, Mohammed Ouçamah Cherkaoui Malki<sup>2</sup>  
FSDM, LPAIS  
Sidi Mohamed Ben Abdellah University  
P.O. Box 1796, Atlas-Fez, Morocco.

**Abstract**—Mobile edge-cloud computing environments appear as a novel computing paradigm to offer effective processing and storage solutions for delay sensitive applications. Besides, the container based virtualization technology becomes solicited due to its natural lightweight and portability as well as its small migration overhead that leads to seamless service migration and load balancing. However, with the mobility property, the users' demands in terms of the backhaul bandwidth is a critical parameter that influences the delay constraints of the running applications. Accordingly, a Binary Integer Programming (BIP) optimization problem is formulated. It minimizes the users' perceived backhaul delays and enhances the load-balancing degree in order to offer more chance to accept new requests along the network. Also, by introducing bandwidth constraints, the available user backhaul bandwidth after the placement are enhanced. Then, the adopted methodology to design two heuristic algorithms based on Ant Colony System (ACS) and Simulated Annealing (SA) is presented. The proposed schemes are compared using different metrics, and the benefits of the ACS-based solution compared to the SA-based as well as a genetic algorithm (GA) based solutions are demonstrated. Indeed, the normalized cost and the total backhaul costs are given by more optimal values using the ACS algorithm compared to the other solutions.

**Keywords**—Mobile edge-cloud computing; delay-sensitive services; container migration; container deployment; backhaul bandwidth; load balancing

## I. INTRODUCTION

Mobile Edge Computing (MEC) is an emerging distributed computing paradigm that can deliver timely services to mobile users [1], [2]. They generally use resource-limited smart mobile devices (SMD) that allow them to run indispensable smart applications related to social networking, learning, businesses and entertainment. To reinforce privacy, reduce latency, preserve bandwidth and offer location-awareness, MEC enables computation and storage at the edge of the network using a set of edge nodes (EN). These nodes are resource-rich network cells or edge servers (ES) that are deployed in close proximity of the end-users and offer virtualized services to allow offloading of the mobile applications' workloads [3]. The use of these applications leads to appear new constraints related to mobility, limited energy, limited computational capacity and short latency.

The MEC model uses the virtualization techniques to master the resource allocation operations for Virtual Services (VSs) [4]. These VSs are often placed, migrated or replicated

over the ENs according to the users' locations and resources availability while considering constraints such as QoS, load balancing and energy. Besides, the new container-based lightweight virtualization solution is intended to decrease the communication network overhead and enhance continuity and quality of services. Though, especially with the user's mobility intrinsic property that is mostly frequent and unpredictable and the limited coverage of nodes, a guaranteed QoS for the deployed virtualized services is the most critical issue [5]. Indeed, when the user moves far from the edge server that deploys the corresponding virtualized service, the service response time becomes significant and can hamper the smooth running of the service. Therefore, a service migration [6] process in this case becomes important to make the service more interactive and guarantee its continuity. But, due to the high cost of this process regarding its time and the consumption of the available network bandwidth and other resources, the migration decision is very critical. Actually, with the non-negligible migration overhead, frequent migration according to the user's movement cannot be tolerated in all network conditions, whereas limited migration leads to the accumulation of communication delays which may degrade the QoS.

Service migration has sprung up recently as a leading problem in MEC networks. It involves complex procedures to dynamically move running services from one edge node to another. It becomes solicited in different edge management procedures, such as service failures handling, load balancing, mobile workloads offloading handling, etc. Also, to guarantee service-level agreements (SLA) or seamless services, it has to meet many constraints related to the available network and computing resources, the latencies' order of magnitude as well as the users' mobility [7]. The migration decisions are taken while optimizing a general cost or profit function that is evaluated in a long-term or short-term scenarios. Its formulation uses many metrics such as the migration duration, service downtime duration, network resources consumption, etc. However, a precise evaluation of these metrics remains a major problem for a good modelling of this problem. On the one hand, because of the great diversity and the strong dynamism of the parameters as well as the mobility of the users. On the other hand, because of the limitation of the resources involved in the migration which accentuates the constraints and limits the number of possible solutions.

## II. RELATED WORKS

With the high-mobility characteristic in the context of Vehicular Edge Network, the authors of [8] considered a delay-based cost function involving wireless transmission, backhaul and computing delays. They examined the problem of joint service migration and mobility optimization with minimum migration cost and travel time. To solve the problem, a multi-agent deep reinforcement learning algorithm was proposed. In [9], the authors use migration frequency and migration time as the migration cost and suggest a QoS aware solution to enhance the handover operations by exchanging additional information in order to perform service migration.

With the user mobility awareness assumption and QoS concerns for efficient service migration in MEC networks, many relevant works target service migration optimization. The work in [10] uses the follow-me edge concept to derive a service performance optimization problem constrained to a long-term cost budget to decide the service migration. The decision metrics include the Computing and Communication delays plus the migration cost. The long-term optimization problem is decomposed using Lyapunov optimization then approximated based on Markov approximation to derive a near-optimal solution with fast convergence rate. Moreover, based on this last concept to guarantee high availability and prop ultra-low latency, in [11] the authors studied four container-based migration strategies. They considered both predefined and unknown path scenarios. The work in [12] considered a cost function with a combination of three metrics: the topology cost that depends on the network structure and routing mechanism, the user-perceived delay and the risk of location privacy leakage. They modelled the migration procedure as a Markov Decision Process (MDP) problem, and propose a modified policy iteration algorithm to find the optimal decision. Also, a distance-based MDP was proposed in [13] to optimize the trade-off between the user-experienced delay and migration cost while considering the distance separating the user and the service locations. The work in [14] considered a dynamic task migration problem with delays, tasks' deadlines and user mobility consideration. The objective function to maximize was the number of tasks with guaranteed deadlines.

However, the mobility information is usually unavailable in real world due to privacy and inaccuracy issues. With this consideration, several recent works tackled the optimization of service or container migration from various perspectives. The work in [15] studied container migration in edge networks using a joint load balancing and migration cost minimization model. The migration cost encompasses two main metrics: network transmission delay and container migration downtime. They designed a migration solution based on a modified Ant Colony System algorithm. In [16] a live migration framework of container-based offloading services is presented. The basic optimization idea consist in sharing common storage layers across the edge hosts. Also in [17], the authors addressed the high network consumption problem while migrating virtual machines within cloud-edge fusion computing. They proposed heuristic algorithms to balance migration and communication costs.

The rest of this work is organized as follows. The system's model is describe in Section III. The obtained optimization problem is presented in Section IV, and its resolution's ap-

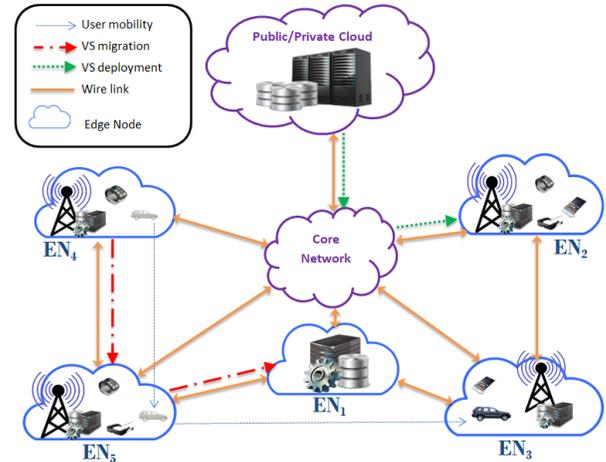


Fig. 1. Mobile Edge-Cloud System Architecture.

proaches are summarized in Section V. Evaluation and results are presented in section VI. Finally, Section VII concludes the paper.

## III. USER'S BACKHAUL AND LOAD BALANCING AWARE MIGRATION AND DEPLOYMENT OF CONTAINERS (UBL-MDC)

In this section, the need to optimise a multiple criteria decision-making problem in the proposed edge-cloud architecture is shown. Then, the involved cost functions as well as the final overall objective function to optimize is formulated.

### A. System Model

In this paper, the service deployment and migration problem from the perspective of an edge-cloud service provider is studied. As shown in Fig. 1, an edge-cloud network that uses a public/private cloud (PC) and a set of Edge Nodes (ENs) within a 2-D geographical local area is considered. Each EN is equipped with an Edge Server (ES) that can be hosted in a Base Station (BS) that offers access to the wireless communication network for all SMDs in its coverage, or simply deployed to offer to the network more processing and storage capabilities. In this last case, the server is called independent edge server and denoted (IS). For ease of use, an EN or its ES are indifferently used, while the edge-cloud server  $i$  is denoted  $s_i$ . A given ES within a BS serves the SMDs within the coverage area of the BS or other remote ones, whereas an independent ES serves only remote SMDs. The PC is supposed to have unlimited capacity, whereas all ESs are supposed heterogeneous with limited resources. Also, each ES can provide a set of independent virtualized services (VS) using the container-based lightweight virtualization technology where each running service uses a container instance and serves one SMD only. The set of all available edge-cloud servers is denoted  $\mathcal{S} = \{s_1, s_2, \dots, s_{\sigma_s}\}$  where  $\sigma_s$  is the number of servers. For ease of use, the set of all involved containers is denoted  $\mathcal{C} = \{c_1, c_2, \dots, c_{\sigma_c}\}$  where  $\sigma_c$  is the number of containers.

1) *UBL-MDC Variables*: To model the involved operations in the studied system, the decision variables are presented:

The migration binary decision variable of container  $i$  from its edge server  $s_i^c$  to EN  $j$  is denoted  $\alpha_{i,j}$  where  $\alpha_{i,j} = 1$  refers to the decision to migrate  $c_i$  from  $s_i^c$  to  $j$ , otherwise,  $\alpha_{i,j} = 0$ .

$$\alpha_{i,j} \in \{0; 1\} \quad ; i \in \mathcal{C}; j \in \mathcal{S} \quad (1)$$

Additionally, when migrating container  $i$  from its edge server  $s_i^c$  to  $j$  the decision variable to select the migration path among the possible paths set  $\mathcal{P}_{s_i^c, j}$  is the binary variable  $\beta_{i,j}^k$  where  $\beta_{i,j}^k = 1$  refers to the decision to use the  $k$ -th path in  $\mathcal{P}_{s_i^c, j}$  to migrate  $i$  from edge server  $s_i^c$  to  $j$ , otherwise  $\beta_{i,j}^k = 0$ .

$$\beta_{i,j}^k \in \{0; 1\} \quad ; i \in \mathcal{C}; j \in \mathcal{S}; k \in \mathcal{P}_{s_i^c, j} \quad (2)$$

2) *Paths and delay*: The SMDs get access to the ESs via wireless channels, while the nearby ENs are connected to each other in wired manner using high speed Ethernet cables or optical fibers. The MEC network topology is given by the set of nodes  $\mathcal{S}$  and the set of links relying them. The set of links is denoted  $\mathcal{L}$  which can be defined as  $\mathcal{L} = \{\mathcal{L}_{j,j'} | j \in \mathcal{S}; j' \in \mathcal{S} \setminus \{j\}\}$  where  $\mathcal{L}_{j,j'}$  is one hop link between ES  $s_j$  and  $s_{j'}$ . Also,  $\mathcal{P}_{s_i^c, j}$  is used to denote the set of feasible<sup>1</sup> paths connecting ESs  $s_i^c$  and  $j$  that can serve to migrate container  $c_i$  located in ES  $s_i^c$  to server  $s_j$ . Without loss of generality, we assume that the set  $\mathcal{P}_{s_i^c, j}$  is precalculated and given while deciding the containers migration. Then,  $\mathcal{P}$  is used to denote the set of all sufficient paths connecting all pairs of distinct nodes  $(j, j')$  defined as:

$$\mathcal{P} = \{\mathcal{P}_{j,j'} / j \in \mathcal{S}; j' \in \mathcal{S} \setminus \{j\}\} \quad (3)$$

Each path  $p_k$  in  $\mathcal{P}_{s_i^c, j}$  is an ordered set of distinct links of length  $|p_k|$  such that  $p_k = (\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_{|p_k|})$ . Here, the source node of link  $\mathcal{L}_1$  is  $s_i^c$  and the target node of the last link  $\mathcal{L}_{|p_k|}$  is  $j$ . For the remaining links, the source node of link  $\mathcal{L}_\ell$  is the target node of link  $\mathcal{L}_{\ell-1}$  and the target node of link  $\mathcal{L}_\ell$  is the source node of link  $\mathcal{L}_{\ell+1}$ . Fig. 2 shows a network topology example given by a set of five ESs  $\mathcal{S} = \{s_1, s_2, s_3, s_4, s_5\}$  where  $\sigma_s = 5$  and six wire links denoted:  $\mathcal{L} = \{\mathcal{L}_{s_1, s_2}, \mathcal{L}_{s_1, s_3}, \mathcal{L}_{s_2, s_3}, \mathcal{L}_{s_1, s_4}, \mathcal{L}_{s_1, s_5}, \mathcal{L}_{s_4, s_5}\}$ . Also, the dotted links show a migration path instance  $p_1$  with its ordered links set given by  $p_1 = (\mathcal{L}_{s_2, s_1}, \mathcal{L}_{s_1, s_4})$ . Then, the set of possible paths connecting  $s_2$  and  $s_4$  is given by the following set  $\mathcal{P}_{2,4} = \{p_1, p_2, p_3, p_4\}$  where:  $p_1 = (\mathcal{L}_{s_2, s_1}, \mathcal{L}_{s_1, s_4})$ ,  $p_2 = (\mathcal{L}_{s_2, s_1}, \mathcal{L}_{s_1, s_5}, \mathcal{L}_{s_5, s_4})$ ,  $p_3 = (\mathcal{L}_{s_2, s_3}, \mathcal{L}_{s_3, s_1}, \mathcal{L}_{s_1, s_4})$  and  $p_4 = (\mathcal{L}_{s_2, s_3}, \mathcal{L}_{s_3, s_1}, \mathcal{L}_{s_1, s_5}, \mathcal{L}_{s_5, s_4})$ . In the proposed model each link  $\ell \in \mathcal{L}$  is characterized by its total available bandwidth  $b(\ell)$ . In addition, given the path  $p_k \in \mathcal{P}_{s_i^c, j}$  and the set  $\mathcal{L}$  of all  $\sigma_l$  links, the binary array  $\delta_{i,j}^k$  of length  $\sigma_l$  indicating membership of all links to  $p_k$  is defined. Accordingly, the binary indicators  $\delta_{i,j}^{k,\ell}$  of each link  $\ell \in \mathcal{L}$  can be computed using the paths in  $\mathcal{P}_{s_i^c, j}$  such that  $\delta_{i,j}^{k,\ell}$  takes 1 if link  $\ell$  in  $\mathcal{L}$  is crossed in path  $p_k \in \mathcal{P}_{s_i^c, j}$ , otherwise it takes 0.

<sup>1</sup>we assume that a restriction set of paths is sufficient to obtain the optimal solution without the need to consider all possible paths

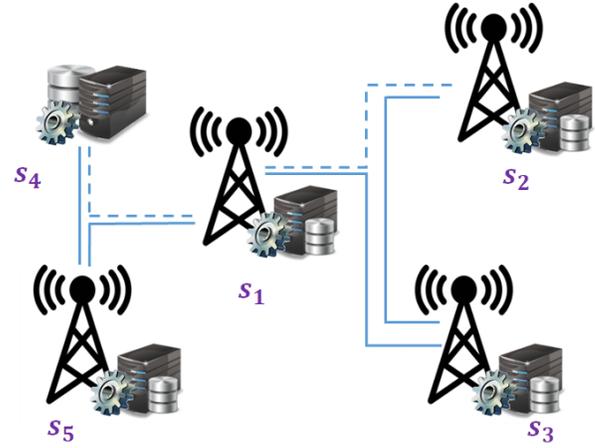


Fig. 2. Inter-Server Routing Paths Example.

Thus, each available path  $p_k \in \mathcal{P}_{j,j'}$  with the hop count  $\mathcal{H}_{j,j'}^k$ , offers an allocatable bandwidth  $\mathcal{B}_{j,j'}^k$ , (see Ref [15]) for multi hop data transmission. They are respectively expressed as:

$$\mathcal{B}_{j,j'}^k = \begin{cases} \infty & ; j=j' \\ \min_{\ell \in p_k} \{b(\ell)\} & ; j \neq j' \end{cases} ; j \in \mathcal{S}; j' \in \mathcal{S}; p_k \in \mathcal{P}_{j,j'} \quad (4)$$

$$\mathcal{H}_{j,j'}^k = \begin{cases} 0 & ; j=j' \\ |p_k| - 1 & ; j \neq j' \end{cases} ; j \in \mathcal{S}; j' \in \mathcal{S}; p_k \in \mathcal{P}_{j,j'} \quad (5)$$

Thus, when container  $c_i$  is transferred to node  $j$ , the backhaul bandwidth between its target node  $s_i^t$  and node  $j$  is given by:

$$\mathcal{B}_{i,j} = \begin{cases} \infty & ; s_i^t = j \\ \max_{k \in \mathcal{P}_{s_i^t, j}} \{\mathcal{B}_{s_i^t, j}^k\} & ; s_i^t \neq j \end{cases} ; i \in \mathcal{C}; j \in \mathcal{S} \quad (6)$$

which gives:

$$\mathcal{B}_i = \sum_{j \in \mathcal{S}} \alpha_{i,j} \mathcal{B}_{i,j} \quad ; i \in \mathcal{C} \quad (7)$$

3) *Containers*: Hereafter and for ease of notation, the following variables  $i, j, k, \ell, m$  are reserved to use for containers, servers, paths, links and resources respectively. Also, from now on, each container  $c_i$  is characterized by the following operating parameters:  $\Omega_i \triangleq \langle s_i^c, s_i^t, \mathcal{R}_i^{dem}, B_i^{ser}, x_i \rangle$  and the set of all operating parameters is denoted  $\Omega = \{\Omega_i\}_{i \in \mathcal{C}}$ . Here,  $s_i^c$  refers to the current server hosting container  $c_i$  and  $s_i^t$  refers to the actual node hosting the communication access point connecting the user of the service associated with container  $c_i$ . This node is considered as the best candidate target node for deployment or migration so that the best transfer paths for  $c_i$  are in  $\mathcal{P}_{s_i^c, s_i^t}$ . Actually, if a path is a feasible solution, container  $c_i$  will be migrated to the direct proximity of the user with no communication overhead. Also,  $\mathcal{R}_i^{dem} = \{r_{i,1}^d, r_{i,2}^d, \dots, r_{i,\sigma_r}^d\}$  represents the resources demand set of  $c_i$  and are given in the number of standardized virtual resource units. Here,  $\sigma_r$  is the number of resource types and  $r_{i,m}^d$  represents the required quantity in terms of resource  $r_m$  demanded by container  $i$ . Furthermore,  $B_i^{ser}$  concerns the minimum allowable data rate in terms of available bandwidth between  $c_i$  and its associated user after the migration or deployment procedures. The binary

$x_i$  indicates whether  $c_i$  is requested for a migration ( $x_i = 1$ ) or for a new deployment procedure ( $x_i = 0$ ).

4) *Edge servers resources*: Each ES provides a set of resources among multiple types including CPU, GPU, memory, storage, etc. Here, the set of possible  $\sigma_r$  resources is denoted  $\mathcal{R} = \{r_1, r_2, \dots, r_{\sigma_r}\}$ . Accordingly, every server  $j$  is characterized by its capacity set in terms of resources which is denoted  $\mathcal{R}_j^{cap} = \{r_{j,1}^c, r_{j,2}^c, \dots, r_{j,\sigma_r}^c\}$ . Here,  $r_{j,m}^c$  represents the maximum available quantity in terms of resource  $r_m$  that  $s_j$  can furnish.

Within the server  $j$  which runs a set of containers using the allocated resources, the deployment and migration will result in hosting new containers and freeing others conforming to the placement decisions. Thus, the utilization of resource  $r_m$  on ES  $j$  after the migration process is calculated as follows:

$$r_{j,m}^u(\alpha) = \sum_{i \in \mathcal{C}} \alpha_{i,j} r_{i,m}^d \quad ; j \in \mathcal{S}; m \in \mathcal{R}. \quad (8)$$

5) *Container deployment*: Deploying a service in this work refers to the transfer of unstarted components of the container (program codes, libraries, databases, etc.) from the storing node to a MEC server in order to make them available to serve a user. The provider's containers are stored in its PC or in a specific known EN depending on the requested service. Thus, all new incoming service requests from the users trigger service deployment from the hosting nodes to the ENs. Here, the same notation  $s_i^c$  is adopted to refer the hosting node of the requested container  $c_i$ .

6) *Container migration*: Migrating a container tries to achieve load balancing of ESs and increase the number of services that meet the execution latency constraints if necessary, this process involves the transfer of all runtime memory states as well as the related storage data that should be synchronized in the target ES. Furthermore, migration traffic routing in MEC networks not only helps to significantly reduce services downtime and interruption by selecting the best routing paths, but it protect the network from route failure. Indeed, if some links are in use or completely fail, alternate paths can be selected to redirect and salvage the data flows. Accordingly, a container migration decision has to found the expedited path to route the migration flows while avoiding the network congested links.

The important notations used are summarized in Table I.

TABLE I. MAIN NOTATIONS

Notation	Definition
$\mathcal{C}$	The set of containers
$\mathcal{S}$	The set of edge-cloud servers
$\mathcal{L}$	The set of links
$\sigma_c, \sigma_s, \sigma_r$	The total number of containers, servers, resources
$\mathcal{P}_{j,j'}$	The set set of sufficient paths connecting servers $s_j$ and $s_{j'}$
$\mathcal{B}_{j,j'}^k$	The bandwidth of path $p_k \in \mathcal{P}_{j,j'}$
$\mathcal{H}_{j,j'}^k$	The hop count of path $p_k \in \mathcal{P}_{j,j'}$
$\mathcal{B}_i^k$	The backhaul bandwidth associated with container $c_i$
$\Omega_i$	The operating parameters of container $c_i$
$r_{i,m}^d$	The $c_i$ demand in terms of resource $r_m$
$r_{j,m}^u$	The $s_j$ resource usage in terms of resource $r_m$

## B. The Cost Models

As already alluded above, the containers' deployment or migration has to be decided while optimizing a cost model as it is the most suitable way to favour one possible migration solution over another. Thus, in the present section the costs that are involved to formulate the objective function of the optimization problem are presented. Table II shows some important notations used to express these costs.

TABLE II. IMPORTANT COST NOTATIONS

Notation	Definition
$Cost_{i,j}^{back}$	The container $c_i$ backhaul cost when transferred to $s_j$
$Cost^{back}$	The overall user backhaul cost
$Cost_j^{proc}$	The processing load cost related to server $s_j$
$Cost^{proc}$	The overall processing load cost
$Cost^{netw}$	The overall network load cost
$Cost(\alpha, \beta)$	The cost or objective function
$\phi_0, \phi_{i,j}$	The pheromone initial and current values
$\Delta_\phi^l, \Delta_\phi^g$	The local and global pheromone evaporation rates
$\epsilon_1, \epsilon_2$	The pheromone and heuristic information parameters
$temp_0$	The initial temperature value

1) *User backhaul cost*: After placing container  $c_i$  at node  $j$ , the backhaul delay of its user depends on the characteristics of the path connecting node  $j$  and its communication access node  $s_i^t$ . In fact, the ideal situation is achieved if  $j = s_i^t$ . Accordingly, to favour such migration, this cost is introduced in order to bring the containers as close as possible to their end users. Generally, the smaller is this cost the more efficient the placement is. To assess this cost, the available bandwidth between nodes  $j$  and  $s_i^t$  as well as the hop count between them are used. Accordingly, the following weighted sum is adopted:

$$Cost_{i,j}^{back} = \begin{cases} 0 & ; s_i^t = j \\ \min_{k \in \mathcal{P}_{s_i^t,j}} \left\{ \Delta_r \frac{\min_{k' \in \mathcal{P}_{s_i^t,j}} \mathcal{B}_{s_i^t,j}^{k'}}{\mathcal{B}_{s_i^t,j}^k} + \Delta_h \frac{\mathcal{H}_{s_i^t,j}^k}{\max_{k' \in \mathcal{P}_{s_i^t,j}} \mathcal{H}_{s_i^t,j}^{k'}} \right\} & ; s_i^t \neq j \end{cases} \quad (9)$$

Here  $i \in \mathcal{C}; j \in \mathcal{S}$  and  $Cost_{i,j}^{back}$  is ranging in  $[0,1]$ ,  $\Delta_r$  and  $\Delta_h$  are the weights associated respectively with the available data rate (bandwidth) and the hop count costs such that  $\Delta_r + \Delta_h = 1$ . Also, the fractions' max and min expressions are used for normalization purpose. Therefore, with the decision vector  $\alpha$ , the overall user backhaul cost can be obtained as:

$$Cost^{back}(\alpha) = \sum_{i \in \mathcal{C}} \sum_{j \in \mathcal{S}} \alpha_{i,j} Cost_{i,j}^{back} \quad (10)$$

2) *Load balancing cost*: To ensure the service quality while taking into account the service delay, the model favours containers' migration from over-loaded ENs to release resources for future nearby users requests. Also, to avoid the unbalanced network load, e.g. some links are highly loaded while some others are less loaded, the links traffic load metric is introduced. The main intuition behind balancing this load is to select paths that best balance the traffic loads across different links and keep critical links available for future traffic. Accordingly, the load balancing cost involves the processing or computation load cost of the running containers on all ENs and the traffic load of all available links. The processing load

ratios  $\theta_{j,m}$  of resource  $r_m$  in ES  $j$  and their mean value  $\bar{\theta}_m$  are defined as follows:

$$\theta_{j,m}(\alpha) = \frac{r_{j,m}^u(\alpha)}{r_{j,m}^c} \in [0, 1] \quad ; j \in \mathcal{S}; m \in \mathcal{R} \quad (11)$$

$$\bar{\theta}_m(\alpha) = \sum_{j \in \mathcal{S}} \frac{\theta_{j,m}}{\sigma_s} \quad ; m \in \mathcal{R} \quad (12)$$

Then, the processing load related to ES  $j$  with regards to all resource types is defined as:

$$Cost_j^{proc}(\alpha) = \sum_{m \in \mathcal{R}} \frac{|\theta_{j,m}(\alpha) - \bar{\theta}_m(\alpha)|}{\sigma_r} \quad ; j \in \mathcal{S} \quad (13)$$

which gives the following overall processing load:

$$Cost^{proc}(\alpha) = \sum_{j \in \mathcal{S}} \sum_{m \in \mathcal{R}} \frac{|\theta_{j,m}(\alpha) - \bar{\theta}_m(\alpha)|}{\sigma_s \sigma_r} \in [0, 1] \quad (14)$$

On the other hand, the network load balancing cost shows the distribution ratio of the links' load or indicates whether containers receive a fair share of data transfer resources. Hence, the lack of capacity  $\vartheta_\ell$  of link  $\ell$  using the allowable bandwidth  $\mathcal{B}_{s_i^c, j}^k$  is given by:

$$\vartheta_\ell(\alpha, \beta) = \max \left\{ 0; \sum_{i \in \mathcal{C}} \sum_{j \in \mathcal{S}} \sum_{k \in \mathcal{P}_{s_i^c, j}} \left( \alpha_{i,j} \beta_{i,j}^k \delta_{i,j}^{k,\ell} \mathcal{B}_{s_i^c, j}^k \right) - b(\ell) \right\}; \ell \in \mathcal{L} \quad (15)$$

Accordingly, this lack of capacity is chosen as the network load unbalance cost related to link  $\ell$  which gives the following overall network traffic load unbalance cost:

$$Cost^{netw}(\alpha, \beta) = \sum_{\ell \in \mathcal{L}} \vartheta_\ell(\alpha, \beta) \quad (16)$$

Moreover, as  $\vartheta_\ell(\alpha, \beta) \leq b(\ell) * (\sigma_c - 1)$ , herein the following normalization sum is presented:

$$L^{cap} = (\sigma_c - 1) \sum_{\ell \in \mathcal{L}} b(\ell) \quad (17)$$

Finally, the following weighted sum is adopted to asses the overall load balancing cost where  $\Delta_p$  and  $\Delta_n$  are the weights associated respectively with both processing and network loads such that  $\Delta_p + \Delta_n = 1$ . Also, the denominators in this expression are used for normalization purpose.

$$Cost^{load}(\alpha, \beta) = \Delta_p Cost^{proc}(\alpha) + \Delta_n \frac{Cost^{netw}(\alpha, \beta)}{L^{cap}} \in [0, 1] \quad (18)$$

#### IV. THE UBL-MDC PROBLEM FORMULATION

##### A. Multi-objective Cost Function

Now, to get the overall cost model, a multi-criteria migration and deployment decisions by considering all the three cost metrics within the proposed edge computing system is designed. The proposed multi-objective function is formulated as a weighted sum of these four costs using the following function:

$$Cost(\alpha, \beta) = \Delta_b \frac{Cost^{back}(\alpha)}{\sigma_c} + \Delta_l Cost^{load}(\alpha, \beta) \quad (19)$$

Here  $\Delta_b$ , and  $\Delta_l$  are regulatory weights constants to balance this cost function. Their values are ranging in  $[0, 1]$  such that  $\Delta_b + \Delta_l = 1$ . By deciding these weights one can adjust the

priority to attribute to each metric. Here, the variables are given by  $\alpha$  (two dimensions binary array  $[\sigma_c \times \sigma_s]$ ) and  $\beta$  (two dimensions array  $[\sigma_c \times \sigma_s]$  of vectors where  $\beta_{i,j}$  is a vector of binaries of length  $|\mathcal{P}_{i,j}|$ ).

##### B. Constraints

In the proposed model model, the case when container  $i$  is not migrated is represented by setting  $\alpha_{i, s_i^c} = 1$  and  $\alpha_{i,j} = 0$  for  $j \in \mathcal{S} \setminus \{s_i^c\}$  and if migrated, only one target server is selected. Accordingly, the migration decision of container  $i$  has to meet the following constraint:

$$\sum_{j \in \mathcal{S}} \alpha_{i,j} = 1 \quad ; i \in \mathcal{C}; \quad (20)$$

By selecting a path  $p = (\mathcal{L}_{s_i^c, s_1}, \mathcal{L}_{s_1, s_2}, \dots, \mathcal{L}_{s_{|p|-1}, j})$  in  $\mathcal{P}_{s_i^c, j}$  to serve the transfer flow of container  $c_i$  from node  $s_i^c$  to  $j$ , many constraints have to be satisfied. With the start node  $s_i^c$  of path  $p$ , its last node  $j$  must be the placement node of container  $i$  which is expressed as:

$$\sum_{k \in \mathcal{P}_{s_i^c, j}} \beta_{i,j}^k = \alpha_{i,j} \quad ; i \in \mathcal{C}; j \in \mathcal{S} \quad (21)$$

Also, the resource capacity in EN  $j$  must satisfy all the containers resource requirements that are decided to be deployed in or migrated to ES  $j$  for all resource types, which is finally formulated as:

$$\sum_{i \in \mathcal{C}} \alpha_{i,j} r_{i,m}^d \leq r_{j,m}^c \quad ; j \in \mathcal{S}; m \in \mathcal{R} \quad (22)$$

Lastly, the serving bandwidth constraint after the placement of container  $c_i$  using the maximal available bandwidth in (7) is formulated as:

$$\mathcal{B}_i \geq B_i^{ser} \quad ; i \in \mathcal{C} \quad (23)$$

##### C. Formulation

In light of the above clarifications of the studied problem, the formulation of the proposed UBL-MDC framework which aims to efficiently deploy and migrate the involved containers while considering their priorities is presented. The joint deployment, migration and route selection are made while deciding the best placements to minimize the objective consisting of the costs related to the resulting users back-haul bandwidth and the load balancing degree. Finally, the following optimization problem  $\mathcal{P}1$  generates the minimal deployment and migration cost with resource allocation and traffic routing while maximum number of priority containers are satisfied.

$$\begin{aligned} \mathcal{P}1 : & \text{minimize } Cost(\alpha, \beta) \\ & \{\alpha, \beta\} \\ \text{s.t. } & (1), (2), (20), (21), (22), (23) \end{aligned}$$

Indeed, this formulation minimizes the aforementioned four metrics influencing the performance of the studied mobile edge-cloud system and the users' satisfaction according to their priorities.

#### D. The UBL-MDC Problem Complexity

Since problem  $\mathcal{P}1$  is a binary integer programming problem, it is considered to be NP-complete. This is highlighted when showing its search space dimension that is  $2^{\sigma_c \sigma_s} \left( \sum_{i \in \mathcal{C}} \sum_{j \in \mathcal{S}} (2^{|\mathcal{P}_{i,j}|}) \right)$ . For example, when  $\sigma_c = 20$ ,  $\sigma_s = 5$  and  $|\mathcal{P}_{i,j}| = 10$ , the search space size is  $2^{100} \times (100 \times 2^{10}) \simeq 1.298 \times 10^{35}$ . As such, the search space's exponential growth with the problem's dimension is obvious and one can observe the excessive computational requirement to solve such a problem. Therefore, the following section shows the development procedure of a low-complexity heuristic scheme.

### V. PROBLEM RESOLUTION

#### A. The BFS-PS Exact Solution

To get the optimal containers' migration and deployment decision given by problem  $\mathcal{P}1$ , an exhaustive search is performed over all possible solutions using a Brute Force Search with Path Selection that is denoted (BFS-PS). It is presented in Algorithm 1. Unfortunately, this search is an  $O(\sigma_c \times \sigma_s \times N)$  time complexity solution where  $N = \prod_{i=1}^{\sigma_c} \left( \sum_{j=1}^{\sigma_s} (|\mathcal{P}_{i,j}|) \right)$  and is feasible for limited settings. Indeed, when  $\sigma_c = 20$ ,  $\sigma_s = 5$  and  $|\mathcal{P}_{i,j}| = 10$ , the iterations' count  $N \simeq 9.536 \times 10^{33}$ , which is already not feasible.

---

**Algorithm 1** : BFS based Containers' Migration and Deployment

---

**Require:**  $\mathcal{C}, \mathcal{S}, \mathcal{P}, \Omega$

**Ensure:** optimal decisions  $\alpha^*, \beta^*$  with cost  $\Gamma^*$

---

```

1:  $\Gamma^* \leftarrow \infty$ 
2:  $N \leftarrow \prod_{i=1}^{\sigma_c} \left( \sum_{j=1}^{\sigma_s} (|\mathcal{P}_{i,j}|) \right)$ ;
3: for  $l = 0$  to  $N - 1$  do
4:   build  $\beta$  from  $l$ ;
5:   for each container  $i$  in  $\mathcal{C}$  do
6:     for each node  $j$  in  $\mathcal{S}$  do
7:       if  $\sum_{k=1}^{|\mathcal{P}_{i,j}|} \beta_{i,j}^k == 0$  then
8:          $\alpha_{i,j} \leftarrow 0$ ;
9:       else
10:         $\alpha_{i,j} \leftarrow 1$ ;
11:      end if
12:    end for
13:  end for
14:  if constraints of  $\mathcal{P}1$  are satisfied then
15:     $X \leftarrow Cost(\alpha, \beta)$  according to (19);
16:    if  $X < Cost^*$  then
17:       $(\alpha^*, \beta^*, \Gamma^*) \leftarrow (\alpha, \beta, X)$ 
18:    end if
19:  end if
20: end for
21: return  $(\alpha^*, \beta^*, \Gamma^*)$ 

```

---

As input, Algorithm 1 requires the parameters' vector  $\Omega$  as well as the information regarding containers, servers and paths. The main for loop of the algorithm iterates N times over the

instructions' bloc that tries to enhance the best solution using variables  $\alpha$  and  $\beta$  that are built using the current iteration value.

#### B. ACS-PS Approximate Algorithm

To get a feasible containers' migration and deployment decisions, hereafter an efficient discrete ACS-based algorithm with Paths Selection (ACS-PS) is designed with two different migration strategies. To compare its performance, two other meta-heuristic algorithms based on simulated annealing (SA) and genetic algorithms (GA) are used. The first is summarized in Algorithm 4 whereas the second is based on the work in [15].

1) *Algorithm description*: ACS schemes adopt pheromone evaporation and sharing strategies to share the learned experience among different ants' groups. They simulate the feeding process of ants to simulate the decision of containers' migration and deployment. The main pieces of this algorithm are summarized as follows:

- Ants are randomly placed in the containers to be transferred.
- every ant  $A_a$  selects a mapping tuple  $\langle c_i; s_j \rangle$  with a probability  $p_{i,j}$ , referring the transfer of container  $c_i$  to node  $s_j$  using path  $p_k$  according to the pheromones  $\phi_{i,j}$  and the heuristic information  $\psi_{i,j}$ . Then,  $c_i$  is placed into tabu list  $Tabu_a$  of  $A_a$ .
- To get its migration plan, ant  $A_a$  returns to the next container in the transfer containers set  $\mathcal{C}$ , and repeats the previous process to complete the next migration allocation.
- That all the ants complete the allocation of all the transfer containers in  $\mathcal{C}$  once, can be regarded as one iteration.
- The algorithm terminates when the maximum iterations' number is reached.

2) *Algorithm skeleton*: In practice, ants use a kind of chemical substance named pheromone to share information with each other [18]. Its initial value is defined as follows:

$$\phi_0 = \frac{1}{\sigma_c} \quad (24)$$

**Pheromone variation rules**: When transferring the containers, the ACS algorithm dumps the ants' search experience using the matrix  $[\phi]$  of size  $\sigma_c \times \sigma_s$ . Each element  $\phi_{i,j}$  saves the pheromone amount that informs ants about the tendency to choose pair  $(c_i; s_j)$ .

The next equations are the rules serving to update the pheromone locally and globally, respectively:

$$\phi_{i,j}^{new} = \phi_{i,j}^{old} \times (1 - \Delta_{\phi}^l) \quad (25)$$

$$\phi_{i,j}^{new} = \phi_{i,j}^{old} + \Delta_{\phi}^g \times \Delta_{i,j}^a \quad (26)$$

here  $\Delta_{\phi}^l$  and  $\Delta_{\phi}^g$  are the local and global pheromone evaporation rates respectively.  $\Delta_{i,j}^a$  is its increment of additional

pheromone defined by:

$$\Delta_{i,j}^a = \begin{cases} \frac{1}{Cost(X_a^+)} & ; \text{ if } \alpha_{i,j} = 1 \text{ in } X_a^+ \\ 0 & ; \text{ otherwise} \end{cases} \quad (27)$$

where  $Cost(X_a^+)$  is the cost value of an iteration's best solution found by ant  $A_a$ . Actually, when the mapping relation tuple  $\langle c_i; s_j \rangle$  is chosen, the ant updates locally the pheromone value of this path using Eq. (25). On the other hand, when the mapping relation tuples of all current solutions is completed, the best one w.r.t.  $Cost$  is chosen to perform pheromone update globally using Eq. (26) in order to maintain the experience of the global best solution.

**Heuristic information:** The proposed model uses heuristic information  $\psi_{i,j}$  that is obtained based on the maximum allowable bandwidth to transfer container  $c_i$  to node  $n_j$  that is expressed as:

$$\psi_{i,j} = \max_{k' \in \mathcal{P}_{s_i^k, j}} \mathcal{B}_{s_i^k, j}^{k'} \quad (28)$$

Usually ants tend to choose the path with more pheromones and higher expectations of the ongoing path. Nevertheless, this deterministic choice has the disadvantage to fall into local optimum. Accordingly, ACS algorithm reacts by using a pseudorandom rule where ants probabilistically select the next mapping transfer tuple  $\langle c_i, s_j, p_k \rangle$  using a probabilistic rule. First, Eq. (29) defines the set  $\omega_a(i)$  of possible target nodes  $j'$  related to ant  $A_a$  and their leading routes  $k'$  that verify all constraints in (31). Each element in this set represents a possible candidate placement node  $j$  with its associated possible leading routes that are given by the set  $\omega_{a,j}(i)$ . The set of candidate placement nodes only in  $\omega_a(i)$  is denoted  $\overline{\omega}_a(i)$ .

$$\omega_a(i) = \{ (j', k') \mid \text{if (31) are satisfied} \} \quad (29)$$

$$\overline{\omega}_a(i) = \{ j \mid (j, k) \in \omega_a(i) \} \quad (30)$$

$$\begin{cases} \sum_{i' \in \mathcal{C}} \alpha_{i',j} r_{i',m}^d + r_{i,m}^d \leq r_{j',m}^c & m \in \mathcal{R} \\ \mathcal{B}_{s_i^k, j'}^{k'} \geq \mathcal{B}_i \end{cases} \quad (31)$$

**The nodes selection:** The next pair container-node is chosen based on the following equation:

$$j = \begin{cases} \operatorname{argmax}_{j' \in \overline{\omega}_a(i)} \{ (\phi_{i,j})^{\varepsilon_1} \times (\psi_{i,j})^{\varepsilon_2} \} & \text{if } q \leq q_0 \\ \text{Roulette Wheel} \{ \overline{\omega}_a(i); \chi_{i,j} \} & \text{otherwise} \end{cases} \quad (32)$$

where  $q$  is a uniformly distributed random number ranging in  $[0, 1]$  and  $q_0 \in [0, 1]$  is a threshold parameter.  $\varepsilon_1$  and  $\varepsilon_2$  are pheromone and heuristic information parameters, respectively. When  $q \leq q_0$ ,  $A_a$  choose pair  $(i, j)$  with the maximum value to transfer  $c_i$  to node  $j$ . Otherwise, the pair  $(i, j)$  is chosen with the Roulette Wheel procedure (see Alg.(2)) within the set  $\overline{\omega}_a(i)$  using probabilities  $\chi_{i,j}$  defined in Eq. (33).

$$\chi_{i,j} = \frac{(\phi_{i,j})^{\varepsilon_1} \times (\psi_{i,j})^{\varepsilon_2}}{\sum_{j' \in \overline{\omega}_a(i)} (\phi_{i,j'})^{\varepsilon_1} \times (\psi_{i,j'})^{\varepsilon_2}} \quad (33)$$

**The node-path pair selection:** if container  $c_i$  is selected for transfer, the model proposes to select the pair  $s_j - p_k$

**Algorithm 2 :** Roulette Wheel Rule Algorithm for Container  $c_i$  using  $\overline{\omega}_a(i)$ .

**Require:**  $\mathcal{S}, \mathcal{P}, \overline{\omega}_a(i), \Omega_i, \varepsilon_1$  and  $\varepsilon_2$

**Ensure:** the candidate node  $j_0$ ;

```

1: for each node  $j$  in  $\mathcal{S}$  do
2:   if  $j$  in  $\overline{\omega}_a(i)$  then
3:     calculate  $\chi_{i,j}$  using Eq. (33)
4:   else
5:      $\chi_{i,j} \leftarrow 0$ ;
6:   end if
7: end for
8:  $q1 \leftarrow \text{random}(0, 1) * \chi^{total}$ ;
9:  $p \leftarrow 0$ ;
10: for each node  $j$  in  $\overline{\omega}_a(i)$  do
11:    $p \leftarrow p + \chi_{i,j}$ ;
12:   if  $q1 \geq p$  then
13:      $j_0 \leftarrow j$ ;
14:     break;
15:   end if
16: end for
17: return  $j_0$ 

```

denoted  $(j, k)$  as the target node and the path of its transfer. The adopted path selection strategy uses two versions: the first strategy denoted (ACS-PS-1) select the path with the maximum allowable bandwidth, while the second one denoted (ACS-PS-2) adopts a random selection strategy. With the first strategy ACS-PS-1, the following equation that gives the maximum transfer bandwidth while choosing path  $p_k$  is adopted:

$$k \leftarrow \operatorname{argmax}_{k' \in \omega_{a,j}(i)} \{ \mathcal{B}_{s_i^k, j}^{k'} \} \quad (34)$$

3) *Algorithm pseudo-code:* The pseudo-code of the proposed algorithm is summarized in Algorithm 3 where a solution  $X_a$  is given by the variables' arrays  $(\alpha, \beta)$  and  $X$  is the solutions' set of all ants.

As input, Algorithm 3 requires the sets  $\mathcal{C}, \mathcal{S}$  and  $\mathcal{P}$ ; the parameters' vector  $\Omega$ , the maximum iterations count parameter  $n^{max}$ , the ants' count  $\sigma_a$ , the pheromone initial value  $q_0$ , the local and global pheromone evaporation rates  $\Delta_{\phi}^l$  and  $\Delta_{\phi}^g$ ;  $\varepsilon_1, \varepsilon_2$  the pheromone and heuristic information parameters and the path selection strategy  $s$ . In lines 1 to 3, the initial solution's vectors are built and the optimal cost  $F^*$  associated with the optimal solution  $(\alpha^*, \beta^*)$  is initialized. In line 4, the general for loop repeat the process using  $n^{max}$  iterations where in each iteration all ants are involved using the loop in line 6. At each ant step, probability matrix is updated (lines 7-11), the containers' placement decisions with paths' selection are performed using Eq. (32) and strategy  $s$  which results in the vectors  $\alpha$  and  $\beta$  (lines 12-35); and the local update of pheromone is executed. Then the iteration solutions corresponding to all ants are examined with a global pheromone update (lines 38-40) using the best solution and Eq.(26).

### C. The SA-PS Approximate Algorithm

In this section, the proposed Simulated Annealing based heuristic solution with Paths Selection (SA-PS) is described. This heuristic optimization technique is characterized by its simplicity and general applicability features. In terms of speed,

**Algorithm 3** : ACS-Based Container Transfer Algorithm with Path Selection (ACS-PS)

**Require:**  $\mathcal{C}, \mathcal{S}, \mathcal{P}, \Omega, n^{max}, \sigma_a, q_0, \Delta_\phi^l, \Delta_\phi^g, \varepsilon_1, \varepsilon_1$  and strategy  $s$

**Ensure:** the Global solution  $(\alpha^*, \beta^*)$ ;

```

1: Generate an initial solution  $(\alpha, \beta)$ 
2: Calculate  $F = Cost(\alpha, \beta)$  according to (19);
3:  $(\alpha^*, \beta^*, F^*) \leftarrow (\alpha, \beta, F)$ 
4: for  $n = 1$  to  $n^{max}$  do
5:    $X \leftarrow \{\}$ 
6:   for  $a = 1$  to  $\sigma_a$  do
7:     for each container  $i$  in  $\mathcal{C}$  do
8:       for each node  $j$  in  $\mathcal{S}$  do
9:         calculate  $\chi_{i,j}$  using Eq. (33)
10:      end for
11:     end for
12:     for each container  $i$  in  $\mathcal{C}$  do
13:       choose pair  $\langle s_{j_0}; p_{k_0} \rangle$  from  $\omega_a(i)$  using
14:       Eq. (32) and strategy  $s$ ;
15:       for each node  $j$  in  $\mathcal{S}$  do
16:         if  $j = j_0$  then
17:            $\alpha_i^j \leftarrow 1$ ;
18:           for each path  $k$  in  $\mathcal{P}_{s_i^c, j_0}$  do
19:             if  $k = k_0$  then
20:                $\beta_{i, j_0}^k \leftarrow 1$ ;
21:             else
22:                $\beta_{i, j_0}^k \leftarrow 0$ ;
23:             end if
24:           end for
25:         else
26:            $\alpha_i^j \leftarrow 0$ ;
27:           for each path  $k$  in  $\mathcal{P}_{s_i^c, j}$  do
28:              $\beta_{i, j}^k \leftarrow 0$ ;
29:           end for
30:         end if
31:       end for
32:       update the local pheromone according to
33:       Eq. (25);
34:       put  $c_i$  into  $Tabu_a$ ;
35:     end for
36:     put solution  $X_a = (\alpha, \beta)$  into  $X$ ;
37:   end for
38:    $X^+ \leftarrow \underset{X_a \in X}{\operatorname{argmin}} \{Cost(X_a)\}$ ;
39:    $F \leftarrow Cost(X^+)$ 
40:   update the global pheromone according to Eq. (26);
41:   if  $F < F^*$  then
42:      $(\alpha^*, \beta^*, F^*) \leftarrow (\alpha, \beta, F)$ 
43:   end if
44: end for

```

it is considered among the main efficient heuristics compared to other techniques. Probabilistically, this algorithm accepts not only cost gain, but also cost degradation in order to leave the local minima. Inspired by the Very Fast Simulated Annealing [19] variant, this algorithm use the cost function  $Cost$  as the thermodynamic system's energy. During the solutions' space probabilistic iteration, the acceptance of the current state is done such that new states with less energy compared to the

previous energy are accepted; otherwise, the new state is accepted when the probability  $\exp\left(\frac{|F-F_{new}|}{temp}\right)$  is greater than a random generated float using a uniform distribution  $U[0, 1]$ . Also, with decreasing temperature process, the chance for the system to accept such penalizing transitions decreases. The temperature schedule in this algorithms is given by:

$$temp_k = temp_0 e^{\left(-0.5k \frac{1}{2\sigma_c}\right)} \quad (35)$$

where  $k$  is the current iteration number and  $temp_0$  is the initial temperature parameter. The detail of the solution is presented in Algorithm (4).

**Algorithm 4** : SA-Based Container Transfer Algorithm with Path Selection (SA-PS)

**Require:**  $\mathcal{C}, \mathcal{S}, \mathcal{P}, \Omega, k^{max}$  and  $temp_0$ .

**Ensure:** the Global solution  $(\alpha^*, \beta^*)$ ;

```

1: Generate an initial solution  $(\alpha, \beta)$ 
2: Calculate  $F = Cost(\alpha, \beta)$  according to (19);
3:  $(\alpha^*, \beta^*, F^*) \leftarrow (\alpha, \beta, F)$ 
4: for  $n=1$  to  $k^{max}$  do
5:    $temp \leftarrow temp_0 e^{-0.5n \frac{1}{2\sigma_c}}$ ;
6:    $\alpha_{new} \leftarrow \operatorname{rand\_neighbour}(\alpha)$ ;
7:   Build best  $\beta_{new}$  using  $\alpha_{new}$ 
8:   Calculate  $F_{new} = Cost(\alpha_{new}, \beta_{new})$  using (19);
9:    $\Delta_F \leftarrow F_{new} - F$ 
10:  if  $\Delta_F < 0$  or  $e^{\frac{-|\Delta_F|}{temp}} \geq \operatorname{random}(0,1)$  then
11:     $(\alpha, \beta, F) \leftarrow (\alpha_{new}, \beta_{new}, F_{new})$ 
12:    if  $F < F^*$  then
13:       $(\alpha^*, \beta^*, F^*) \leftarrow (\alpha, \beta, F)$ 
14:    end if
15:  end if
16: end for
17: return  $(\alpha^*, \beta^*)$ 

```

As input, Algorithm 4 requires the sets  $\mathcal{C}, \mathcal{S}$  and  $\mathcal{P}$ ; the parameters' vector  $\Omega$ , the maximum iterations count parameter  $k^{max}$ , the initial temperature value  $temp_0$ . In lines 1 to 3, the initial solution's vectors are built and the optimal cost  $F^*$  associated with the optimal solution  $(\alpha^*, \beta^*)$  is initialized. Then a for loop (line 4) is used in order to repeat the annealing process using  $k^{max}$  iterations. At each step, the temperature value  $temp$  is updated (line 5); then, a neighboring state  $\alpha_{new}$  of the current state  $\alpha$  in line 6 is generated and its corresponding paths selection vector is built in line 7. Then, the new cost  $F_{new}$  is evaluated in line 8. Then, the new state is accepted if generating more profit; otherwise it is accepted using a probabilistic test (lines 10 to 15). Here,  $\operatorname{random}(0, 1)$  is a function's call that uniformly generates a random number in  $[0, 1]$ .

## VI. EVALUATION AND RESULTS

In this section, the proposed experiments used in order to compare the proposed solutions are presented based on the execution time and the cost function metrics.

### A. Simulation Setup

All developed simulation programs were ran using a 2.4GHz Intel Core i5 processor in a PC with a maximum 8GB

of RAM. Moreover, the basic parameters of the simulation experiments are listed in Table III.

TABLE III. SIMULATIONS' PARAMETERS

Parameter	values
$\sigma_s; \sigma_r$	5; 3
$ \mathcal{P}_{i,j} $	$\llbracket 3; 5 \rrbracket$
$n^{max}; k^{max}$	100; 200
$q_0$	0.3
$\Delta_\phi^l; \Delta_\phi^g$	0.1; 0.7
$\Delta_r; \Delta_h$	0.5; 0.5
$\Delta_p; \Delta_n$	0.5; 0.5
$\Delta_i; \Delta_b$	0.5; 0.5
$\varepsilon_1$	1
$\varepsilon_2$	2
$temp_0$	200

### B. Exact vs. Heuristic Performance

To investigate the feasibility and limitation of Algorithm 1, the first experiment is carried where the achieved costs are measured and the execution time of all five solutions is recorded. In fact, the performance of the optimal BFS based solution is studied compared to the proposed heuristic solutions where the ACS-PS algorithm is studied relatively to both proposed strategies denoted ACS-PS-1 and ACS-PS-2. Accordingly, the containers' count ( $\sigma_c$ ) is varied between 2 and a maximum feasible experimentation value  $\sigma_c = 9$  while the nodes' count  $\sigma_s = 5$ , and  $|\mathcal{P}_{i,j}| \in \llbracket 3; 5 \rrbracket$ . The obtained results are depicted in Fig. 3.

The obtained normalized cost for the proposed solutions is

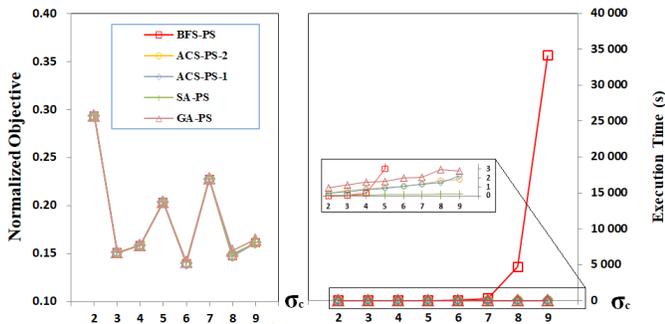


Fig. 3. Normalized Cost and Execution Time with  $\sigma_c; \sigma_s = 5$ .

shown in the left part of this figure. The variations of the same curve in this figure is only the result of using different data from one point to another and does not carry any information. Thus, the figure shows similar results for all solutions when  $\sigma_c \in [2, 7]$ ; elsewhere the results of the GA-PS solution only deviate little from the optimal BFS-PS solution. The right side of this figure shows the variation of the execution time of the studied solutions. For clarity reason in this part of the figure, the results are zoomed to show the achievements of the heuristic solutions. Accordingly, the exponential growth of the BFS-PS solution execution times is demonstrated. Indeed, it achieves better performance for  $\sigma_c \in [2, 4]$  compared to all other solution; elsewhere, it enormously goes beyond feasible times. For instance, it reaches 34123.15s with  $\sigma_c = 9$ . The SA-PS solution achieves the minimum execution times by little exceeding the achievements of the ACS-PS and GA-PS

solutions. In fact, with  $\sigma_c = 9$  it reaches only 0.192s; whereas ACS-PS-1, ACS-PS-2 and GA-PS solutions respectively attain 2.242, 1.883 and 2.784 seconds. This experiment shows a slightly stable execution time for the heuristic solutions and the infeasibility of the BFS-PS solution beyond the value  $\sigma_c = 5$ .

### C. Heuristic Solutions Comparison

The second experiment studies the heuristic solutions' performance only. In this experiment, the containers' number ( $\sigma_c$ ) is taken such that  $\sigma_c \in \{10, 20, 30, 40, 50, 60, 70, 80, 90, 100\}$ . With regard to the total number of containers, Fig. 4 shows the achieved Normalized Cost obtained as the value of the objective function defined in Eq. (19). The results demonstrate the superiority in performance of the ACS-PS solution for both strategies. In particular, the ACS-PS-2 solution gives the best results compared to all other solutions for all values of  $\sigma_c$ . Also, the results of the solutions based on GA-PS and SA-PS are slightly bigger in that order compared to those of ACS-PS.

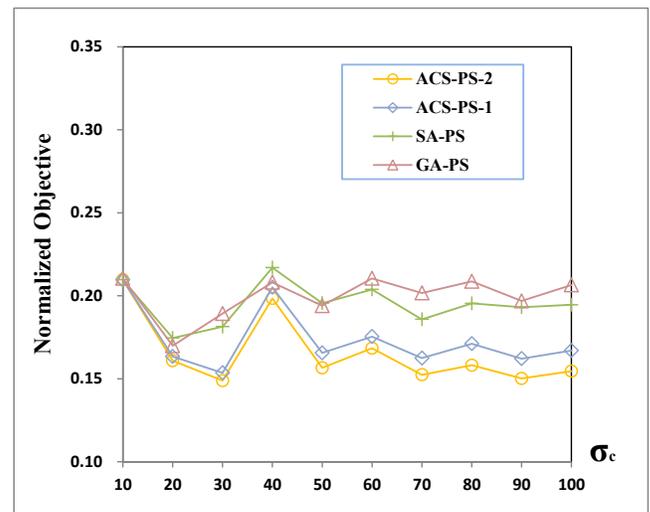


Fig. 4. Normalized Cost with  $\sigma_c; \sigma_s = 5$ .

### D. The Total Backhaul Cost

Now, the next evaluation is introduced where the performance related to the total backhaul cost achievements for all heuristic solutions is studied. The reported values are obtained using Eq. (10). First, the experience is performed such that  $\sigma_c \in \{10, 20, 30, 40, 50, 60, 70, 80, 90, 100\}$  with  $\sigma_s = 5$  and record the overall backhaul costs using ACS-PS, SA-PS and GA-PS heuristic methods. In each value of  $\sigma_c$  the overall achieved backhaul cost is shown without normalization using different settings. Thus, the variation shape of the same curve does not provide any information. Hence, Fig. 5 depicts the obtained results of this first experiment. Once again, the ACS-PS-2 solution gives the best results compared to all other solutions for all values of  $\sigma_c$ . Mainly, the performance results of the solutions based on ACS-PS widely exceed the performance of GA-PS and SA-PS although there is no clear and fixed preference between GA-PS and SA-PS in terms of results. Indeed, ACS-PS-1, ACS-PS-2, SA-PS and GA-PS attain respectively 0.221, 0.101, 1.244 and 1.203 for  $\sigma_c = 100$ ,

whereas they attain 0.302, 0.169, 1.071 and 1.169 for  $\sigma_c = 90$ . Now, the following second part of the experiment studies the

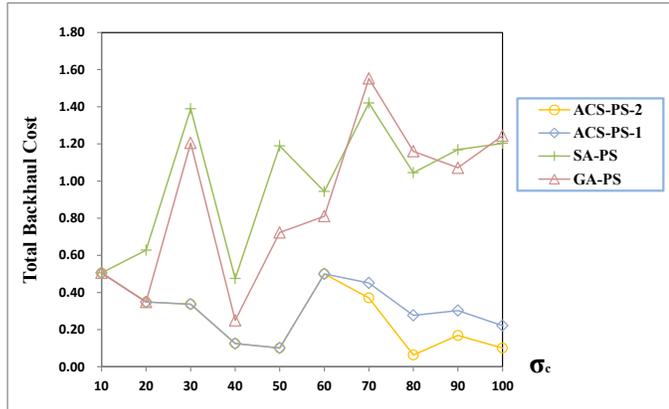


Fig. 5. Total Backhaul Costs with  $\sigma_c$ ;  $\sigma_s = 5$ .

impact of the regulatory factor  $\Delta_b$  on the result in terms of the total backhaul cost.  $\Delta_b$  is taken in the interval  $[0.05, 0.5]$  with the setting  $\sigma_c = 30$ ;  $\sigma_s = 5$ ;  $\Delta_l = 1.0 - \Delta_b$ . The obtained results are reported in Figure 6.

The balance effect is well observed from this figure. Indeed,

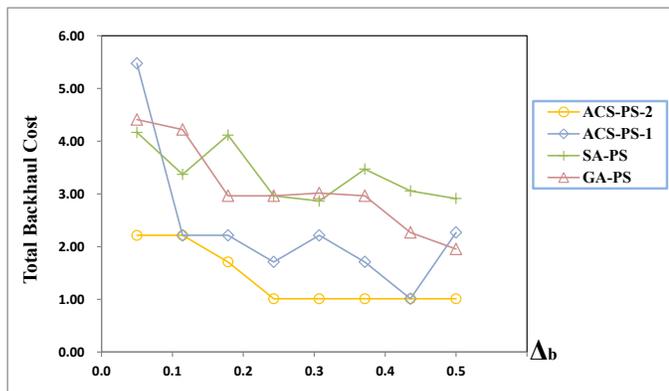


Fig. 6. Total Backhaul with  $\Delta_b$ ;  $\sigma_c = 30$ ;  $\sigma_s = 5$ ;  $\Delta_l = 1.0 - \Delta_b$ .

when the value of  $\Delta_b$  increases, the total backhaul cost generally decreases except for a few values where small tolerable increases are observed. these increases can be explained by the probabilistic aspect of these heuristic solutions which remain acceptable. The same figure further demonstrates superior performance of the ACS-PS-2 solution. Indeed, for this solution only, the variation of the total backhaul cost remains decreasing for all values of the experience. Consequently, this experiments shows that the factor  $\Delta_b$ , used as regulator coefficient to balance the importance of the backhaul bandwidth cost among the other metrics, really fulfills its role.

## VII. CONCLUSIONS AND PERSPECTIVES

In this paper, a containers' deployment and migration problem with resource consideration within a multi-server mobile edge-cloud system is studied. The model considers a set of containers to deploy and migrate to a set of edge-cloud nodes where the transfer is compellable to users' backhaul

bandwidth constraints. The formulated optimization problem minimizes a derived multi-objective function that jointly minimizes end-users perceived bandwidths and the system's load balance degree. Accordingly, the optimal transfer decisions are established by solving the obtained optimization problem. To handle its high complexity, two moderate complexity algorithms based respectively on Ant Colony System and Simulated Annealing are proposed. Then, a set of simulation experiments are performed to study their performance. The results reveal that the proposed BFS-based exact method is inefficient with big settings and it is highly time consuming. Furthermore, the ACS-PS is considerably efficient and gives good result with more acceptable execution time, whereas the SA-based solution is very efficient in terms of execution time. Moreover, the balance effect of the  $\Delta_b$  factor serving to balance the importance degree of the backhaul cost is well established. Finally, we plan as perspectives to involve the transfer delays regarding the migrations types in the studied edge-cloud system.

## REFERENCES

- [1] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, 2019.
- [2] G. Premsankar, M. Di Francesco, and T. Taleb, "Edge computing for the internet of things: A case study," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1275–1284, 2018.
- [3] M. El Ghmary, M. O. Cherkaoui Malki, Y. Hmimz, and T. Chanyour, "Energy and computational resources optimization in a mobile edge computing node," in *2018 9th International Symposium on Signal, Image, Video and Communications (ISIVC)*, pp. 323–328, IEEE, 2018.
- [4] Y. Zhao, W. Wang, Y. Li, C. C. Meixner, M. Tornatore, and J. Zhang, "Edge computing and networking: A survey on infrastructures and applications," *IEEE Access*, vol. 7, pp. 101213–101230, 2019.
- [5] H. Abdah, J. P. Barraca, and R. L. Aguiar, "Qos-aware service continuity in the virtualized edge," *IEEE Access*, vol. 7, pp. 51570–51588, 2019.
- [6] S. Wang, J. Xu, N. Zhang, and Y. Liu, "A survey on service migration in mobile edge computing," *IEEE Access*, vol. 6, pp. 23511–23528, 2018.
- [7] F. A. Salaht, F. Desprez, and A. Lebre, "An overview of service placement problem in fog and edge computing," *ACM Computing Surveys (CSUR)*, vol. 53, no. 3, pp. 1–35, 2020.
- [8] Q. Yuan, J. Li, H. Zhou, T. Lin, G. Luo, and X. Shen, "A joint service migration and mobility optimization approach for vehicular edge computing," *IEEE Transactions on Vehicular Technology*, 2020.
- [9] J. Li, X. Shen, L. Chen, D. P. Van, J. Ou, L. Wosinska, and J. Chen, "Service migration in fog computing enabled cellular networks to support real-time vehicular communications," *IEEE Access*, vol. 7, pp. 13704–13714, 2019.
- [10] T. Ouyang, Z. Zhou, and X. Chen, "Follow me at the edge: Mobility-aware dynamic service placement for mobile edge computing," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2333–2345, 2018.
- [11] R. A. Addad, D. L. C. Dutra, M. Bagaa, T. Taleb, and H. Flinck, "Fast service migration in 5g trends and scenarios," *IEEE Network*, vol. 34, no. 2, pp. 92–98, 2020.
- [12] W. Wang, S. Ge, and X. Zhou, "Location-privacy-aware service migration in mobile edge computing," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, 2020.
- [13] S. Wang, R. Uргаonkar, M. Zafer, T. He, K. Chan, and K. K. Leung, "Dynamic service migration in mobile edge computing based on markov decision process," *IEEE/ACM Transactions on Networking*, vol. 27, no. 3, pp. 1272–1288, 2019.
- [14] F. Tang, C. Liu, K. Li, Z. Tang, and K. Li, "Task migration optimization for guaranteeing delay deadline with mobility consideration in mobile edge computing," *Journal of Systems Architecture*, p. 101849, 2020.

- [15] Z. Ma, S. Shao, S. Guo, Z. Wang, F. Qi, and A. Xiong, "Container migration mechanism for load balancing in edge network under power internet of things," *IEEE Access*, vol. 8, pp. 118405–118416, 2020.
- [16] L. Ma, S. Yi, N. Carter, and Q. Li, "Efficient live migration of edge services leveraging container layered storage," *IEEE Transactions on Mobile Computing*, vol. 18, no. 9, pp. 2020–2033, 2018.
- [17] C. Ling, W. Zhang, H. He, and Y.-c. Tian, "Network perception task migration in cloud-edge fusion computing," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–16, 2020. <https://doi.org/10.1186/s13677-020-00193-8>.
- [18] M. Dorigo, G. D. Caro, and L. M. Gambardella, "Ant algorithms for discrete optimization," *Artificial life*, vol. 5, no. 2, pp. 137–172, 1999.
- [19] D. Pei, J. A. Quirein, B. E. Cornish, D. Quinn, and N. R. Warpinski, "Velocity calibration for microseismic monitoring: A very fast simulated annealing (vfsa) approach for joint-objective optimization," *Geophysics*, vol. 74, no. 6, pp. WCB47–WCB55, 2009.

# Zero-resource Multi-dialectal Arabic Natural Language Understanding

Muhammad Khalifa<sup>1</sup>, Hesham Hassan<sup>2</sup>, Aly Fahmy<sup>3</sup>  
Cairo University, Egypt

**Abstract**—A reasonable amount of annotated data is required for fine-tuning pre-trained language models (PLM) on downstream tasks. However, obtaining labeled examples for different language varieties can be costly. In this paper, we investigate the zero-shot performance on Dialectal Arabic (DA) when fine-tuning a PLM on modern standard Arabic (MSA) data only — identifying a significant performance drop when evaluating such models on DA. To remedy such performance drop, we propose self-training with unlabeled DA data and apply it in the context of named entity recognition (NER), part-of-speech (POS) tagging, and sarcasm detection (SRD) on several DA varieties. Our results demonstrate the effectiveness of self-training with unlabeled DA data: improving zero-shot MSA-to-DA transfer by as large as  $\sim 10\%$   $F_1$  (NER), 2% accuracy (POS tagging), and 4.5%  $F_1$  (SRD). We conduct an ablation experiment and show that the performance boost observed directly results from the unlabeled DA examples used for self-training. Our work opens up opportunities for leveraging the relatively abundant labeled MSA datasets to develop DA models for zero and low-resource dialects. We also report new state-of-the-art performance on all three tasks and open-source our fine-tuned models for the research community.

**Keywords**—Natural language processing; natural language understanding; low-resource learning; semi-supervised learning; named entity recognition; part-of-speech tagging; sarcasm detection; pre-trained language models

## I. INTRODUCTION

Neural language models [1], [2] with contextual word representations [3] have become dominant for a wide range of Natural Language Processing (NLP) downstream tasks. More precisely, contextual representations from transformer-based [4] language models [5], [6], pre-trained on large amounts of raw data and then fine-tuned on labeled task-specific data, has produced state-of-the-art performance on many tasks, even when using fewer labeled examples. Such tasks include question answering [7], text classification [6], named entity recognition (NER), and part-of-speech (POS) tagging [8], [9].

Typically, such language models see a huge amount of data during pre-training, which could mistakenly lead us to assume they have a strong generalization capability even in situations where the language varieties seen at test time are different from those the language model was fine-tuned on. To investigate this particular situation, we first study the impact of using a language model pre-trained on huge Arabic corpora for two popular sequence tagging tasks (NER and POS tagging) and one text classification task (sarcasm detection) when fine-tuned on available labeled data, regardless of language variety (Section VII-A). To test the model utility for tasks based on exclusively dialectal Arabic (DA), we then remove all

dialectal data from the training splits and fine-tune a model only on MSA. Evaluating such a model in a *zero-shot* setting, i.e., on Egyptian (EGY), Gulf (GLF), and Levantine (LEV) varieties, we observe a significant performance drop. This shows the somewhat brittle ability of pre-trained language models without dialect-specific fine-tuning.

Unfortunately, the scarcity of labeled DA resources covering sufficient tasks and dialectal varieties has significantly slowed down research on DA [10]. Consequently, a question arises: “How can we develop models nuanced to downstream tasks in dialectal contexts without annotated DA examples?”. We apply self-training, a classical semi-supervised approach where we augment the training data with confidently-predicted dialectal data. We empirically show that self-training is indeed an effective strategy, which proves to be useful in *zero-shot* (where no gold dialectal data are included in training set) independently as well as with self-training (Sections VII-B and VII-C, respectively).

Our experiments reveal that self-training is always a useful strategy that *consistently* improves over mere fine-tuning. In order to understand why this is the case (i.e., why combining self-training with fine-tuning yields better results than mere fine-tuning), we perform an extensive error analysis based on our NER data. We discover that self-training helps the model most with improving false positives (approximately 59.7%). This includes in cases involving DA tokens whose MSA orthographic counterparts [11] are either named entities or trigger words that frequently co-occur with named entities in MSA. Interestingly, such out-of-MSA tokens occur in highly dialectal contexts (e.g., interjections and idiomatic expressions employed in interpersonal social media communication) or ones where the social media context in which the language (DA) employed affords more freedom of speech and a platform for political satire. We present our error analysis in Section VIII.

We choose Arabic as our experimental playground since it affords a rich context of linguistic variation: In addition to the standard variety, MSA, Arabic also has several dialects, thus offering an excellent context for studying our problem. From a geopolitical perspective, Arabic also has a strategic significance. This is a function of Arabic being the native tongue of 400 million speakers in 22 countries, spanning across two continents (Africa and Asia). In addition, the three dialects of our choice (EGY, GLF, LEV) are popular dialects that are widely used online. This makes our resulting models highly useful in practical situations at scale. Pragmatically, ability to develop NLP systems on dialectal tasks with no-to-small labeled dialect data immediately eases a serious bottleneck. Arabic dialects differ among themselves and from

MSA at all linguistic levels, posing challenges to traditional NLP approaches. Having to develop annotated resources across the various dialects for the different tasks would be quite costly, and perhaps unnecessary. Therefore, zero-shot cross-dialectal transfer would be valuable when only some language varieties have the labeled resources. We also note that our method is language-independent, and we hypothesize it can be directly applied to other varieties of Arabic or in other linguistic contexts for other languages and varieties.

Our research contributions in this paper are 3-fold:

- 1) We study the problem of MSA-to-DA transfer in the context of sequence labeling and text classification and show, through experiments, that when training with MSA data only, a wide performance gap exists between testing on MSA and DA. That is, models fine-tuned on MSA generalize poorly to DA in zero-shot settings.
- 2) We propose self-training to improve zero- and few-shot MSA-to-DA transfer. Our approach requires little-to-no labeled DA data. We evaluate extensively on three different dialects across the three aforementioned tasks, and show that our method indeed narrows the performance gap between MSA and DA by a margin as wide as  $\sim 10\%$   $F_1$  points. Moreover, we conduct an ablation experiment to evaluate the importance of using unlabeled DA rather than MSA data in the zero-shot setting, and we show that unlabeled DA data is indeed much more effective and necessary for adapting the model to DA data during testing.
- 3) We develop state-of-the-art models for the three tasks of (NER, POS tagging, and SRD), which we intend to publicly release for the research community.

We now review relevant literature.

## II. RELATED WORK

Classical machine learning techniques, including SVM and Conditional Random Fields (CRFs) [12] applied manually-extracted, hand-crafted word- and character-level features, were previously employed for various sequence labeling tasks including NER, POS tagging, chunking. More recently, however, neural architectures, have become the *de facto* approach for various tasks including sequence labeling. This usually includes an autoregressive architecture such as vanilla Recurrent Neural Networks (RNN) [13] or the more sophisticated Long Short-Term Memory networks (LSTM) [14]. The networks process the input text in a word-by-word fashion, and the network is trained to predict the correct label for each word. In addition, more capacity can be given to such networks by adding an additional layer that processes the input in a right-to-left fashion [15], [16].

Neural approaches usually make use of both word- and character- features. Word-level features usually consist in semantic word embeddings, which are trained on a large raw corpus in a self-supervised fashion [17], [18]. Character-level features can be extracted through an additional network such as LSTM [19] or CNN [20]. Neural techniques has produced better or comparable results to classical approaches in addition to alleviating the need to manually hand-craft features.

In the context of Arabic NLP, the above neural techniques have also been applied to sequence tagging tasks including NER [21], [22], [23], [24], POS tagging [25], [26], and segmentation [27], outperforming classical rule-based approaches [28], [29], which certainly shows the promise of these techniques when applied to morphologically-rich languages such as Arabic.

With respect to **NER** but mostly in the context of MSA, due to lack of dialectal NER datasets. For example, [30] applied a CRF layer over n-gram features to perform NER. [31] combined a decision tree [32] with rule-based features. Other, but little, work has focused on NER in the context of social media data, where DA and MSA are usually mixed together. For instance, [29] used cross-lingual resources, namely English to improve Arabic NER. However, they obtained poor results when evaluating on social media data. More recently, [21] applied bi-directional LSTM networks on both character- and word-levels to perform NER on the Tweets dataset [29]. As for Egyptian dialect, specifically, [33] performed NER by applying a CRF tagger on a set of lexical, morphological, and gazetteer-based features. Their approach showed improvements over baselines but the performance on dialectal data was not on par with it on MSA data, showing the challenges brought by dialectal contexts. To the best of our knowledge, little attention has been given to NER on dialectal Arabic and no prior work has studied the performance when training on MSA data and evaluating on DA data, respectively.

As for **POS tagging** and similarly to NER, the performance of models trained on MSA drops significantly when used with DA [34], [25]. Initial systems for Arabic POS tagging relied on both statistical features and linguistic rules crafted by experts [35], [36] or combined machine learning techniques with rules [37]. More recent work adopted classical machine learning model such as SVM applied on n-gram features [38], [39]. Other work used n-gram features. RNNs and their variants were later adapted for the task [40], [25], [41].

Dialectal Arabic POS tagging has received some attention although usually limited to work individual dialects such as Gulf [42], [25] and Egyptian [43], [44]. [45] studied multi-dialectal POS tagging by proposing an annotated DA dataset from twitter spanning 4 different dialects, namely, Gulf, Egyptian, Levantine, and Maghrebi. While their results show a performance drop on DA when training on MSA only, no attempt was done to improve the DA performance in that case. We can see that despite both the difficulty and scarcity of annotated DA data for all of the different dialects and tasks, most previous work has focused on annotating uni-dialectal datasets attempting to leverage the already abundant MSA datasets. A classical work [43], who employed an MSA morphological analyzer with a minimal supervision to perform POS tagging on Egyptian data with unlabeled Egyptian and Levantine data.

**Sarcasm Detection (SRD)** is the task of identifying sarcastic utterances where the author intends a different meaning than what is being literally enunciated [46]. Sarcasm detection is crucial for NLU as neglecting sarcasm can easily lead to the misinterpretation of the intended meaning, and therefore significantly degrade the accuracy of tasks such as sentiment classification, emotion recognition, and opinion mining. Much research effort has addressed Sarcasm detection in English,

where abundant resources exist [47], [48], [49], [50]. Earlier methods employed linguistic rules [51] or classical machine learning models [49], [52]. More recent methods used neural networks [53], [54], [55], [56], [57], [58] or pre-trained language models [59], [60], [61], [62].

With respect to Arabic Sarcasm Detection, the majority of research has focused on detecting sarcastic tweets. The author in [63] used Random Forests to identify sarcastic political tweets. [64] proposed a shared task on irony detection in Arabic Tweets. The submitted systems to the shared task varied in their approaches from classical models with count-based features [65], [66] to deep models [67], [68]. [69] highlighted the connection between sentiment analysis and sarcasm detection, by showing how sentiment classifiers fail with sarcastic inputs. They also proposed the largest publicly available Arabic sarcasm detection dataset, ArSarcasm, which we use in this work. We can see that so far, sarcasm detection methods have been applied to social media data collectively, with no effort made to study the zero-shot performance across dialects of state-of-the-art methods.

**Pre-trained Language Models.** Sequential transfer learning, where a network is first pre-trained on a relevant task before fine-tuning on the target task, originally appeared in domain of computer vision, and has recently been adapted in NLP. The author in [70] proposed to pre-train a LSTM network for language modeling and then fine-tune for classification. Similarly, ELMO [3] leveraged contextual representations obtained from a network pretrained for language modeling to perform many NLP tasks. Similar approaches were proposed such as BERT [5] that relied not on RNNs, but on bidirectional Transformers [4], and on a different pre-training objective, namely masked language modeling. Other variations appeared including RoBERTa [6], MASS [71], and ELECTRA [72]. Fine-tuning these pre-trained models on task-specific data has produced state-of-the-art performance, especially in cases when sufficiently large labeled data does not exist. They have been applied to several tasks, including text classification, question answering, named entity recognition [9], and POS tagging [8].

**Cross-lingual Learning.** Cross-lingual learning (CLL) refers to using labeled resources from resource-rich languages to build models for data-scarce languages. In a sense, knowledge learned about language structure and tasks is *transferred* to low-resource languages. Cross-lingual learning is of particular importance due to the scarcity of labeled resources in many of the world's languages, some of which are spoken by millions of people (Marathi and Gondi, for example). While our work can be better described as cross-dialectal, the techniques used for cross-lingual learning can easily be adapted for settings such as ours. In this work, Modern Standard Arabic (MSA) and Arabic dialects (DA) represent the high-resource and low-resource languages, respectively.

Many techniques were proposed for CLL, including using cross-lingual word embeddings [73], [74], [75], [76], where the two monolingual vector spaces are mapped into the same shared space. While cross-lingual word embeddings enable comparing meaning across languages [73], they typically fail when we do not have enough data to train good monolingual embeddings. In addition, adversarial learning [77] has played an important role in cross-lingual learning where an adversarial

objective is employed to learn language-independent representations [78], [79], [80], [81]. As a result, the model learns to rely more on general language structure and commonalities between languages, and therefore can generalize across languages. Multilingual extensions of pre-trained language models have emerged through joint pre-training on several languages. Examples include mBERT [5], XLM [82] and XLM-RoBERTa [9]. During pre-training on multiple languages, the model learns to exploit common structure among pre-training languages even without explicit alignment [83]. These models have become useful for few-shot and zero-shot cross-lingual settings, where there is little or no access to labeled data in the target language. For instance [9] evaluate a cross-lingual version of RoBERTa [6], namely XLM-RoBERTa, on cross-lingual learning across different tasks such as question answering, text classification, and named entity recognition.

**Semi-supervised Learning.** Several methods were proposed for leveraging unlabeled data for learning including co-training [84], graph-based learning [85], tri-training [86], and self-training [87]. A variety of semi-supervised learning methods have been successfully applied to a number of NLP tasks including NER [88], [89], POS tagging [90], parsing [91], word sense disambiguation [92], and text classification [93], [94]. Self-training has been applied in cross-lingual settings where gold labels are rare in the target language. For example, [95] proposed a combination of Active learning and self-training for cross-lingual sentiment classification. [96] made use of self-training for named entity tagging and linking across 282 different languages. [97] used self-training for cross-lingual word mapping to create additional word pairs for training. [98] employed self-training to improve zero-shot cross-lingual sentiment classification with mBERT [5]. With English as their source language, they improved performance on 7 languages by self-training using unlabeled data in their target languages. Lastly, [99] used the self-labeled examples produced by self-training to create adversarial examples in order to improve robustness and generalization.

We now introduce our tasks.

### III. TASKS

Named Entity Recognition (NER) is defined as the information extraction task that attempts to locate, extract, and automatically classify named entities into predefined classes or types in unstructured texts [100]. Typically, NER is integrated into more complex tasks, where, for example, we might need to handle entities in a special way. For instance, when translating the Arabic sentence “*حقق كرم فضية المصارعه*” to English, it would be useful to know that “*كرم*” is a person name, and therefore should not be translated into the word “generosity”. Similarly, NER can be useful for other tasks question answering, information retrieval and summarization.

Part-of-Speech (POS) tagging is the task of assigning a word in a context to its part-of-speech tag. Such tags include adverb (ADV), adjective (ADJ), pronoun (PRON), and many others. For example, given an input sentence “*أنا أحب كرة القدم*”, our goal is to tag each word as follows: أنا (PRON) أحب (VERB) كرة (NOUN) ال (DET) قدم (NOUN). POS tagging is an essential NLU task with many applications

in speech recognition, machine translation, and information retrieval. Both NER and POS tagging are sequence labeling tasks, where we assign a label to each word in the input context.

Sarcasm Detection is the task of identifying sarcastic utterances where the author intends a different meaning than what is being literally enunciated [46]. Sarcasm detection is crucial for NLU as neglecting to detect sarcasm can easily lead to the misinterpretation of the intended meaning, and therefore significantly degrade the accuracy of tasks such as sentiment classification, emotion recognition, and opinion mining [69]. For example the word “سعيد” in the utterance “أنا سعيد جدا بهذا الجوال البطيء” can erroneously lead sentiment classifiers into positive sentiment, although the sentiment has negative sentiment. Sarcasm Detection is typically treated as a binary classification task, where an utterance is classified as either sarcastic or not.

#### IV. METHOD

In this work, we show that models trained on MSA for NER, POS tagging, and Sarcasm Detection generalize poorly to dialect inputs when used in zero-shot-settings (i.e., no annotated DA data used during training). Across the three tasks, we test how self-training would fare as an approach to leverage unlabeled DA data to improve performance on DA. Self-training involves training a model using its own predictions on a set of unlabeled data identical from its original training split. Next, we formally describe our algorithm. The notation used in this section to describe our algorithm is directed towards sequence labeling (since we experiment with 2 sequence labeling tasks out of 3). However, it should be straightforward to adapt it to the context of text classification as in [98].

##### A. Self-training for Sequence Labeling

For sequence labeling, our proposed self-training procedure is given two sets of examples: a labeled set  $L$  and an unlabeled set  $U$ . To perform zero-shot MSA-to-DA transfer, MSA examples are used as the labeled set, while unlabeled DA examples are the unlabeled set. As shown in Fig. 1, each iteration of the self-training algorithm consists mainly in three steps. First, a pre-trained language model is fine-tuned on the labeled MSA examples  $L$ . Second, for every unlabeled DA example  $u_i$ , we use the model to tag each of its tokens to obtain a set of predictions and confidence scores for each token  $p_{u_i} = (l_1^{(i)}, c_1^{(i)}), (l_2^{(i)}, c_2^{(i)}), \dots, (l_{|u_i|}^{(i)}, c_{|u_i|}^{(i)})$ , where  $(l_j^{(i)}, c_j^{(i)})$  are the label and confidence score (Softmax probability) for the  $j$ -th token in  $u_i$ . Third, we employ a selection mechanism to identify examples from  $U$  that are going to be added to  $L$  for the next iteration.

For a selection mechanism, we experiment with both a thresholding approach and a fixed-size [98] approach. In the thresholding method, a threshold  $\tau$  is applied on the minimum confidence per example. That is, we only add an example  $u_i$  to  $L$  if  $\min_{(l_j^{(i)}, c_j^{(i)}) \in p_{u_i}} c_j^{(i)} \geq \tau$ . See Algorithm 1. The fixed-size approach involves, at each iteration, the selection of the top  $S$  examples with respect to the minimum confidence score

---

#### Algorithm 1: MSA-to-DA Self-Training for Sequence Labeling

---

```
1 Given set  $L$  of labeled MSA examples, set  $U$  of  
   unlabeled DA examples,  $\tau$  parameter for probability  
   threshold selection.  
2 repeat  
3   Fine-tune model  $M$  for  $K$  epochs on labeled  
   MSA examples  $L$ ;  
4   for  $u_i \in U$  do  
5     Obtain prediction  $p_{u_i}$  on unlabeled DA  
     example  $u_i$  using model  $M$ ;  
6     if  $\min_{(l_j^{(i)}, c_j^{(i)}) \in p_{u_i}} c_j^{(i)} \geq \tau$  then  
7       | remove  $u_i$  from  $U$  and add it to  $L$ ;  
8     end  
9 until stopping criterion satisfied
```

---

$\min_{(l_j^{(i)}, c_j^{(i)}) \in p_{u_i}} c_j^{(i)}$ , where  $S$  is a hyper-parameter. We experiment with both approaches and report results in Section VII.

##### B. Self-training for Classification

For sarcasm detection, we follow [98] who select an equivalent number of examples from each class, which we will refer to as *class balancing*. In other words, let  $c_{u_i}$  be the confidence of the most probable class assigned to example  $u_i$ . Then we sort the unlabeled examples in a descending order according to their confidence and select the top  $\lfloor S/C \rfloor$  examples from each class such that we have a total of  $S$  examples, where  $C$  is the number of classes.

For example if  $S = 100$  and  $C = 2$  i.e we have 2 classes, we will select the top 50 confident examples that were classified as positive and the top 50 confident examples classified as negative. Similarly to [98], we observe the positive effect of class balancing on the performance of self-training in sarcasm detection<sup>1</sup> and we compare class balancing against selecting the top  $S$  confident example regardless of their predicted class. See Section VII-C.

#### V. PRETRAINED LANGUAGE MODEL

In this work, we turn our attention to fine-tuning pre-trained language models (PLMs) on our three tasks. While self-training can basically be applied to many types of other models such as LSTM networks [14], we select PLMs for two reasons. First, PLMs have been shown to outperform models trained from scratch on a wide variety of tasks [5], [70], [82]. Second, we aim to show that even state-of-the-art models still perform poorly in certain low-resource settings asserting that we still need methods to handle such scenarios.

Pre-trained language models make use As a pre-trained language model, we use XLM-RoBERTa [9] (XML-R for short). XLM-R is a cross-lingual model, and we choose it since it is reported to perform better than mBERT, the multilingual

---

<sup>1</sup>We do not use class balancing with sequence labeling tasks since each example contains a set of tokens, each assigned to a possibly different class, which makes it very difficult to guarantee that an equal number of examples are selected for each class.

---

**Algorithm 2:** MSA-to-DA Self-Training for Classification

---

- 1 **Given** set  $L$  of labeled MSA examples, set  $U$  of unlabeled DA examples,  $S$  total number of unlabeled examples to add to the training data every iteration,  $C$  the number of classes.
  - 2 **repeat**
  - 3   Fine-tune model  $M$  for  $K$  epochs on labeled MSA examples  $L$ ;
  - 4   Obtain class predictions and confidences on all unlabeled DA examples  $u_i$  using model  $M$ ;
  - 5   Sort all unlabeled examples  $u_i$  in descending order by the confidence of their most probable class  $c_{u_i}$ ;
  - 6   Select the top  $\lfloor S/C \rfloor$  examples from each class, remove them from  $U$ , and add them to  $L$ ;
  - 7 **until** stopping criterion satisfied
- 

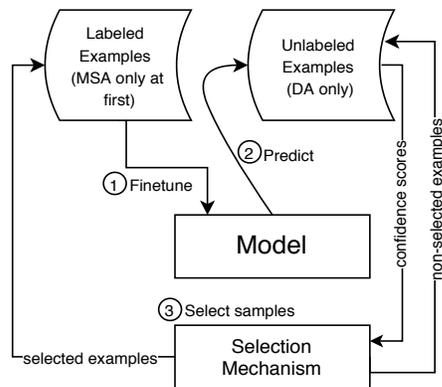


Fig. 1: MSA-to-DA Self-Training Transfer.

model from Google [5]. XLM-R also uses Common Crawl for training, which is more likely to have dialectal data than Wikipedia Arabic (used in mBERT), making it more suited to our work. We now introduce our experiments.

## VI. EXPERIMENTS

We begin our experiments with evaluating the standard fine-tuning performance of XLM-R models on NER, POS tagging, and SRD against strong baselines. We then use our best models from this first round to investigate the MSA-to-DA zero-shot transfer, showing a significant performance drop even when using pre-trained XLM-R. Consequently, we evaluate self-training in zero- (NER, POS tagging, SRD) and few-shot (POS tagging) settings, showing substantial performance improvements in both cases. We now introduce our datasets.

### A. Datasets

**NER:** For our work on NER, we use four datasets: ANERCorp [101]; ACE 2003 [102] BNews (BN-2003); ACE 2003 Newswire (NW-2003); and Twitter [29]. Named entity types in all datasets are *location* (LOC), *organization* (ORG), and *person* (PER).

**POS Tagging:** There are a number of Arabic POS tagging datasets, mostly on MSA [103] but also on dialects such as

EGY [104]. To show that the proposed approach is able to work across multiple dialects, we ideally needed data from more than one dialect. Hence, we use the multi-dialectal (MD) dataset from [45], comprising 350 tweets from various Arabic dialects including MSA, Egyptian (EGY), Gulf (GLF), and Levantine (LEV). This dataset has 21 POS tags, some of which are suited to social media (since it is derived from Twitter). We show the POS tag set from [45] in Table XIII (in the Appendix). We further evaluate fine-tuning XLMR for POS tagging on a Classical Arabic dataset, namely the Quranic Arabic Corpus (QAS). [105].

**Sarcasm Detection:** We use the Ar-Sarcasm dataset provided by [69], which has a total of 10,547 example split into training and test sets. Each example in this dataset is labeled by its dialect and sarcasm label. For our experiments, we set aside 20% of the training data as a development set. Table I shows sizes of the datasets used. We now introduce our baselines.

### B. Baselines

For the **NER task**, we use the following baselines:

- **NERA [31]:** A hybrid system of rule-based features and a decision tree classifier.
- **WC-BiLSTM [21]:** A character- and a word-level Bi-LSTM with a conditional random fields (CRF) layer.
- **WC-CNN [22]:** A character- and a word-level CNN with a CRF layer.
- **mBERT [5]:** A fine-tuned multilingual BERT-Base-Cased (110M parameters), pre-trained with a masked language modeling objective on the Wikipedia corpus of 104 languages (including Arabic). For fine-tuning, we find that (based on experiments on our development set) a learning rate of  $6 \times 10^{-5}$  works best with a dropout of 0.1.

In addition, we compare to the published results in [28], AraBERT [106], and CAMEL [107] for the ANERCorp dataset. We also compare to the published results in [22] for the 4 datasets.

For the **POS tagging task**, we compare to our own implementation of WC-BiLSTM (since there is no published research that uses this method on the task, as far as we know) and run mBERT on our data. We also compare to the CRF results published by [45]. In addition, for the Gulf dialect, we compare to the BiLSTM with compositional character representation and word representations (CC2W+W) published results in [25].

For the **Sarcasm Detection task**:

- **Word-level BiLSTM:** A bidirectional LSTM on the word level. We use the same hyper-parameters as in [69].
- **Word-level CNN [108]:** the network is has one convolutional layer of 10 filters of sizes 3, 5, and 7.
- **mBERT [5]:** mBERT fine-tuned for SRD. Here, we find that a different learning rate of  $5 \times 10^{-6}$  performs best.

### C. Experimental Setup

Our main models are XLM-R<sub>BASE</sub> ( $L = 12, H = 768, A = 12$ , 270M params) and XLM-R<sub>LARGE</sub> ( $L = 24, H = 1024, A = 16$ , 550M params), where  $L$  is number of

TABLE I: Datasets used for Each of the 3 Tasks Studied

Task	Dataset	Size
NER	ANERCorp [101]	~150K tokens
	ACE 2003-BNews [102]	~15K tokens
	ACE 2003-News Wire [102]	~27K tokens
	Twitter [29]	~81K tokens
POS Tagging	Multi-dialectal (MD) - MSA [45]	~26K tokens
	Multi-dialectal (MD) - EGY [45]	~23K tokens
	Multi-dialectal (MD) - GLF [45]	~21K tokens
	Multi-dialectal (MD) - LEV [45]	~23K tokens
	Quranic Arabic Corpus (QAC)	~134K tokens
Sarcasm Detection	Ar-Sarcasm [69]	~10K sentences

layers,  $H$  is the hidden size,  $A$  is the number of self-attention heads. For XLM-R experiments, we use Adam optimizer with  $1e^{-5}$  learning rate, batch size of 16. We typically fine-tune for 20 epochs, keeping the best model on the development set for testing. We report results on the test split for each dataset, across the two tasks. For all BiLSTM experiments, we use the same hyper-parameters as [22].

For all the self-training experiments, we use the dialect subset of the Arabic online news commentary (AOC) dataset [109], comprising the EGY, GLF, and LEV varieties limiting to equal sizes of 9K examples per dialect (total =27K)<sup>2</sup>. We use the split from [110] of AOC, removing the dialect labels and just using the comments themselves for our self-training. Each iteration involved fine-tuning the model for  $K = 5$  epochs. As a stopping criterion, we use early stopping with patience of 10 epochs. Other hyper-parameters are set as listed before. For selecting confident samples, we experiment with a fixed number of top samples  $S = [50, 100, 200]$  and selection based on a probability threshold  $\tau = [0.80, 0.90, 0.95]$  (softmax values)<sup>3</sup>. For all evaluations, we use the *seqeval* toolkit<sup>4</sup>.

## VII. RESULTS

### A. Fine-tuning XLM-R

We start by showing the result of fine-tuning XLM-R on the **NER task**, on each of the four Arabic NER (ANER) datasets listed in Section VI-A. Table II shows the test set macro  $F_1$  score on each of the four ANER datasets. Clearly, the fine-tuned XLM-R models outperform other baselines on all datasets, except on the NW-2003 where WC-CNN [22] performs slightly better than XLM-R<sub>LARGE</sub>.

For **POS Tagging**, Table III shows test set word accuracy of the XLM-R models compared to baselines on the Quranic Arabic Corpus (QAC) and four different subsets from the multi-dialectal dataset [45]. Again, XLM-R models (both base and large) outperform all other models. A question arises why XLM-R models outperform both mBERT and AraBERT. As noted before, for XLM-R vs. mBERT, XLM-R was pre-trained on much larger data: CommonCrawl for XLM-R vs.

Wikipedia for mBERT. Hence, the *larger dataset* of XLM-R is giving it an advantage over mBERT. For comparison with AraBERT, although the pre-training data for XLM-R and AraBERT may be comparable, even the smaller XLM-R model (XLM-R<sub>BASE</sub>) has more than twice the number of parameters of the BERT<sub>BASE</sub> architecture on which AraBERT and mBERT are built (270M v. 110M). Hence, XLM-R model *capacity* gives it another advantage. We now report our experiments with zero-shot transfer from MSA to DA.

For **Sarcasm Detection**, we fine-tune XLM-R<sub>BASE</sub> and XLM-R<sub>LARGE</sub> on the full Ar-Sarcasm dataset and compare their performance against three different baselines in Table IV. Worst performance is given by CNN, which can be attributed to the way CNNs work; by capturing local n-gram features, the CNN filters fail to learn the wide contextual features required to detect sarcasm. Clearly, mBERT is performing very well compared to BiLSTM and CNN but XLM-R<sub>BASE</sub> and XLM-R<sub>LARGE</sub> outperform all other baselines on the task with 69.83% and 74.07% macro F1 points, respectively, achieving new state-of-the-art on the Ar-Sarcasm dataset.

### B. MSA-DA Zero-Shot Transfer

As before, we start by the discussion of **NER experiments**. To evaluate the utility of approach, we obviously need DA data labeled for NER. We observed that the dataset from [29] contains both MSA and DA examples (tweets). Hence, we train a binary classifier to distinguish DA data from MSA<sup>5</sup>. We then extract examples that are labeled with probability  $p > 0.90$  as either DA or MSA. We obtain 2,027 MSA examples (henceforth, *Darwish-MSA*) and 1,695 DA examples (henceforth, *Darwish-DA*), respectively. We split these into development and test sets with 30% and 70% ratios. As for **POS Tagging**, we already have MSA data for training and the three previously used DA datasets, namely EGY, GLF and LEV, for evaluation. We use those for the zero-shot setting by omitting their training sets and using only the development and test sets.

We first study how well models trained for NER and POS tagging on MSA data only will generalize to DA inputs during test time. We evaluate this zero-shot performance on both the XLM-R<sub>BASE</sub> and XLM-R<sub>LARGE</sub> models. For **NER**, we train on ANERCorp (which is pure MSA) and evaluate

<sup>2</sup>We note that our approach could be scaled with an even bigger unlabeled dataset, given the performance gains we report with self-training in this work.

<sup>3</sup>It is worth noting that our  $S$  values are similar to those used in [98]. We also experimented with other values for  $\tau$  and  $S$ , but found them sub-optimal and hence we report performance only for the listed values of these two hyper-parameters here.

<sup>4</sup><https://github.com/chakki-works/seqeval>

<sup>5</sup>The classifier is XLM-R<sub>BASE</sub> fine-tuned on the AOC data. The fine-tuned model achieved development and test accuracies of 90.3% and 89.4%, respectively, outperforming the best results in [110].

TABLE II: Test Set Macro F<sub>1</sub> Scores for NER

Model	ANERCorp	BN-2003	NW-2003	NW-2004	Twitter
NERA [31]	88.77	–	–	–	–
CAMeL [107]	85.00	–	–	–	–
Hybrid [28]	90.66	–	–	–	–
WC-BiLSTM [21]	88.56	94.92	90.32	89.62	64.93
WC-CNN [22]	88.77	94.12	<b>91.20</b>	<b>91.47</b>	65.34
mBERT (ours)	85.86	89.52	87.19	88.58	58.92
AraBERT [106]	84.2	–	–	–	–
XLM-R <sub>BASE</sub> (ours)	87.75	95.35	85.25	89.61	60.39
XLM-R <sub>LARGE</sub> (ours)	<b>91.43</b>	<b>97.33</b>	91.10	90.78	<b>68.91</b>

TABLE III: Test Set Accuracy for POS Tagging using Several Baselines

Model	QAC	MD-MSA	MD-EGY	MD-GLF	MD-LEV
BiLSTM (CC2W + W) [25]	–	–	–	89.7	–
CRF [45]	–	93.6	92.9	87.8	87.9
WC-BiLSTM (ours)	91.65	94.63	93.41	88.79	86.13
mBERT (ours)	94.83	90.57	92.88	87.85	72.30
XLM-R <sub>BASE</sub> (ours)	<b>96.70</b>	96.30	94.70	92.18	89.98
XLM-R <sub>LARGE</sub> (ours)	96.59	<b>98.21</b>	<b>97.00</b>	<b>94.41</b>	<b>93.19</b>

TABLE IV: Macro F1 Scores with Several Baselines for Sarcasm Detection. Dataset used is Ar-Sarcasm [69]

Model	DEV	TEST
BiLSTM [69]	63.51	62.19
CNN	59.7	58.50
mBERT	68.87	69.51
XLM-R <sub>BASE</sub> (ours)	73.22	69.83
XLM-R <sub>LARGE</sub> (ours)	<b>73.72</b>	<b>74.07</b>

on both Darwish-MSA and Darwish-DA. While for POS tagging, we train on the MSA subset [45] and evaluate on the corresponding test set for each dialect. As shown in Table V, For NER, a significant generalization gap of around 20 % F<sub>1</sub> points exists between evaluation on MSA and DA using both models. While for **POS tagging**, the gap is as large as 18.13 % accuracy for the LEV dialect with XLM-R<sub>BASE</sub>. The smallest generalization gap is on the GLF variety, which is perhaps due to the high overlap between GLF and MSA [25].

**For Sarcasm Detection**, Since Ar-Sarcasm is labeled by dialect, it is trivial to extract the MSA examples for training. Similarly to what was done with the NER data, we split all<sup>6</sup> the remaining DA examples into development and test sets with 30% and 70% ratios, respectively for evaluation. Finally, we obtain 4506 MSA training, 1202 DA development, and 2268 DA test examples. As shown in Table V, a performance gap of around 8 macro F1 points with both XLM-R<sub>BASE</sub> and XLM-R<sub>LARGE</sub>, showing poor generalization on DA in context of text classification, as well. In the next section, we evaluate the ability of self-training to close this MSA-DA performance gap.

<sup>6</sup>Without this, we had only 528 and 698 development and test examples, respectively and it resulted in high variance in the results obtained. So we had to increase the sizes of the development and test sets by sacrificing the DA training data.

### C. Zero-shot Self-Training

Here, **for NER**, similar to Section VII-B, we train on ANERCorp (pure MSA) and evaluate on Darwish-MSA and Darwish-DA. Table VI shows self-training NER results employing the selection mechanisms listed in Section IV, and with different values for  $S$  and  $\tau$ . The best improvement is achieved with the thresholding selection mechanism with a  $\tau = 0.90$ , where we have an F<sub>1</sub> gain of 10.03 points. More generally, self-training improves zero-shot performance in all cases albeit with different F<sub>1</sub> gains. Interestingly, we find that self-training also improves test performance on MSA with the base XLM-R model. This is likely attributed to the existence of MSA content in the unlabeled AOC data. It is noteworthy, however, that the much higher-capacity large model deteriorates on MSA if self-trained (dropping from 68.32% to 67.21%). This shows the ability of the large model to learn representations very specific to DA when self-trained. It is also interesting to see that the best self-trained base model achieving 50.10% F<sub>1</sub>, outperforming the large model before the latter is self-trained (47.35% in the zero-shot setting). This shows that a base self-trained model, suitable for running on terminal machines with less computational capacity, can (and in our case does) improve over a large (not-self-trained) model that needs significant computation. The fact that, when self-trained, the large model improves 15.35% points over the base model in the zero-shot setting (55.42 vs. 40.07) is remarkable.

As **for POS tagging**, we similarly observe consistent improvements in zero-shot transfer with self-training (Table VII). The best model achieves accuracy gains of 2.41% (EGY), 1.41% (GLF), and 1.74% (LEV). Again, this demonstrates the utility of self-training pre-trained language models on the POS tagging task even in absence of labeled dialectal POS data (zero-shot).

**For Sarcasm Detection**, we follow [98] in balancing the examples selected in each self-training iteration through selecting an equal number of examples from each class (sarcastic and non-sarcastic). Without the balancing step, we find that

TABLE V: Zero-shot Transfer Results on the DA Test Sets. Metrics used are Macro  $F_1$  for NER and Sarcasm Detection, and Accuracy for POS Tagging. Models are Trained on MSA only and Evaluated on DA. Datasets used are: Darwish-MSA and Darwish-DA [29] (NER), Multi-Dialectal [45] (POS Tagging), and Ar-Sarcasm [69] (Sarcasm Detection). As shown, a Significant Performance Drop Exists when Training on MSA and Evaluating on DA

Model	NER		POS Tagging			Sarcasm Detection		
	MSA	DA	MSA	EGY	GLF	LEV	MSA	DA
XLM-R <sub>BASE</sub>	60.42	40.07	96.30	78.38	83.72	78.17	68.68	60.17
XLM-R <sub>LARGE</sub>	68.32	47.35	98.21	82.28	85.95	81.24	71.55	62.90

TABLE VI: Test Set Macro  $F_1$  in the Zero-Short Setting for NER. Training was Done on MSA Data Only. **ST** Stands for Self-Training. Models were Trained on ANERCorp (Pure MSA) and Evaluated on Darwish-MSA and Darwish-DA Extracted from the Twitter Dataset [45]. Self-training Boosts the Performance on DA Data by 10% Macro F1 Points with XLM-R<sub>BASE</sub> and  $\tau = 0.90$

Model	Darwish-MSA	Darwish-DA
XLM-R <sub>BASE</sub>	61.88	40.07
XLM-R <sub>BASE</sub> , ST, S=50	60.98	43.88
XLM-R <sub>BASE</sub> , ST, S=100	61.13	42.01
XLM-R <sub>BASE</sub> , ST, S=200	61.46	43.49
XLM-R <sub>BASE</sub> , ST, $\tau = 0.80$	<b>63.36</b>	46.97
XLM-R <sub>BASE</sub> , ST, $\tau = 0.90$	61.02	<b>50.10</b>
XLM-R <sub>BASE</sub> , ST, $\tau = 0.95$	62.25	47.91
XLM-R <sub>LARGE</sub>	<b>68.32</b>	47.35
XLM-R <sub>LARGE</sub> + ST, $\tau = 0.90$	67.21	<b>55.42</b>

the selected examples come from the most frequent class (non-sarcastic), which hurts performance since the model is learning only one class. The results for sarcasm detection are shown in Table VIII, where we see that self-training adds 3% and 2.5% (for XLM-R<sub>BASE</sub>) and 5.9% and 4.5% (for XLM-R<sub>LARGE</sub>) macro F1 points on the development and test sets, respectively using the best settings for self-training ( $S = 100$  with class balancing). We also find that selection based on probability thresholds performs much worse than fixed-size selection, hence we omit these results.

TABLE VII: Test Set Accuracy in the Zero-Shot Setting for POS Tagging. **ST** Stands for Self-Training. Models were Trained on the MSA Data of the When Training on MSA Only. Self-Training Boosts Performance of XLM-R<sub>BASE</sub> by Around 2% Accuracy Points on Different Dialects with the Best Setting of  $S = 50$

Model	MSA	EGY	GLF	LEV
XLM-R <sub>BASE</sub>	96.30	78.38	83.72	78.17
XLM-R <sub>BASE</sub> , ST, S=50	-	<b>80.79</b>	<b>85.13</b>	<b>79.91</b>
XLM-R <sub>BASE</sub> , ST, S=100	-	80.43	84.74	79.16
XLM-R <sub>BASE</sub> , ST, S=200	-	78.75	84.21	79.40
XLM-R <sub>BASE</sub> , ST, $\tau = 0.90$	-	79.52	83.97	79.21
XLM-R <sub>BASE</sub> , ST, $\tau = 0.85$	-	78.97	83.53	79.06
XLM-R <sub>BASE</sub> , ST, $\tau = 0.80$	-	78.88	83.72	78.50
XLM-R <sub>LARGE</sub>	98.21	82.28	85.95	81.24
XLM-R <sub>LARGE</sub> + ST, S=50	-	<b>82.65</b>	<b>87.76</b>	<b>83.70</b>

#### D. Ablation Experiment

Here, we conduct an ablation experiment with the NER task in order to verify our hypothesis that the performance boost primarily comes from using unlabeled DA data for self-training. By using a MSA dataset with the same size as our unlabeled DA one<sup>7</sup>, we can compare the performance of the self-trained model in both settings: MSA and DA unlabeled data. We run three different self-training experiments using 3 different values for  $\tau$  using each type of unlabeled data. Results are shown in Table IX. While we find slight performance boost due to self-training even with MSA unlabeled data, the average F1 score with unlabeled DA is better by 2.67 points, showing that using unlabeled DA data for self-training has helped the model adapt to DA data during testing.

### VIII. ERROR ANALYSIS

#### A. NER

To understand why self-training the pre-trained language model improves over mere fine-tuning, we perform an error analysis. For the error analysis, we focus on the NER task where we observe a huge self-training gain. We use the development set of Darwish-DA (see Section VII-C) for the error analysis. We compare predictions of the standard fine-tuned XLM-R<sub>BASE</sub> model (FT) and the best performing self-training ( $\tau = 0.9$ ) model (ST) on the data. The error analysis leads to an interesting discovery: The greatest benefit from the ST model comes mostly from reducing *false positives* (see Table X). In other words, self-training helps regularize the model predictions such that tokens misclassified by the original FT model as a named entities are now correctly tagged as *unnamed entity* “O”.

To understand why the ST model improves false positive rate, we manually inspect the cases it correctly identifies that were misclassified by the FT model. We show examples of these cases in Table XIV (in the Appendix). As the table shows, the ST model is able to identify dialectal tokens whose equivalent MSA forms can act as trigger words (usually followed by a PER named entity). We refer to this category as *false trigger words*. An example is the word **نبي** “prophet” (row 1 in Table XIV). A similar example that falls within this category is in row (2), where the model is confused by the token **الى** (“who” in EGY, but “to” in MSA and hence the wrong prediction as LOC). A second category of errors is caused by *non-standard social media language*, such as use of letter repetitions in interjections (e.g., in row (3) in

<sup>7</sup>We use a set of MSA tweets from the AOC dataset mentioned before.

TABLE VIII: Macro F<sub>1</sub> in the Zero-Shot Setting for Sarcasm Detection on the Ar-Sarcasm [69] Dataset. Training was Done on MSA Data Only. **ST**: Stands for Self-Training. An Obvious Performance Boost Occurs when using Self-Training in the Best Setting with  $S = 100$  and Class Balancing

Model	MSA		DA	
	DEV	TEST	DEV	TEST
XLM-R <sub>BASE</sub>	65.64	68.68	61.66	60.17
XLM-R <sub>BASE</sub> + ST, S=50,	-	-	62.53	60.82
XLM-R <sub>BASE</sub> + ST, S=100	-	-	61.15	59.46
XLM-R <sub>BASE</sub> + ST, S=200	-	-	62.57	60.25
XLM-R <sub>BASE</sub> + ST, S=50, class balancing	-	-	62.49	59.34
XLM-R <sub>BASE</sub> + ST, S=100, class balancing	-	-	<b>64.72</b>	<b>62.66</b>
XLM-R <sub>BASE</sub> + ST, S=200, class balancing	-	-	62.89	59.46
XLM-R <sub>LARGE</sub>	67.81	71.55	62.28	62.90
XLM-R <sub>LARGE</sub> + ST, S=100, class balancing	-	-	<b>68.21</b>	<b>67.43</b>

TABLE IX: Ablation Experiment with MSA Unlabeled Data for Zero-Shot NER. Development Set Macro F1 is Shown when Using Both Unlabeled MSA and DA Data with the Same Size. Average Performance with DA Unlabeled Data is Higher Showing the Effect of Unlabeled DA on the Model Final Performance

Setting	Unlbl. MSA	Unlbl. DA
XLM-R <sub>BASE</sub> , ST, $\tau = 0.80$	43.88	44.46
XLM-R <sub>BASE</sub> , ST, $\tau = 0.90$	44.69	47.83
XLM-R <sub>BASE</sub> , ST, $\tau = 0.95$	43.43	46.87
Avg	43.67	<b>46.34</b>

Table XIV). In these cases, the FT model also assigns the class PER, but the ST model correctly identifies the tag as “O”. A third class of errors arises as a result of *out-of-MSA* vocabulary. For example, the words in rows (4-6) are all out-of-MSA where the FT model, not knowing these, assigns the most frequent named entity label in train (PER). A fourth category of errors occurs as a result of a token that is usually part of a named entity in MSA, that otherwise functions as part of an *idiomatic expression* in DA. Row (7) in Table XIV illustrates this case.

We also investigate errors shared by both the FT and ST models (errors which the ST model also could not fix). Some of these errors result from the fact that often times both MSA and DA use the same word for both person and location names. Row (1) in Table XV (in the Appendix) is an example where the word “Mubarak”, name of the ex-Egypt President, is used as LOC. Other errors include *out-of-MSA* tokens mistaken as named entities. An example is in row (3) in Table XV, where بأمارة (“proof” or “basis” in EGY) is confused for إمارة (“emirate”, which is a location). *False trigger words*, mentioned before, also play a role here. An example is in row (7) where يبطل is confused for PER due to the trigger word يا “Hey!” that is usually followed by a person name. *Spelling mistakes* cause third source of errors, as in row (4). We also note that even with self-training, detecting ORG entities is more challenging than PER or LOC. The problem becomes harder when such organizations are not seen in training such as in rows (8) قناة العربية (9) الاخوان المسلمين

and (10) المجلس العسكري, all of which do not occur in the training set (ANERCorp).

Here we investigate the false negatives produces by the self-trained models observing a number of named entities that were misclassified by the self-trained model as unnamed ones. See Table XVI (in the Appendix). As an example, we take the last name الجزوري which was classified both correctly and incorrectly in different contexts by the self-trained model. Context of correct classification is “هاش تاج لكمال الجزوري”, while it is “ماسك على الناس كلها سي دي الا الجزوري ماسك عليه فلوبي” for the incorrect classification. First, we note that الجزوري is not a common name (zero occurrences in the MSA training set). Second, we observe that in the correct case, the word was preceded by the first name كمال which was correctly classified as PER, making it easier for the model to assign PER to the word afterwards as a surname.

TABLE X: Comparison of Error Categories in Percentage between the Fine-Tuned Model (FT) and the Model Combining Fine-Tuned+self-trained (ST) Model for NER. The Values are based on the Dialectal Part of the Development Set

Measure	FT	ST	% improvement
True Positives	155	165	+6.5 %
False Positive	159	64	+59.7 %
False Negatives	162	168	-3.7 %
True Negatives	5,940	6,035	+1.5 %

TABLE XI: **NER task**. Sample False Negatives Produced by Self-Training

no.	Word	Gold	FT	ST
(1)	الاخوان	ORG	ORG	O
(2)	للبرادي	PER	PER	O
(3)	محمدي الجبلاد	PER	PER	O
(4)	فان ديزل	PER	PER	O
(5)	الجزوري	PER	PER	O
(6)	زين يسون	PER	PER	O

## B. Sarcasm Detection

We also conduct an error analysis on Sarcasm Detection comparing the predictions of XLM-R<sub>BASE</sub> with and without self-training. For that we use the best model on the development set (XLM-R<sub>BASE</sub>, S=100 with class balancing). Our analysis with SRD yields a similar observation to NER, where the performance boost driven by self-training is mostly due to the alleviation of false positives or the improvement of true negatives<sup>8</sup>. Table XII compares performance measures between the two models. However, we can see that, unlike NER, false negatives increase by as much as 44%, which is likely due to the self-training regularization effect mentioned earlier.

We also analyze sample errors that were fixed by the self-trained model. See Table XVII (in the Appendix). The first four examples represent false negatives, where the fine-tuned model assumed to be non-sarcastic. We can see that in such dialectal contexts, the fine-tuned model suffers from many unseen words during training on MSA. More specifically, words such as *بيه* and *غساله* in example (1), or *عاهات* in (2), *عبيط* in (4), or an idiom such as *حاميها حراميها* in (3), or *ما كانش حد غلب* in (5), or *ياترى* in (6), all of which represent dialect-specific language that is not encountered in MSA contexts, and therefore represents a significant challenge in zero-shot settings.

In addition, we show sample errors shared between the fine-tuned and the self-training models. See Table XVIII (in the Appendix). As to why the self-trained model has not corrected these errors, we can hypothesize that it may be due to that the vocabulary used in these inputs was not seen during self-training. In other words, this vocabulary was either not selected by the self-training selection mechanism to be added to the training data or not existing at all in the unlabeled examples used for self-training. As a result, the model was not adapted sufficiently to handle these or similar contexts. We assume the performance on these inputs could improve with larger and more diverse unlabeled examples used for self-training.

TABLE XII: Comparison of Error Categories in Percentage between the Fine-Tuned Model (FT) and the Model Combining Fine-Tuned+Self-Trained (ST) Model for Sarcasm Detection, based on the Dialectal Part of the Development Set

Measure	FT	ST	% improvement
True Positives	737	688	-6.6 %
False Positive	230	185	+19.7 %
False Negatives	111	160	-44.1 %
True Negatives	124	169	+36.29 %

## IX. CONCLUSION

Even though pre-trained language models have improved many NLP tasks, they still need a significant amount of labeled data for high-performance fine-tuning. In this paper, we proposed to self-train pre-trained language models by using unlabeled Dialectal Arabic (DA) data to improve zero-shot performance when training on Modern Standard Arabic (MSA) data only. Our experiments showed substantial performance

<sup>8</sup>We can see that in binary classification, every false positive removed is a true negative added

gains on two sequence labeling tasks (NER and POS), and one text classification task (sarcasm detection) on different Arabic varieties. Our method is dialect- and task-agnostic, and we believe it can be applied to other tasks and dialectal varieties. We intend to test this claim in future research. Moreover, we evaluated the fine-tuning of the recent XLM-RoBERTa language models, establishing new state-of-the-art results on all of the three tasks studied.

## REFERENCES

- [1] W. Xu and A. Rudnicky, "Can artificial neural networks learn language models?" in *Sixth international conference on spoken language processing*, 2000.
- [2] Y. Bengio, R. Ducharme, P. Vincent, and C. Jauvin, "A neural probabilistic language model," *Journal of machine learning research*, vol. 3, no. Feb, pp. 1137–1155, 2003.
- [3] M. E. Peters, M. Neumann, M. Iyyer, M. Gardner, C. Clark, K. Lee, and L. Zettlemoyer, "Deep contextualized word representations," in *Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, NAACL-HLT 2018, New Orleans, Louisiana, USA, June 1-6, 2018, Volume 1 (Long Papers)*, M. A. Walker, H. Ji, and A. Stent, Eds. Association for Computational Linguistics, 2018, pp. 2227–2237. [Online]. Available: <https://doi.org/10.18653/v1/n18-1202>
- [4] 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.
- [5] J. Devlin, M. Chang, K. Lee, and K. Toutanova, "BERT: pre-training of deep bidirectional transformers for language understanding," pp. 4171–4186, 2019. [Online]. Available: <https://doi.org/10.18653/v1/n19-1423>
- [6] Y. Liu, M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov, "Roberta: A robustly optimized BERT pretraining approach," *CoRR*, vol. abs/1907.11692, 2019. [Online]. Available: <http://arxiv.org/abs/1907.11692>
- [7] A. Yang, Q. Wang, J. Liu, K. Liu, Y. Lyu, H. Wu, Q. She, and S. Li, "Enhancing pre-trained language representations with rich knowledge for machine reading comprehension," in *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, 2019*, pp. 2346–2357.
- [8] H. Tsai, J. Riesa, M. Johnson, N. Arivazhagan, X. Li, and A. Archer, "Small and practical BERT models for sequence labeling," pp. 3630–3634, 2019. [Online]. Available: <https://doi.org/10.18653/v1/D19-1374>
- [9] A. Conneau, K. Khandelwal, N. Goyal, V. Chaudhary, G. Wenzek, F. Guzmán, E. Grave, M. Ott, L. Zettlemoyer, and V. Stoyanov, "Unsupervised cross-lingual representation learning at scale," pp. 8440–8451, 2020. [Online]. Available: <https://www.aclweb.org/anthology/2020.acl-main.747/>
- [10] K. Darwish, M. Attia, H. Mubarak, Y. Samih, A. Abdelali, L. Márquez, M. Eldesouki, and L. Kallmeyer, "Effective multi dialectal arabic pos tagging," *Natural Language Engineering*, vol. 1, no. 1, p. 18, 2020.
- [11] K. Shaalan, "A survey of arabic named entity recognition and classification," *Computational Linguistics*, vol. 40, no. 2, pp. 469–510, 2014.
- [12] H. M. Wallach, "Conditional random fields: An introduction," *Technical Reports (CIS)*, p. 22, 2004.
- [13] L. R. Medsker and L. Jain, "Recurrent neural networks," *Design and Applications*, vol. 5, 2001.
- [14] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
- [15] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks," *IEEE transactions on Signal Processing*, vol. 45, no. 11, pp. 2673–2681, 1997.
- [16] Z. Huang, W. Xu, and K. Yu, "Bidirectional LSTM-CRF models for sequence tagging," *CoRR*, vol. abs/1508.01991, 2015. [Online]. Available: <http://arxiv.org/abs/1508.01991>

- [17] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean, "Distributed representations of words and phrases and their compositionality," in *Advances in neural information processing systems*, 2013, pp. 3111–3119.
- [18] J. Pennington, R. Socher, and C. 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.
- [19] Q. Wang and M. Iwaihara, "Deep neural architectures for joint named entity recognition and disambiguation," pp. 1–4, 2019. [Online]. Available: <https://doi.org/10.1109/BIGCOMP.2019.8679233>
- [20] X. Ma and E. H. Hovy, "End-to-end sequence labeling via bi-directional lstm-cnns-crf," 2016. [Online]. Available: <https://doi.org/10.18653/v1/p16-1101>
- [21] M. Gridach, "Character-aware neural networks for arabic named entity recognition for social media," in *Proceedings of the 6th workshop on South and Southeast Asian natural language processing (WSANLP2016)*, 2016, pp. 23–32.
- [22] M. Khalifa and K. Shaalan, "Character convolutions for arabic named entity recognition with long short-term memory networks," *Computer Speech & Language*, vol. 58, pp. 335–346, 2019.
- [23] M. Al-Smadi, S. Al-Zboon, Y. Jararweh, and P. Juola, "Transfer learning for arabic named entity recognition with deep neural networks," *IEEE Access*, vol. 8, pp. 37 736–37 745, 2020.
- [24] I. El Bazi and N. Laachfoubi, "Arabic named entity recognition using deep learning approach," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 9, no. 3, 2019.
- [25] R. Alharbi, W. Magdy, K. Darwish, A. AbdelAli, and H. Mubarak, "Part-of-speech tagging for arabic gulf dialect using bi-lstm," in *Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018)*, 2018.
- [26] W. AlKhwitter and N. Al-Twaresh, "Part-of-speech tagging for arabic tweets using crf and bi-lstm," *Computer Speech & Language*, vol. 65, p. 101138, 2021.
- [27] Y. Samih, M. Attia, M. Eldesouki, A. Abdelali, H. Mubarak, L. Kallmeyer, and K. Darwish, "A neural architecture for dialectal arabic segmentation," in *Proceedings of the Third Arabic Natural Language Processing Workshop*, 2017, pp. 46–54.
- [28] K. Shaalan and M. Oudah, "A hybrid approach to arabic named entity recognition," *Journal of Information Science*, vol. 40, no. 1, pp. 67–87, 2014.
- [29] K. Darwish, "Named entity recognition using cross-lingual resources: Arabic as an example," in *Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, vol. 1, 2013, pp. 1558–1567.
- [30] A. Abdul-Hamid and K. Darwish, "Simplified feature set for Arabic named entity recognition," in *Proceedings of the 2010 Named Entities Workshop*. Association for Computational Linguistics, 2010, pp. 110–115.
- [31] S. Abdallah, K. Shaalan, and M. Shoaib, "Integrating rule-based system with classification for arabic named entity recognition," in *International Conference on Intelligent Text Processing and Computational Linguistics*. Springer, 2012, pp. 311–322.
- [32] Y.-Y. Song and L. Ying, "Decision tree methods: applications for classification and prediction," *Shanghai archives of psychiatry*, vol. 27, no. 2, p. 130, 2015.
- [33] A. Zirikly and M. Diab, "Named entity recognition for arabic social media," in *Proceedings of the 1st Workshop on Vector Space Modeling for Natural Language Processing*, 2015, pp. 176–185.
- [34] A. Pasha, M. Al-Badrashiny, M. T. Diab, A. El Kholly, R. Eskander, N. Habash, M. Pooleery, O. Rambow, and R. Roth, "Madamira: A fast, comprehensive tool for morphological analysis and disambiguation of arabic," in *LREC*, vol. 14, no. 2014. Citeseer, 2014, pp. 1094–1101.
- [35] S. Khoja, "Apt: Arabic part-of-speech tagger," in *Proceedings of the Student Workshop at NAACL*. Citeseer, 2001, pp. 20–25.
- [36] S. Alrainy, "A morphological-syntactical analysis approach for arabic textual tagging," 2008.
- [37] Y. Tlili-Guiassa, "Hybrid method for tagging arabic text," *Journal of Computer science*, vol. 2, no. 3, pp. 245–248, 2006.
- [38] M. Diab, K. Hacioglu, and D. Jurafsky, "Automatic tagging of arabic text: From raw text to base phrase chunks," in *Proceedings of HLT-NAACL 2004: Short papers*, 2004, pp. 149–152.
- [39] J. H. Yousif and T. M. T. Sembok, "Arabic part-of-speech tagger based support vectors machines," in *2008 International Symposium on Information Technology*, vol. 3. IEEE, 2008, pp. 1–7.
- [40] K. Darwish, H. Mubarak, A. Abdelali, and M. Eldesouki, "Arabic pos tagging: Don't abandon feature engineering just yet," in *Proceedings of the Third Arabic Natural Language Processing Workshop*, 2017, pp. 130–137.
- [41] K. Alrajhi and M. A. ELAffendi, "Automatic arabic part-of-speech tagging: Deep learning neural lstm versus word2vec," *International Journal of Computing and Digital Systems*, vol. 8, no. 03, pp. 307–315, 2019.
- [42] S. Khalifa, S. Hassan, and N. Habash, "A morphological analyzer for gulf arabic verbs," in *Proceedings of the Third Arabic Natural Language Processing Workshop*, 2017, pp. 35–45.
- [43] K. Duh and K. Kirchoff, "Pos tagging of dialectal arabic: a minimally supervised approach," in *Proceedings of the acl workshop on computational approaches to semitic languages*, 2005, pp. 55–62.
- [44] R. Al-Sabbagh and R. Girju, "Yadac: Yet another dialectal arabic corpus," in *LREC*, 2012, pp. 2882–2889.
- [45] K. Darwish, H. Mubarak, A. Abdelali, M. Eldesouki, Y. Samih, R. Alharbi, M. Attia, W. Magdy, and L. Kallmeyer, "Multi-dialect arabic pos tagging: a crf approach," in *Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018)*, 2018.
- [46] C. Van Hee, E. Lefever, and V. Hoste, "Semeval-2018 task 3: Irony detection in english tweets," in *Proceedings of The 12th International Workshop on Semantic Evaluation*, 2018, pp. 39–50.
- [47] F. Barbieri, H. Saggion, and F. Ronzano, "Modelling sarcasm in twitter, a novel approach," in *Proceedings of the 5th Workshop on Computational Approaches to Subjectivity, Sentiment and Social Media Analysis*, 2014, pp. 50–58.
- [48] G. Abercrombie and D. Hovy, "Putting sarcasm detection into context: The effects of class imbalance and manual labelling on supervised machine classification of twitter conversations," in *Proceedings of the ACL 2016 student research workshop*, 2016, pp. 107–113.
- [49] A. Joshi, V. Sharma, and P. Bhattacharyya, "Harnessing context incongruity for sarcasm detection," in *Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing (Volume 2: Short Papers)*, 2015, pp. 757–762.
- [50] M. Bouazizi and T. O. Ohtsuki, "A pattern-based approach for sarcasm detection on twitter," *IEEE Access*, vol. 4, pp. 5477–5488, 2016.
- [51] S. K. Bharti, K. S. Babu, and S. K. Jena, "Parsing-based sarcasm sentiment recognition in twitter data," in *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. IEEE, 2015, pp. 1373–1380.
- [52] S. Saha, J. Yadav, and P. Ranjan, "Proposed approach for sarcasm detection in twitter," *Indian Journal of Science and Technology*, vol. 10, no. 25, pp. 1–8, 2017.
- [53] S. Porwal, G. Ostwal, A. Phadtare, M. Pandey, and M. V. Marathe, "Sarcasm detection using recurrent neural network," in *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2018, pp. 746–748.
- [54] Y. Ren, D. Ji, and H. Ren, "Context-augmented convolutional neural networks for twitter sarcasm detection," *Neurocomputing*, vol. 308, pp. 1–7, 2018.
- [55] P. K. Mandal and R. Mahto, "Deep cnn-lstm with word embeddings for news headline sarcasm detection," in *16th International Conference on Information Technology-New Generations (ITNG 2019)*. Springer, 2019, pp. 495–498.
- [56] D. Jain, A. Kumar, and G. Garg, "Sarcasm detection in mash-up language using soft-attention based bi-directional lstm and feature-rich cnn," *Applied Soft Computing*, vol. 91, p. 106198, 2020.
- [57] A. Kumar, V. T. Narapareddy, V. A. Srikanth, A. Malapati, and L. B. M. Neti, "Sarcasm detection using multi-head attention based bidirectional lstm," *IEEE Access*, vol. 8, pp. 6388–6397, 2020.

- [58] S. He, F. Guo, and S. Qin, "Sarcasm detection using graph convolutional networks with bidirectional lstm," in *Proceedings of the 2020 3rd International Conference on Big Data Technologies*, 2020, pp. 97–101.
- [59] A. Baruah, K. Das, F. Barbhuiya, and K. Dey, "Context-aware sarcasm detection using bert," in *Proceedings of the Second Workshop on Figurative Language Processing*, 2020, pp. 83–87.
- [60] H. Srivastava, V. Varshney, S. Kumari, and S. Srivastava, "A novel hierarchical bert architecture for sarcasm detection," in *Proceedings of the Second Workshop on Figurative Language Processing*, 2020, pp. 93–97.
- [61] A. Kumar, V. T. Narapareddy, P. Gupta, V. A. Srikanth, L. B. M. Neti, and A. Malapati, "Adversarial and auxiliary features-aware bert for sarcasm detection," in *8th ACM IKDD CODS and 26th COMAD*, 2021, pp. 163–170.
- [62] R. A. Potamias, G. Siolas, and A.-G. Stafylopatis, "A transformer-based approach to irony and sarcasm detection," *Neural Computing and Applications*, vol. 32, no. 23, pp. 17 309–17 320, 2020.
- [63] J. Karoui, F. B. Zitoune, and V. Moriceau, "Soukhria: Towards an irony detection system for arabic in social media," *Procedia Computer Science*, vol. 117, pp. 161–168, 2017.
- [64] B. Ghanem, J. Karoui, F. Benamara, V. Moriceau, and P. Rosso, "Idat at fire2019: Overview of the track on irony detection in arabic tweets," in *Proceedings of the 11th Forum for Information Retrieval Evaluation*, 2019, pp. 10–13.
- [65] M. Khalifa and N. Hussein, "Ensemble learning for irony detection in arabic tweets," in *FIRE (Working Notes)*, 2019, pp. 433–438.
- [66] H. A. Nayel, W. Medhat, and M. Rashad, "Benha@ idat: Improving irony detection in arabic tweets using ensemble approach," in *FIRE (Working Notes)*, 2019, pp. 401–408.
- [67] T. Ranasinghe, H. Saadany, A. Plum, S. Mandhari, E. Mohamed, C. Orasan, and R. Mitkov, "Rgcl at idat: deep learning models for irony detection in arabic language," 2019.
- [68] C. Zhang and M. Abdul-Mageed, "Multi-task bidirectional transformer representations for irony detection," in *Working Notes of FIRE 2019 - Forum for Information Retrieval Evaluation, Kolkata, India, December 12-15, 2019*, ser. CEUR Workshop Proceedings, P. Mehta, P. Rosso, P. Majumder, and M. Mitra, Eds., vol. 2517. CEUR-WS.org, 2019, pp. 391–400. [Online]. Available: <http://ceur-ws.org/Vol-2517/T4-2.pdf>
- [69] I. A. Farha and W. Magdy, "From arabic sentiment analysis to sarcasm detection: The arsarcasm dataset," in *Proceedings of the 4th Workshop on Open-Source Arabic Corpora and Processing Tools, with a Shared Task on Offensive Language Detection*, 2020, pp. 32–39.
- [70] J. Howard and S. Ruder, "Universal language model fine-tuning for text classification," pp. 328–339, 2018. [Online]. Available: <https://www.aclweb.org/anthology/P18-1031/>
- [71] K. Song, X. Tan, T. Qin, J. Lu, and T. Liu, "MASS: masked sequence to sequence pre-training for language generation," vol. 97, pp. 5926–5936, 2019. [Online]. Available: <http://proceedings.mlr.press/v97/song19d.html>
- [72] K. Clark, M. Luong, Q. V. Le, and C. D. Manning, "ELECTRA: pre-training text encoders as discriminators rather than generators," 2020. [Online]. Available: <https://openreview.net/forum?id=r1xMH1BtVB>
- [73] S. Ruder, I. Vulić, and A. Søgaard, "A survey of cross-lingual word embedding models," *Journal of Artificial Intelligence Research*, vol. 65, pp. 569–631, 2019.
- [74] O. Adams, A. Makarucha, G. Neubig, S. Bird, and T. Cohn, "Cross-lingual word embeddings for low-resource language modeling," in *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 1, Long Papers*, 2017, pp. 937–947.
- [75] D. Wang, N. Peng, and K. Duh, "A multi-task learning approach to adapting bilingual word embeddings for cross-lingual named entity recognition," in *Proceedings of the Eighth International Joint Conference on Natural Language Processing (Volume 2: Short Papers)*, 2017, pp. 383–388.
- [76] J. Xie, Z. Yang, G. Neubig, N. A. Smith, and J. G. Carbonell, "Neural cross-lingual named entity recognition with minimal resources," pp. 369–379, 2018. [Online]. Available: <https://doi.org/10.18653/v1/d18-1034>
- [77] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Advances in Neural Information Processing Systems*, Z. Ghahramani, M. Welling, C. Cortes, N. Lawrence, and K. Q. Weinberger, Eds., vol. 27. Curran Associates, Inc., 2014, pp. 2672–2680. [Online]. Available: <https://proceedings.neurips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf>
- [78] A. V. M. Barone, "Towards cross-lingual distributed representations without parallel text trained with adversarial autoencoders," pp. 121–126, 2016. [Online]. Available: <https://doi.org/10.18653/v1/W16-1614>
- [79] J.-K. Kim, Y.-B. Kim, R. Sarikaya, and E. Fosler-Lussier, "Cross-lingual transfer learning for pos tagging without cross-lingual resources," in *Proceedings of the 2017 conference on empirical methods in natural language processing*, 2017, pp. 2832–2838.
- [80] X. Chen, Y. Sun, B. Athiwaratkun, C. Cardie, and K. Weinberger, "Adversarial deep averaging networks for cross-lingual sentiment classification," *Transactions of the Association for Computational Linguistics*, vol. 6, pp. 557–570, 2018.
- [81] P. Keung, Y. Lu, and V. Bhardwaj, "Adversarial learning with contextual embeddings for zero-resource cross-lingual classification and NER," in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing, EMNLP-IJCNLP 2019, Hong Kong, China, November 3-7, 2019*, K. Inui, J. Jiang, V. Ng, and X. Wan, Eds. Association for Computational Linguistics, 2019, pp. 1355–1360. [Online]. Available: <https://doi.org/10.18653/v1/D19-1138>
- [82] A. Conneau and G. Lample, "Cross-lingual language model pretraining," pp. 7057–7067, 2019. [Online]. Available: <http://papers.nips.cc/paper/8928-cross-lingual-language-model-pretraining>
- [83] S. Wu and M. Dredze, "Beto, bentz, becas: The surprising cross-lingual effectiveness of BERT," in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing, EMNLP-IJCNLP 2019, Hong Kong, China, November 3-7, 2019*, K. Inui, J. Jiang, V. Ng, and X. Wan, Eds. Association for Computational Linguistics, 2019, pp. 833–844. [Online]. Available: <https://doi.org/10.18653/v1/D19-1077>
- [84] A. Blum and T. Mitchell, "Combining labeled and unlabeled data with co-training," in *Proceedings of the eleventh annual conference on Computational learning theory*, 1998, pp. 92–100.
- [85] M. Culp and G. Michailidis, "Graph-based semisupervised learning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 1, pp. 174–179, 2007.
- [86] Z.-H. Zhou and M. Li, "Tri-training: Exploiting unlabeled data using three classifiers," *IEEE Transactions on knowledge and Data Engineering*, vol. 17, no. 11, pp. 1529–1541, 2005.
- [87] K. Nigam and R. Ghani, "Analyzing the effectiveness and applicability of co-training," in *Proceedings of the ninth international conference on Information and knowledge management*, 2000, pp. 86–93.
- [88] Z. Kozareva, B. Bonev, and A. Montoyo, "Self-training and co-training applied to spanish named entity recognition," in *Mexican International conference on Artificial Intelligence*. Springer, 2005, pp. 770–779.
- [89] C. Helwe and S. Elbassuoni, "Arabic named entity recognition via deep co-learning," *Artificial Intelligence Review*, vol. 52, no. 1, pp. 197–215, 2019.
- [90] W. Wang, Z. Huang, and M. Harper, "Semi-supervised learning for part-of-speech tagging of mandarin transcribed speech," in *2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07*, vol. 4. IEEE, 2007, pp. IV–137.
- [91] K. Sagae, "Self-training without reranking for parser domain adaptation and its impact on semantic role labeling," in *Proceedings of the 2010 Workshop on Domain Adaptation for Natural Language Processing*, 2010, pp. 37–44.
- [92] R. Mihalcea, "Co-training and self-training for word sense disambiguation," in *Proceedings of the Eighth Conference on Computational Natural Language Learning (CoNLL-2004) at HLT-NAACL 2004*, 2004, pp. 33–40.
- [93] S. Kiritchenko and S. Matwin, "Email classification with co-training," in *Proceedings of the 2001 conference of the Centre for Advanced Studies on Collaborative research*. Citeseer, 2001, p. 8.

- [94] V. V. Asch and W. Daelemans, "Predicting the effectiveness of self-training: Application to sentiment classification," *CoRR*, vol. abs/1601.03288, 2016. [Online]. Available: <http://arxiv.org/abs/1601.03288>
- [95] M. S. Hajmohammadi, R. Ibrahim, A. Selamat, and H. Fujita, "Combination of active learning and self-training for cross-lingual sentiment classification with density analysis of unlabelled samples," *Information sciences*, vol. 317, pp. 67–77, 2015.
- [96] X. Pan, B. Zhang, J. May, J. Nothman, K. Knight, and H. Ji, "Cross-lingual name tagging and linking for 282 languages," in *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, 2017, pp. 1946–1958.
- [97] N. Garneau, M. Godbout, D. Beauchemin, A. Durand, and L. Lamontagne, "A robust self-learning method for fully unsupervised cross-lingual mappings of word embeddings: Making the method robustly reproducible as well," *CoRR*, vol. abs/1912.01706, 2019. [Online]. Available: <http://arxiv.org/abs/1912.01706>
- [98] X. L. Dong and G. de Melo, "A robust self-learning framework for cross-lingual text classification," in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, 2019, pp. 6307–6311.
- [99] X. Dong, Y. Zhu, Y. Zhang, Z. Fu, D. Xu, S. Yang, and G. de Melo, "Leveraging adversarial training in self-learning for cross-lingual text classification," in *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*, 2020, pp. 1541–1544.
- [100] D. Nadeau and S. Sekine, "A survey of named entity recognition and classification," *Lingvisticae Investigationes*, vol. 30, no. 1, pp. 3–26, 2007.
- [101] Y. Benajiba, P. Rosso, and J. M. Benedir, "Anersys: An arabic named entity recognition system based on maximum entropy," in *International Conference on Intelligent Text Processing and Computational Linguistics*, 2007, pp. 143–153.
- [102] A. Mitchell, S. Strassel, M. Przybocki, J. Davis, G. Doddington, R. Grishman, A. Meyers, A. Brunstain, L. Ferro, and B. Sundheim, "Tides extraction (ace) 2003 multilingual training data," *LDC2004T09*, Philadelphia, Penn.: Linguistic Data Consortium, 2003.
- [103] M. Maamouri, A. Bies, T. Buckwalter, and W. Mekki, "The penn arabic treebank: Building a large-scale annotated arabic corpus," in *NEMLAR conference on Arabic language resources and tools*, vol. 27. Cairo, 2004, pp. 466–467.
- [104] M. Maamouri, A. Bies, S. Kulick, M. Ciul, N. Habash, and R. Eskander, "Developing an egyptian arabic treebank: Impact of dialectal morphology on annotation and tool development," in *LREC*, 2014, pp. 2348–2354.
- [105] K. Dukes and N. Habash, "Morphological annotation of quranic arabic," in *Lrec*, 2010.
- [106] W. Antoun, F. Baly, and H. Hajj, "Arabert: Transformer-based model for arabic language understanding," *arXiv preprint arXiv:2003.00104*, 2020.
- [107] O. Obeid, N. Zalmout, S. Khalifa, D. Taji, M. Oudah, B. Alhafni, G. Inoue, F. Eryani, A. Erdmann, and N. Habash, "Camel tools: An open source python toolkit for arabic natural language processing," in *Proceedings of The 12th Language Resources and Evaluation Conference*, 2020, pp. 7022–7032.
- [108] Y. Kim, "Convolutional neural networks for sentence classification," in *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing, EMNLP 2014, October 25-29, 2014, Doha, Qatar, A meeting of SIGDAT, a Special Interest Group of the ACL*, A. Moschitti, B. Pang, and W. Daelemans, Eds. ACL, 2014, pp. 1746–1751. [Online]. Available: <https://doi.org/10.3115/v1/d14-1181>
- [109] O. Zaidan and C. Callison-Burch, "The arabic online commentary dataset: an annotated dataset of informal arabic with high dialectal content," in *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies*, 2011, pp. 37–41.
- [110] M. Elaraby and M. Abdul-Mageed, "Deep models for arabic dialect identification on benchmarked data," in *Proceedings of the Fifth Workshop on NLP for Similar Languages, Varieties and Dialects (VarDial 2018)*, 2018, pp. 263–274.

## APPENDIX

### A. POS Tag Set

### B. Error Analysis

The "regularizing" effect caused by self-training and discussed in section VIII can sometimes produce false negatives as shown in Table XI. We see a number of named entities that were misclassified by the self-trained model as unnamed ones. As an example, we take the last name الجزوري which was classified both correctly and incorrectly in different contexts by the self-trained model. Context of correct classification is "هاش تاج لجمال الجزوري", while it is "ماسك على الناس كلها سي دي الا الجزوري ماسك عليه فلوبي" for the incorrect classification. First, we note that الجزوري is not a common name (zero occurrences in the MSA training set). Second, we observe that in the correct case, the word was preceded by the first name جمال which was correctly classified as PER, making it easier for the model to assign PER to the word afterwards as a surname.

TABLE XIII: The POS Tag Set in [45]

Tag	Description	Tag	Description
ADV	adverb	ADJ	adjective
CONJ	conjunction	DET	determiner
NOUN	noun	NSUFF	noun suffix
NUM	number	PART	particle
PUNC	punctuation	PRON	pronoun
PREP	preposition	V	verb
ABBREV	abbreviation	VSUFF	verb suffix
FOREIGN	non-Arabic	FUT_PART	future particle
PROG_PART	progressive particle	EMOT	Emoticon/Emoji
MENTION	twitter mention	HASH	Hashtag
URL	URL	-	-

TABLE XIV: NER task. Bigger Sample False Positives Mitigated by Self-Training. These were Correctly Predicted as the Unnamed Entity “O” by the Self-Trained Model

no.	Token	Eng.	MSA	Context/Explanation	FT Pred.
(1)	نبي	we want	نريد	... نبي نعرف من... (we want to know who)	PER
(2)	ماكانوا	wasn't	لم يكونوا	... أغلب الي ماكانوا مصدقين (most of those who wasn't believing)	LOC
(3)	لوووول	LOL	ضحك	... لوووول (interjection)	PER
(4)	عشان	for	لكي	... تبي بطاريات عشان تلعب (she wants batteries to play)	LOC
(5)	دلوقتي	now	الآن	... اقنعوه ينزل دلوقتي (convince him to move now)	PER
(6)	ايش	what	ماذا	... ايش رأيك (what do you think?)	PER
(7)	قادر	capable	قادر	... وبقدرة قادر... (magically; idiomatic expression)	PER
(8)	المشين	shameful	المشين	... المشين طنطاوي (shameful Tantawy; Playful for General Tant.)	PER
(9)	ايديكوا	your hands	أيديكم	... ابوس ايديكوا اقنعوه... (I entreat you to convince him)	PER
(10)	اسالك	I ask you	أسألك	... ودي اسالك شنهبي (I ask you what)	ORG
(11)	مين	who	مين	... صوتك مع مين البدوي (who do you vote for, Badawi)	PER
(12)	فلوبي ديسك	floppy disk	قرص مرن	... ماسك عليه فلوبي ديسك (holds a floppy disk against him)	PER
(13)	لحباب	loved ones	الأحباء	... تعال علم يف لحاباب (come teach your loved ones)	LOC
(14)	ماي	water	ماء	... جبت لهم ماي (brought them water)	PER
(15)	ريتويت	retweet	إعادة تغريد	... لو قرفان دوس ريتويت (if depressed click retweet)	PER

TABLE XV: NER task. Sample Errors that are Not Fixed by Self-Training (Shared with the Mere Fine-Tuned Model)

no.	Token(s)	Context/Explanation	Gold	FT	ST
(1)	بالمبارك	... بالمبارك عاد احنا (We are still in Mubarak)	LOC	PER	O
(2)	محشش	... محشش دخل المحاضرة (a drunk entered the lecture)	O	PER	PER
(3)	بأمانة	... بأمانة ايه وفي (what is the evidence/sign and where?)	O	LOC	LOC
(4)	لمستشفى	... لمستشفى قصر الدوباره (to Qasr AlDobara Hospital)	LOC	O	O
(5)	كنتاكي	... عند كنتاكي (by Kentucky [restaurant])	LOC	O	O
(6)	داون تاون	... مشروع داون تاون بطنطا (a down town Tanta project)	LOC	O	O
(7)	يا بطل	... مبروك يا بطل (Congratulations, hero!)	O	PER	PER
(8)	الاخوان	... نختلف مع الاخوان (we disagree with the Muslim brotherhood)	ORG	O	O
(9)	قناة العربية	... شفت قناة العربية (watched Al Arabya Channel)	ORG	O	O
(10)	المجلس العسكري	... اللي عمله المجلس العسكري (what the military council did)	ORG	O	O

TABLE XVI: NER task. Sample False Negatives Produced by Self-Training

no.	Word	Gold	FT	ST
(1)	الاخوان	ORG	ORG	O
(2)	للبرادي	PER	PER	O
(3)	محمدي الحلال	PER	PER	O
(4)	فان ديزل	PER	PER	O
(5)	الختوري	PER	PER	O
(6)	زين يسون	PER	PER	O

TABLE XVII: **SRD task.** Sample Errors that were Fixed by Self-Training

no	Example	FT	ST
(1)	لن يفهما غير العباقرة كنت عامل بيه غساله	Non-Sarcastic	sarcastic
(2)	هذا وضعكم بدون ميسي يا تافهين يا عاهات	Non-sarcastic	sarcastic
(3)	حاميا حراميا	Non-sarcastic	sarcastic
(4)	ايز لكل رجل قبيله عايزها متقسمه حاصع عبيط رسمي نظمي	Non-sarcastic	sarcastic
(5)	للعلم ده مهرجان درجه اولي ما لو بالفلوس ما كانش حد غلب	Sarcastic	Non-sarcastic
(6)	الاستاذه ميريام فارس ليها اغاني حلوه فشح مش واخده حقها	Sarcastic	Non-sarcastic
(7)	يا تري بين هيلاري كلنتون ودونالد ترامب مين تختار	Sarcastic	Non-sarcastic
(8)	دعوه الست قصده هيلاري كلنتون مثلا	Sarcastic	Non-sarcastic

TABLE XVIII: **SRD task.** Sample Errors that Were not Fixed by Self-Training (Shared with the Mere Fine-Tuned Model)

no	Example	Prediction	Gold
(1)	عارفصوره وجدتها علي فيسبوك	sarcastic	non-sarcastic
(2)	فضيعه	sarcastic	non-sarcastic
(3)	بغنيلا وبدئلا وغير بحبك ما بنلا	sarcastic	Non-sarcastic
(4)	انت العالي اللي بقالي سنين بهواه	Sarcastic	Non-sarcastic
(5)	هه دنتم مسخره ياراقل هونو علي انفسكم يا مبن فرنسا	non-sarcastic	sarcastic
(6)	يعني حيكون زي اللورد دارث فيدرر هه	non-sarcastic	sarcastic
(7)	يا جماعه هذا بوكيمون ما حدا عرف يصطاده ويطعميه للجرذان	non-sarcastic	sarcastic
(8)	حضرتك مفيش فكه تاخذ بالباقي ريتويتس	non-sarcastic	sarcastic

# Distributed Mining of High Utility Sequential Patterns with Negative Item Values

Manoj Varma<sup>1</sup>, Saleti Sumalatha<sup>2</sup>, Akhileshwar reddy<sup>3</sup>  
School of Engineering and Sciences  
Computer Science and Engineering  
SRM University AP  
India

**Abstract**—The sequential pattern mining was widely used to solve various business problems, including frequent user click pattern, customer analysis of buying product, gene microarray data analysis, etc. Many studies were going on these pattern mining to extract insightful data. All the studies were mostly concentrated on high utility sequential pattern mining (HUSP) with positive values without a distributed approach. All the existing solutions are centralized which incurs greater computation and communication costs. In this paper, we introduce a novel algorithm for mining HUSPs including negative item values in support of a distributed approach. We use the Hadoop map reduce algorithms for processing the data in parallel. Various pruning techniques have been proposed to minimize the search space in a distributed environment, thus reducing the expense of processing. To our understanding, no algorithm was proposed to mine High Utility Sequential Patterns with negative item values in a distributed environment. So, we design a novel algorithm called DHUSP-N (Distributed High Utility Sequential Pattern mining with Negative values). DHUSP-N can mine high utility sequential patterns considering the negative item utilities from Bigdata.

**Keywords**—High utility sequential pattern mining; big data; utility mining; negative utility; distributed algorithms

## I. INTRODUCTION

These days we can't imagine the volume of data that is produced every day in the form of sequences [14] [15]. Mining high utility patterns is a prominent job in data mining that discovers the itemsets which appear frequently in sequences. Many current algorithms [5] [16] [24] only take into account the frequency of each object in a sequence and presume that the importance of items is the same for various items. In [6], the authors depicted such approaches are not sufficient for industry needs. In reality, these algorithms mined patterns are not especially related to business needs, so they don't really know the patterns are interesting for their business. For example, in a retail market analysis, each item possess its own profit value, and an item will exist in the purchasing record of a customer many times. Utility was introduced to mine frequent patterns to resolve this issue by considering the profit (quality) and quantity of products. This introduce a novel field of study, namely, high utility itemset mining and high utility sequential pattern mining (HUSP), these are able to mine insightful knowledge, given a minimum utility defined by the user instead of minimum support. Utility model-based knowledge can supply more useful and applicable decision-making information than those based on a conventional support framework. High utility sequential pattern (HUSP) mining [2] [23] is used to extract profitable and more beneficial sequential

patterns from databases. It considers a business intention such as profit, user interests, value, etc. A sequence mined from a sequence database is said to be a high utility sequential pattern only if it is having an utility not less than the minimum utility threshold supplied by the user. So, we came up with a new method for mining sequential patterns with high utility that includes negative item values using a distributed approach. Here we use algorithms like Hadoop map reduce [9] to operate data quickly in parallel. We suggest few pruning strategies to eliminate unpromising items that leads to minimize the search space in distributed circumstances.

The following are the contributions of the current work:

1. We made a complete overhaul to HUSP-NIV [21] algorithm and studied the distributed solution to the problem of HUSP-N [22] mining.
2. MapReduce algorithm is proposed for extracting HUSPs with negative item values.
3. Proposed a distributed utility upper bound that supports global mining of HUSP-N's.
4. Several experimental evaluations have been accomplished on the real as well as synthetic datasets to assess the efficiency of DHUSP-N algorithm.

The remaining sections in the paper are composed as follows: Description of related work is mentioned in Section II. Section III provides a detailed description of problem definition. The details of DHUSP-N are given in Section IV. The performance details of DHUSP-N obtained from the experimental results are noted in Section V. The enhancements of the current work and its conclusion is given in Section VI.

## II. RELATED WORK

Sequential pattern mining became a buzzword and many algorithms [1] [4] [7] [8] [17] have been proposed. Sequential pattern mining is an extension to frequent itemset mining based on support framework that was firstly introduced by Srikant and Agrawal [1] in their studies. He gave a new definition by adding different time constraints and other attributes like sliding time window, user-defined taxonomy, and introduced a generalised sequential pattern (GSP) algorithm. Wang et al. [20] proposed novel pruning strategies namely, RSU and PEU to remove the sequences with less utility and designed HUS-Span algorithm to efficiently extract HUSPs. Truong-Chi & Fournier-Viger [8] has described about high utility

TABLE I. SAMPLE DATASET

$S_i d$	$Q - sequence$
1	$\langle\langle(I_5, 2)[(I_1, 4)(I_2, 2)](I_4, 4)\rangle\rangle$
2	$\langle\langle[(I_1, 3)(I_2, 1)][(I_1, 1), (I_3, 1), (I_4, 3)][(I_1, 2), (I_4, 3)(I_5, 3)]\rangle\rangle$
3	$\langle\langle[(I_3, 4)(I_6, 6)][(I_2, 3)(I_4, 3)]\rangle\rangle$
4	$\langle\langle[(I_2, 1)(I_3, 6)][(I_1, 3)(I_4, 3)][(I_1, 4)(I_2, 1)(I_3, 2)]\rangle\rangle$
5	$\langle\langle[(I_2, 2)(I_5, 3)][(I_1, 3)(I_6, 2)][(I_1, 2)(I_2, 1)]\rangle\rangle$

sequence mining. Many other pattern mining problems were generalized by the authors, such as frequent itemset mining in transaction databases, sequential pattern mining in sequence databases, and high utility itemsets in databases of quantitative transactions. The sequential order between the items and their utility has been considered to mine high utility sequences from a quantitative sequence database. Guha et al. [11] used the regular expressions as a constraint for user-controlled focus on mining sequential patterns. Some more algorithms like USpan [23], HUS-Span [20] and HuspExt [3] algorithms have been designed to extract high utility patterns based on utility concept but they are not designed to use negative patterns. Negative sequential patterns (such as missing medical check-ups) are crucial and more useful than positive sequential patterns (e.g. visiting a medical check-up) in many intellectual systems and applications such as healthcare analysis and risk management. However, exploring sequential patterns with negative item values is considerably more complex than sequential pattern mining including positive item values because of acute time complexity occurred by non-repeating elements, high time complexity and large search space in finding negative sequential patterns. Xu et al. [21] came up with HUNSPM. This algorithm considers the items that do not occur into attention. These are the first studies to mine HUNSPM (high utility negative sequential pattern mining). These algorithms can mine HUSPs efficiently from a non-decentralized database using a single machine, however, they cannot handle big data [12]. Also, their proposed pruning techniques cannot be applied in a distributed environment. Mining patterns from big data on a single machine is very costly to execute the mining algorithms. Developing a distributed algorithm that mines HUNSPs is a key to handle the problem. Recently, Lin et al. [13] introduced an algorithm for high utility itemset mining which is applicable for handling big data. The approach proposed in [13] do not consider the sequential ordering of itemsets. Adding the sequential order of itemsets makes it more challenging to mine. Recently, we proposed a distributed MapRedcue algorithm that can mine high utility time interval sequential patterns [19]. However, we do not include the negative item values. This motivates us to study a novel approach of mining HUSP that includes negative item values from a distributed environment.

No approach has been introduced till now for high utility sequential pattern mining that can consider both the utilities and negative values in a distributed environment, to the best of our understanding. So, we design a novel algorithm called DHUSP-N that can extract all sequential patterns with high utility and negative item values that appear in bigdata.

### III. PROBLEM DEFINITION

Given a sequential database  $D$ , the problem of mining sequential patterns of high utility with negative item values

TABLE II. QUALITY TABLE

Item	$I_1$	$I_2$	$I_3$	$I_4$	$I_5$	$I_6$
Quality	5	-3	1	2	4	1

from large databases in a distributed way is described here. Let a set of distinct items be  $I = \{i_1, i_2, i_3, i_4, \dots, i_n\}$ . A positive or negative number  $p(i_k)$ , called its external utility is associated with each item  $i_k$ . The quantity or internal utility of  $I$  is called a q-item  $(i, q)$ , where  $i \in I$  and  $q$  denotes the purchased amount of  $i$ . Our problem is to mine all high utility sequential patterns with negative item values (DHUSP-N) in a distributed environment with a minimum utility threshold  $\delta$ .

Example: Consider a Q-sequence database as in Table I. Each entry in the Q-sequence database is said to be a q-sequence. The q-sequence  $S_1$  depicts the items  $I_5, I_1, I_2$  and  $I_4$  with internal utility of 2, 4, 2 and 4. Table II gives us the external utilities of these items respectively 4, 5, -3 and 2. So the item  $I_2$  is sold at loss.  $[(I_1, 4)(I_2, 2)]$  is the itemset with two q-items.

Definition 1: Sequence  $\alpha = k_1, k_2, \dots, k_i$  is a sub-sequence of sequence  $\beta = k_1, k_2, \dots, k_j (i \leq j)$  or the other way  $\beta$  is a super-sequence of  $\alpha$ .

Definition 2: Every element in the itemset consists of positive number  $p(I)$ , called the external utility (e.g. price/profit per unit). Every item  $I$  in itemset  $X_d$  of particular sequence  $S_r$  (i.e.,  $S_r^d$ ) has a positive number  $q(I, S_r^d)$ , called as its internal utility (e.g., quantity) of  $I$  in itemset of particular sequence.

Definition 3: The utility of a q-item is defined as the product of internal utility and external utility. The utility of a q-itemset is defined as the sum of each item utility in the q-itemset. The q-sequence utility is defined as the sum of each item utility having positive external utility. For example, utility of  $(I_1, 4)$  in itemset 2 of sequence  $S_1$  is  $4 \times 5 = 20$ . The utility of itemset  $[(I_1, 4)(I_2, 2)]$  is  $S_1$  is  $4 \times 5 + 2 \times -3 = 20 - 6 = 14$ . The q-sequence utility of  $S_1 = \langle\langle(I_5, 2)[(I_1, 4)(I_2, 2)](I_4, 4)\rangle\rangle$  is  $2 \times 4 + 4 \times 5 + 2 \times 4 = 8 + 20 + 8 = 36$ .

Definition 4: The sequence local utility in partitioned database  $D_i$  is defined as  $su_L(\alpha, D_i) = \sum_{S_r \in D_i} su(\alpha, S_r)$  for sequence  $\alpha$  in the partition  $D_i$ . The sum of local utilities of  $\alpha$  in each partition  $D_i$  is defined as its global utility and denoted as  $su_G$ .

Definition 5: The total utility of a partition  $D_i$  is denoted as  $U_{D_i}$  and is defined as sum of sequence utility of each  $S_i$ , where  $S_i$  is an input sequence in  $D_i$ . The total utility of sequence database  $D$  is denoted as  $U_D$  and is defined as the sum of total utility of each  $D_i$ .

Definition 6: Given a sequence  $\alpha$ , it is called a local high utility sequential pattern with negative value (L-HUSP-N), iff  $su_L(\alpha, D_i) \geq \delta \cdot U_{D_i}$ , where  $\delta$  is the minimum utility threshold.

Definition 7: Given a sequence  $\alpha$ , it is called a global high utility sequential pattern with negative value (G-HUSP-N), iff  $su_G(\alpha, D) \geq \delta \cdot U_D$ , where  $\delta$  is the minimum utility threshold.

Definition 8: Given a sequence dataset  $D$  and a minimum utility threshold  $\delta$ , then the sequence  $\alpha$  is said to be a high

TABLE III. UTILITY MATRIX FOR SEQUENCE  $S_1$

Item	q-itemset1	q-itemset2	q-itemset3
a	(0,36)	(20,8)	(0,8)
b	(0,36)	(-6,8)	(0,8)
d	(0,36)	(0,8)	(8,0)
e	(2,28)	(0,8)	(0,8)

GSWU sequence if and only if  $GSWU(\alpha, D) \geq \delta \cdot UD$ .

Definition 9: Mining of HUSP with/without Negative Item Values - Selecting the highest utility from the utility estimations of every q-sequence and add them together to address the sequence's utility in a given sequence database. The max utility is used to denote the utility of a sequence  $t$  and it is characterized as  $u_{max}(t) = \sum_{s \in S} \max\{u(t, s)\}$ .

HUSP mining is to mine all the HUSPs from the database where each item possess only positive external utilities, whereas HUSP-N mining is to mine all the HUSPs from the database where each item in the database may have either positive or negative external utilities. The sequence  $t$  is called as HUSP in Q-sequence Database  $S$  if and only if  $u_{max}(t) \geq \delta$ . The properties defined for HUSP-N mining are as follows [21]:

Property 1: HUSP can have items with negative external utilities.

Property 2: No less than one item having a positive external utility must be included in a high utility sequential pattern.

Definition 10: Sequence-weighted Utilization (SWU) of a particular sequence  $t$  in q-sequence database  $S$  is defined as sum of q-sequence utilities where  $t$  is a subsequence to q-sequence.

Definition 11: Given a bunch of sequences  $D_i$ , the Local Sequence-Weighted Utility (LSWU) of a sequence  $\alpha$  in  $D_i$ , indicated as  $LSWU(\alpha, D_i)$ , is characterized as the amount of the utilities of sequences containing  $\alpha$  in  $D_i$ , where  $\alpha \leq S$  implies  $\alpha$  is a subsequence of  $S$ . In like manner, the Global Sequence-Weighted Utility (GSWU) of a sequence  $\alpha$  in information base  $D$  is characterized as:  $GSWU(\alpha, D) = \sum_{(D_i \subset D)} LSWU(\alpha, D_i)$ .

Property 3: Sequence-weighted Downward Closure Property- Given the S database of q-sequences, and two  $t_1$  and  $t_2$  sequences, where  $t_2$  contains  $t_1$ , then  $t_2$  contains  $t_1$ , then  $SWU(t_2) \leq SWU(t_1)$ .

Definition 12: Utility matrix (UM)- It is a data structure introduced in USpan [23] algorithm to store the q-sequence utility. Each element in the matrix stores two values, the first one is item's utility, where as the second is item's remaining utility.

Definition 13: The remaining utility in the Utility Matrix is only the sum of all remaining q-sequence items' positive external utility values.

From Definitions 12 and 13, the utility matrix created for sequence  $S_1$  in our sample database is shown in Table III.

Definition 14: Given a sequence pattern  $\alpha$ , an I-concatenate pattern  $\beta$  is a sequence obtained by including an item  $I$  to the last itemset  $\alpha$ .

Definition 15: Given a sequence  $\alpha$ , S-concatenate pattern  $\beta$  denotes a sequence obtained by including a 1-Itemset  $\{I\}$  after the last itemset of  $\alpha$ .

#### IV. METHODOLOGY

Mining HUSP with negative values in the big data era is a hectic job to do due to the hurdles of data growth in an exponential way. It is expensive to mine patterns in a single individual machine. Designing a distributed and parallel algorithm is the one solution that we are thinking of. To implement this approach, we need to address a few key issues like decreasing the search space in the data, decreasing the communication overhead between different local machines, and finally the scalability issues to be answered.

We propose an algorithm namely DHUSP-N (Distributed High utility sequential pattern mining with negative values). This algorithm mines high utility patterns in a distributed approach. Fig. 1 demonstrates the phases of the methodology. In the initialization phase, the sequence database is divided into many partitions. Each partition is given to a mapper which in turn gives a utility matrix [21]. The data structure UM [21] is used in later stages to retrieve utility values. This stage also identifies the items which do not form HUSP, which are pruned by DHUSP-N in the later stage.

1. Initialization phase: This comprises of two stages, namely, map and reduce.

Map stage: In each partition, utility matrix (UM) is constructed by the mapper for every input sequence in the given partition of database. Here UM refers to a data structure which contains utility values and the leftover utility of rest of items. This data structure is used to determine the LHUSP-N from each partitioned node. With this representation of utility matrix the mining takes place even faster. These are stored in Resilient Distributed Dataset (RDD). All elements in the database may not form high utility patterns. We use local sequence weighted utility (LSWU) and global sequence weighted utility (GSWU) to find the unpromising items which may not form good patterns. The pruned items are based on LSWU and GSWU values. The results are stored in a resilient distributed dataset.

Reduce Stage: Each reducer receive the output of the same key. So, basically, by adding all the LSWU values of the similar items, the reducer calculates the GSWU values of each item. The reducers emit the items for which the calculated GSWU values are less than the user supplied minimum utility threshold. These are referred as unpromising items. These are also stored and maintained in resilient distributed dataset which is used to update UM's in next phase.

2. Local HUSP-N mining: In this stage, the search space is reduced by pruning all the unnecessary items from each partition. Since it is hard to find global search space initially, we will find local HUSP-N from each partition then we will find DHUSP-N using this stage. Two map transformation stages play a key role in mining local HUSP-N. Map transformation 1 is used to prune unpromising items and map transformation 2 is used to find potential global HUSP. Rather than finding all the patterns in the partition with non-zero utility, we discover HUSPs locally. Pruning of low utility sequential patterns from the sequential patterns will not result in any loss of global

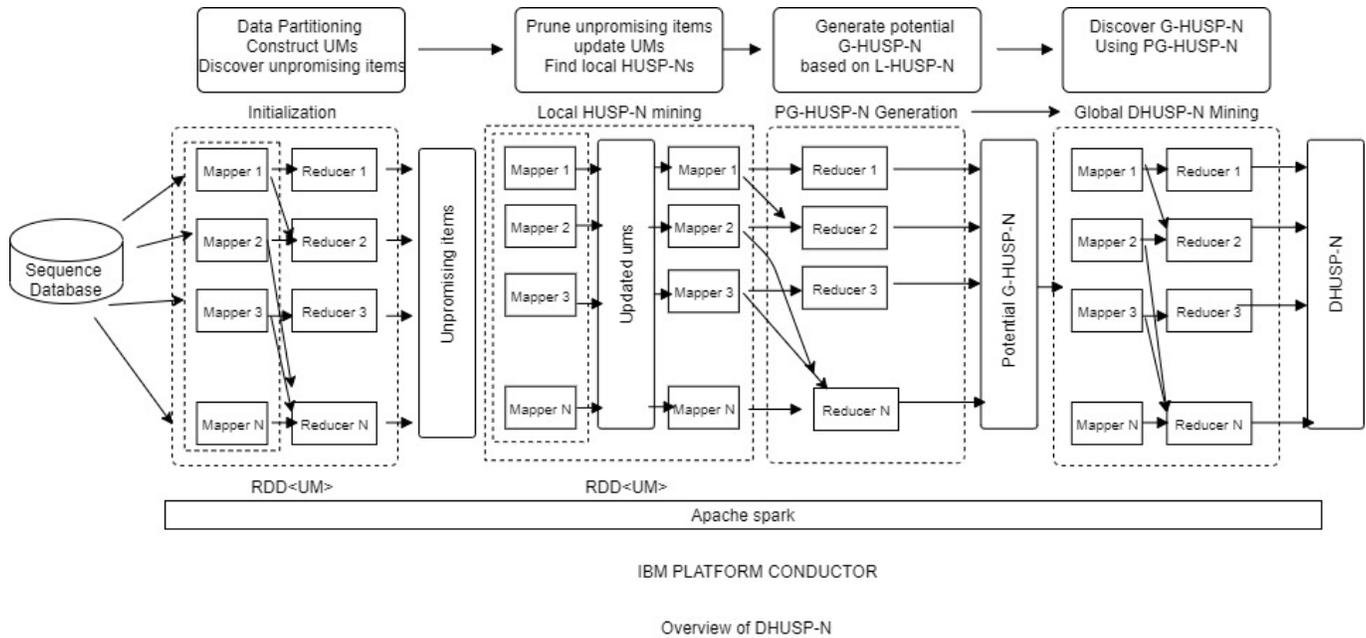


Fig. 1. Workflow of DHUSP-N.

HUSP. Thus, there is no loss of GHUSP while L-HUSP-N mining.

**Map Transformation 1:** In this map transformation the original UM's which is obtained from the previous stage results us the unpromising items. All the unpromising items in each utility matrix is pruned by mappers. The mappers output the updated utility matrix which will be stored in resilient distributed dataset.

**Map Transformation 2:** From the given input we have minimum utility threshold  $\delta$ , partition  $D_i$ , updated Utility matrix and total utility, DHUSP-N applies HUSP-NIV [21] algorithm to find the local High Utility Sequential patterns with negative item values whose utility is greater than minimum utility threshold. Each mapper outputs the LHUSP's  $\langle Patt, \langle D_i, utility \rangle \rangle$ , where  $D_i$  is the id of partitioned database and utility is the utility of pattern patt in  $D_i$ . These are stored in resilient distributed dataset.

**3. Discovering potential globally distributed HUSP-N:** To find the potential global patterns, global utility of each local HUSP obtained from the L-HUSP-N phase needs to be determined. As the number of local High utility patterns are very large, we only consider potentially global patterns and prune all local HUSP's which are not PG-HUSP-N's. In this stage for whose maximum utility values is less than a certain threshold will be pruned resulting in potential GHUSP-N. Since maximum utility represents the upper bound of utility of pattern, for those patterns where the utility value is less than the threshold limit will be pruned. Continuously pruning with a threshold of maximum utility will not miss any high utility patterns.

**Reduce stage:** Every L-HUSP-N with same key is collected into same reducer. The reducers in this stage return PG-HUSP-N's whose utility exceeds the user supplied minimum utility threshold.

**4. DHUSP-N Mining:** The DHUSP-N mining process finds each patterns global utility in the given set. Given the set of PG-HUSP-N, it discovers GHUSP-N's. The reducer finds the sum of each patterns utility in the set after all possible GHUSP-N's are read. All patterns with a total utility greater than the threshold defined are returned as GHUSP-N's.

**Map Stage:** Given PG-HUSP-N's, each mapper finds the local utility of the patterns as follows: If certain pattern among PG-HUSP-N is local high utility sequential pattern in the given partition  $D_i$ , as we already obtained utility from the previous phase, the mapper outputs  $\langle \alpha, \langle D_i, utility \rangle \rangle$ . The mapper otherwise calculates the utility of  $\alpha$ . To find  $\alpha$ 's utility in a partition, we build a pattern-growth approach that passes through the reduced search space. It undergoes both I-concatenate sequence and S-concatenate sequence.

**Reduce stage:** From the given set of PG-HUSP-N's, utility values are directed to the same reducer which has the same key. The reducer's input is a pattern, an utility in which the utility is the local utility resulting from map stage. Later, after reading each PG-HUSP-N, each pattern utility is added by the reducer. Finally, the patterns whose total utility exceeds the threshold are returned as Global DHUSP-N.

## V. EXPERIMENTAL RESULTS

To assess the efficiency of DHUSP-N, experiments have been run on two synthetic datasets and three real-world datasets. As this is the first of this kind there is no suitable algorithm to compare with DHUSP-N. The generic algorithm such as USPAN [23] is not appropriate to compare with DHUSP-N because it does not use negative values and it is a centralized approach. Even we cannot compare it with BIGHUSP [25] as it does not consider the negative values. Hence these algorithms are not suitable to compare with respect to run time or any other parameters.

TABLE IV. REAL DATASETS

Dataset	Sequence count	Item count	Average sequence length
Kosarak	990002	41270	8.099
BMSWebview2	77512	3340	4.62
MSNBC	989818	17	5.7

TABLE V. SYNTHETIC DATASET PARAMETERS

Parameter Name	Description
C	Average number of itemsets in each sequence
T	Average number of items in each itemset
D	Number of sequences (in millions)
N	Total number of items

TABLE VI. SYNTHETIC DATASETS

Dataset	C	T	D	N
C10T2.5D5N1000	10	2.5	5	1000
C15T3D10N10000	15	3	10	10000

The Distributed environment is equipped with 1 master node and 6 worker nodes. All the nodes are designated with Intel Xeon 2.6 GHz and 128Gb of RAM and the spark 3.0.0 is employed on the IBM platform conductor. A distributed platform is required for implementation. For this, we use apache spark distributed framework. This runs in a variety of platforms like the IBM platform for Spark [10], Hadoop, and Mesos clusters. We choose IBM Platform Conductor as it permits organizations to execute multiple instances of spark frameworks at the same time on a single infrastructure. It results in best usage of resources along with its efficient resource planning.

In DHUSP-N, we used the following parameters as performance measure: a) Run time: total time to mine DHUSP-N from the data set b) Number of candidates generated with varying utility c) scalability

A. Datasets

For this experiment, we used two synthetic datasets generated by IBM data generator and three real-time data sets, namely, Kosarak, BMSWebView2 and MSNBC. The real datasets are acquired from SPMF data mining libray.<sup>1</sup> The parameters of real datasets are given in Table IV. Table V depicts the parameters of synthetic data and the datasets are given in Table VI.

B. Effect of Minimum Utility

The performance of DHUSP-N is tested on real as well as synthetic datasets. Each experiment is conducted for distinct values of minimum utility threshold and the outcomes are reported in Fig. 2 and Fig. 3. Fig. 2 depicts the results on real datasets, whereas Fig. 3 describes the results on synthetic datasets. From the figures, it is clear that the execution time required for the completion of DHUSP-N is high at low values of minimum utility and tends to fall off with a rise in minimum utility. On Kosarak dataset, the execution time is

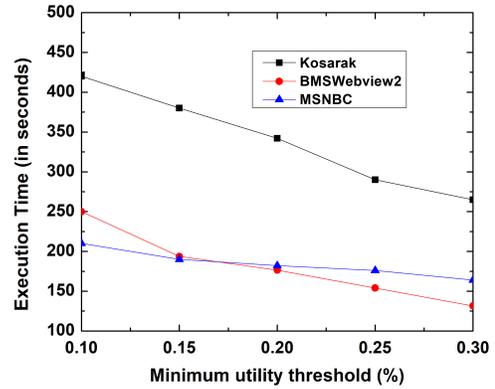


Fig. 2. Run Time Performance of DHUSP-N on Real Datasets.

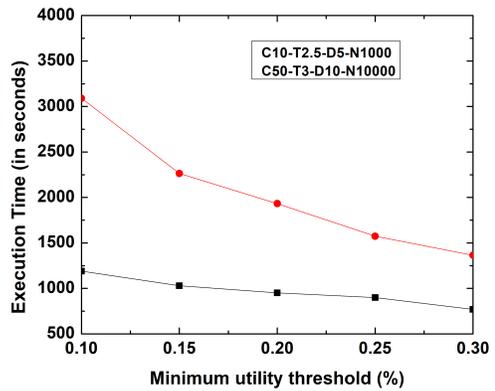


Fig. 3. Run Time Performance of DHUSP-N on Synthetic Datasets.

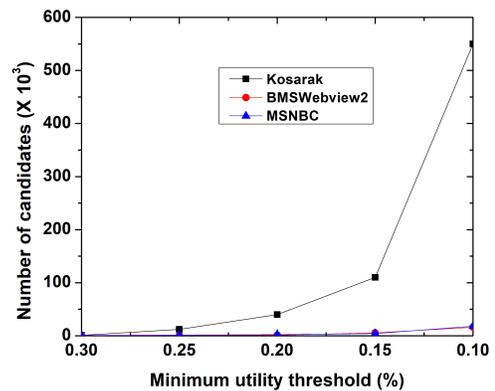


Fig. 4. Number of Candidates Generated on Real Datasets.

420 seconds for 0.1% threshold and it is 265 seconds for 0.3% threshold. Similarly on BMSWebview2 dataset, the execution time is 250 seconds for 0.1% threshold and it is 131 seconds for 0.3% thresholds, and it is 210 seconds and 164 seconds for 0.1% and 0.3% utility respectively on MSNBC dataset.

<sup>1</sup><https://www.philippe-fournier-viger.com/spmf/>

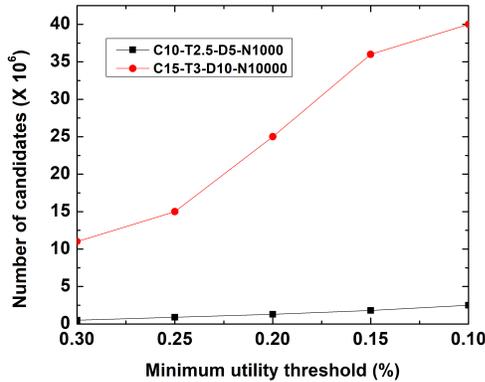


Fig. 5. Number of Candidates Generated on Synthetic Datasets.

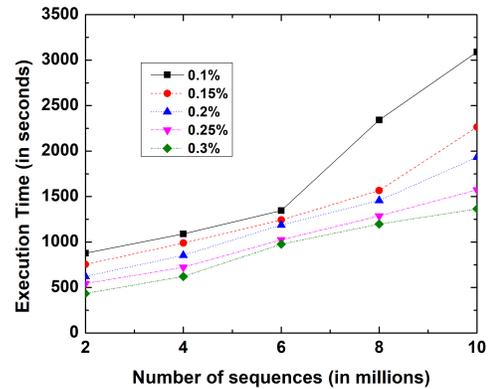


Fig. 7. Scalability Test on C15T3D10N10000.

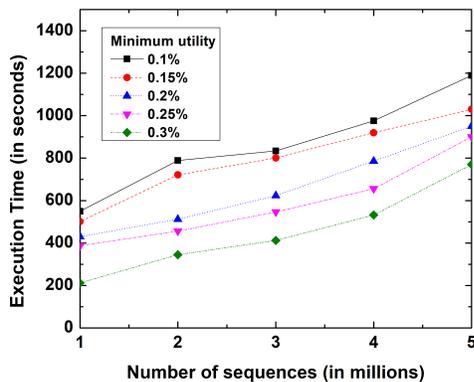


Fig. 6. Scalability Test on C10T2.5D5N1000.

To know the performance on large datasets, we conducted the experiment on two synthetic datasets having 5 million and 10 million sequences respectively. The former dataset require 1190 seconds for completion, whereas later dataset completed its execution in 3090 seconds. This is for 0.1% threshold and the execution times for the remaining thresholds are shown in Fig. 3. The number of candidates generated is also reported in Fig. 4 and Fig. 5. It is clearly noticed in Fig.5 that the candidates generated is high for larger dataset i.e. C15T3D10N10000. The reason is due to the increase in the sequence count from 5 to 10 and increase in the itemsets count per sequence from 10 to 15. Moreover, the difference in the execution time is high for lower values of minimum utility compared to higher values of minimum utility.

### C. Scalability

To assess the scalability of DHUSP-N, we conducted the experiments on both the synthetic datasets. In case of C10T2.5D5N1000 dataset, initially we considered the first 1 million sequences and noted the execution time of the algorithm. Later, the database is scaled by 1 million sequences and repeated until 5 million sequences. Similarly, for C15T3D10N10000 dataset, the process is repeated from

2 to 10 million sequences in steps of 2 million sequences. The experiment is conducted for varying minimum utility. The results reported in Fig. 6 and Fig. 7 depicts the scalability of DHUSP-N. It is observed that the time for execution increase with the increase in the sequence count. The processing time increased significantly after 6 million sequences for 0.1% utility as shown in Fig. 7.

## VI. CONCLUSION

This paper introduced a novel algorithm called DHUSP-N for mining high utility sequential patterns with negative values in a distributed environment. To our understanding, no methods were introduced in the utility mining literature to mine high utility sequential patterns with negative values in distributed environment. The performance of DHUSP-N is assessed on real as well as synthetic datasets. As this is the initial step of distributed approach to HUSP-N mining problem, there is a lot for the improvement as future work. More efficient data structures and techniques for pruning can be studied in the future. The current problem can be further extended to incremental mining of high utility negative sequential patterns [18]. Also, time intervals can be included in addition to the order of items purchased which leads to time interval high utility sequential pattern mining [19] with negative values.

## ACKNOWLEDGMENT

The authors would like to thank the parent institute for the enormous support.

## REFERENCES

- [1] Agrawal.R and Srikant.R, Mining sequential patterns, Mining Sequential Patterns. In: Proceedings of the Eleventh international conference on data engineering, 1995, pp. 3–14.
- [2] Ahmed.C.F, Tanbeer.S.K, and Jeong.B, A novel approach for mining high-utility sequential patterns in sequence databases, ETRI Journal, vol. 32, 2010, pp. 676–686.
- [3] Alkan.O.K and Karagoz.P, CRoM and HuspExt: Improving Efficiency of High Utility Sequential Pattern Extraction, IEEE Transactions on Knowledge and Data Engineering, vol. 27 (10), 2015, pp. 2645-2657.
- [4] Aloysius, G. and Binu, D. An approach to products placement in supermarkets using PrefixSpan algorithm. Journal of King Saud University - Computer and Information Sciences, vol. 25 (1), 2013, pp.77-87.

- [5] Ayres J., Flannick J., Gehrke J., and T. Yiu, Sequential pattern mining using a bitmap representation, In Proceedings of Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2002, pp. 429–435.
- [6] Cao Y., Zhao H., Zhang D., Luo C. Zhang, and E. Park, Flexible frameworks for actionable knowledge discovery, IEEE Transactions on Knowledge and Data Engineering, vol. 22 (9), 2010, pp. 1299–1312.
- [7] Chen Jinlin, An UpDown Directed Acyclic Graph Approach for Sequential Pattern Mining. IEEE Transactions on Knowledge and Data Engineering, vol. 22 (7), 2010, 913–928.
- [8] Chi-Truong, T. and Fournier-Viger, P. A Survey of High Utility Sequential Pattern Mining. Lecture Notes in Computer Science, 2019, 97–129.
- [9] Dean J., and Ghemawat S. MapReduce: simplified data processing on large clusters. ACM Communications, vol. 51(1), 2008, pp. 107–113.
- [10] Fu J., Sun J., and Wang K., SPARK – A Big Data Processing Platform for Machine Learning, In 2016 International Conference on Industrial Informatics - Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII), Wuhan, 2016, pp. 48-51.
- [11] Guha, S., Rastogi, R. and Shim, K. Rock: A robust clustering algorithm for categorical attributes. Information Systems, vol. 25 (5), 2000, pp. 345–366.
- [12] Kitchin R., Big Data. John Wiley and Sons, Ltd, 2016. [Online]. Available: <http://dx.doi.org/10.1002/9781118786352.wbieg0145>.
- [13] Lin Y. C., Wu, C.-W. and Tseng, V. S. Mining High Utility Itemsets in Big Data. Lecture Notes in Computer Science, 2015, pp. 649–661.
- [14] Mabroukeh N.R., and Ezeife.C.I, A taxonomy of sequential pattern mining algorithms, ACM Computing Surveys, vol. 43 (1), 2010, pp. 3:1–3:41.
- [15] Mooney C.H., and Roddick J.F., Sequential pattern mining approaches and algorithms, ACM Computing Surveys, vol. 45 (2), 2013, pp. 19:1–19:39.
- [16] Pei J., Han J.W., Mortazavi-Asl B., and Pinto H., PrefixSpan: Mining sequential patterns efficiently by prefix-projected pattern growth, In Proceedings of International Conference on Data Engineering, 2001, pp. 215–224.
- [17] Saleti S., and Subramanyam R.B.V. A novel mapreduce algorithm for distributed mining of sequential patterns using co-occurrence information. Applied Intelligence, vol. 49, 2019, pp. 150–171.
- [18] Saleti S., and Subramanyam R.B.V. A MapReduce solution for incremental mining of sequential patterns from big data. Expert systems with applications, vol. 133, 2019, pp.109-125.
- [19] Saleti S., and Subramanyam R.B.V. Distributed mining of high utility time interval sequential patterns using mapreduce approach. Expert systems with applications, vol. 141, 2020.
- [20] Wang J.Z., Yang Z.H., and Huang J.L., An efficient algorithm for high utility sequential pattern mining, Frontier and Innovation in Future Computing and Communications, Lecture Notes in Electrical Engineering, vol. 301(2014).
- [21] Xu T., Dong X., Xu J., and Dong X. Mining High Utility Sequential Patterns with Negative Item Values. International Journal of Pattern Recognition and Artificial Intelligence, vol. 31 (10), 2017, 1750035.
- [22] Xu T., Li T., and Dong X. Efficient High Utility Negative Sequential Patterns Mining in Smart Campus. IEEE Access, vol. 6, 2018, 23839–23847.
- [23] Yin J., Zheng Z., and Cao L., Uspan: An efficient algorithm for mining high utility sequential patterns, In Proceedings of ACM SIGKDD, 2012, pp. 660–668.
- [24] Zaki M.J., SPADE: An efficient algorithm for mining frequent sequences, Machine Learning, vol. 42 (1), 2001, pp. 31–60.
- [25] Zihayat M., Hut Z. Z., An, A., and Hut, Y. Distributed and parallel high utility sequential pattern mining. In 2016 IEEE International Conference on Big Data, 2016, pp. 853-862.

# Deep Neural Network-based Relationship Identification Framework to Discriminate Fake Profile Over Social Media

Suneet Joshi<sup>1</sup>, Deepak Singh Tomar<sup>2</sup>  
Department of Computer Science  
Maulana Azad National Institute of Technology  
Bhopal, India

**Abstract**—Involvement of social media like personal, business and political propaganda activities, attracts anti-social activities and has also increased. Anti-social elements get a wider platform to spread negativity after hiding their identity behind fake and false profiles. In this paper, an analytical and methodological user identification framework is developed to significantly binds implicit and explicit link relationship over the end-users graphical perspective. Identify malicious user, its communal information and sockpuppet node. Apart from that, this work provides the concept of the deep neural network approach over the graphical and linguistic perspective of end-user to classify as malicious, fake and genuine. This concept also helps identify the trade-off between the similarity of nodes attributes and the density of connections to classifying identical profile as sockpuppet over social media.

**Keywords**—Social media; anomaly detection; malicious activity; spam account; fake account; sockpuppet; deep neural network

## I. INTRODUCTION

Social media has entered our lives in many areas, among 7.5 billion people globally; 3.1 billion are active on social media. Many activities, such as communication, entertainment, political campaigning, and shopping, are carried out on social media platforms [1]. As a result of this, huge data generated spontaneously on social media platforms continuously emerge. The spread and popularity of social media have attracted the attention of antisocial elements. These people, unfortunately, use social media to scam or cyberbullying activity through a fake account.

Ungenuine user-profiles opened by users for mischievous purposes in social networks such as Facebook, Twitter and LinkedIn are called fake accounts. Fake accounts are usually opened for lack of trust, fear or hiding from anyone, protecting oneself from the potential loss of important news and accessing information by hiding. Apart from this, fake accounts are also opened in celebrities' names to gather followers, run ad campaigns, run negative campaigns about a brand, or get personal information and profile information of users. The credibility and global expansion of social media can infer that fake accounts opened using individuals or companies' names can pose a major problem.

Domenico et al. [2] state that false profiles on social networks are those that do not comply with the terms and conditions established by the platform, they do not belong to real people, they do not belong to the person they indicate,

and they pretend to be real profiles existing. They also indicate fake, manual or artisan profiles (created by people) and those generated and manipulated manually and automatically (bots or robots). They mention that there are different types of "tasks" of a fake profile: stalker, cyberbullying, gamers, spammers, pornography, digital reputation, media manipulation, cybercrime.

There are different categories of fake profiles, generated for different purposes. Some of them (gamers or stalkers) may be harmless. Still, others have a clear intention of causing damage or seeking financial gain for themselves, insults, extortion, threats, scams and worst Cases, corruption and grooming of minors.

Recently, researchers applying classification approach to detect fake account over social media. But due to a lack of graphical and linguistic implicit information [3], [4] for end node, the performance of this research does not get significant results. On the other hand, linguistic pattern and geocommunal information of end-user are crucial characteristics to identify the pattern of the end-user.

However, graphical communal characteristics depend upon the implicit and explicit link relationship. The explicit link relationship easily extracted from the graphical structure. Whereas, extraction of the implicit link relationship is a challenging task. Mining of linguistics and behavioural pattern of user-generated content such as, like, dislike, follow, comment and share lead to extract implicit graphical structure.

In this paper, an analytical and methodological user identification framework is developed to significantly binds implicit and explicit link relationship over the end-users graphical perspective. Identify malicious user, its communal information and sockpuppet node. Apart from that, this work provides the concept of the deep neural network approach over the graphical and linguistic perspective of end-user to classify as malicious, fake and genuine. This concept also helps identify the trade-off between the similarity of nodes attributes and the density of connections for Influence maximization.

The organization of the paper is as follows. In the second part, the relevant literature is given, and the social media analysis and fake account detection programs are briefly mentioned. In the third part, the algorithms we developed and used are mentioned. While the evaluation results are mentioned in the fourth section, results and suggestions are given in the last

section.

## II. RELATED WORK

Social networking has become an increasingly important application in recent years, because of its unique ability to enable social contact over the internet for geographically dispersed users. A social network can be represented as a graph, in which nodes represent users, and links represent the connections between users.

The purpose of the literature survey is to gain and understand the diverse and dynamic nature of social media data for feature extraction to extract Misuse of Fake Profiles for Review Spam On Social Media [1-7], Detection of fake review spreading community [8,10].

Along with that total eight articles (published in 2016 to 2019) presented in this paper are summarized in Table 1 that contains six columns. The main task of the articles is illustrated in the second column. Column third illustrates method used. Column fourth illustrate method and algorithm used for account verification in different application. Whereas sixth column describes the name of data sets and its source that has been used for evaluating different methodology.

Cresci et al. [5] developed a behaviour model inspired by biological DNA in detecting spambots in social networks in another bot research. By changing the genetic algorithm's different parameters, it was determined how advanced bots escaped from detection techniques, in another Galindo et al. [6] examined political bots in the General Elections. The accounts considered in the study using three different data sets are grouped as bot or human. To classify the data set, features such as the age and location of the relevant Twitter accounts, the length of the user step, the sickness per tweet, and the time between two retweets were used. AdaBoost, logistic regression, support vector machine and naive Bayes have been tested as the classification algorithm. Logistic regression worked the best among them. Based on the data in Chasma, author can say that bots retweet slightly less than real accounts. Also, bots include more external URLs in their tweets than original accounts.

Ruiz et al. [7] claim that when detecting bots on Twitter, follower friends' ratio will not always give us correct results. They think that bots can unfollow accounts that do not automatically follow back. Instead, the text in the tweets of bot accounts is more uniform than the actual accounts. They use text entropy to measure similarity. It also deals with the methods used to access Twitter to detect bot and human accounts. For example, most human accounts use the web or mobile application, while the bots have stated that they use other applications such as API, they also stated that human accounts have a more complex timing behaviour than bots and cyborgs. In this study, they use multiple classification methods as bots or human accounts in the Twitter social network. The process of updating has been carried out. By applying feature extraction techniques to the data set, it has been prepared for the dilution process.

## III. PROPOSED WORK

A graphical, linguistics and social theory based relationship identification (RIF) framework is developed to identify mali-

cious end-user over social media, as shown in Fig. 1. This framework amalgamates linguistics, temporal and contextual ethics of user-generated content with profile and graphical information.

The RIF framework extract feature vector to delineate user behaviours and similarity index over social media. Classifying identical profile concerning to similar user via Jaccard coefficient over linguistics pattern of tweets and provide linguistics, temporal and contextual meaning to develop a mathematical model for classifying identical profile as sockpuppet over social media.

### A. Data Extraction

RIF framework analyze and extract user pattern from user-generated content, profile and graphical information of social media user. This approach encapsulates social media mining concepts, theories, with the concept of natural language processing to extract the communal intersection of user-generated and profile content from social media.

### B. User Feature Vector

RIF framework examine and correlate user profile ( $u_f$ ), generated data ( $c_f$ ) with graphical perspective ( $g_f$ ) of social media data as .

$$\rho = \{u_f \bowtie c_f \bowtie g_f\} \quad (1)$$

The taxonomy of user feature includes profile, content, and graph-based feature, as shown in Fig. 2. Whereas in this work profile-based feature comprises validation of profile information such as suspicious user profile is verified or not, profile age, profile cover, and picture as

$$u_f = \begin{cases} verified & \text{if } v_f = y \\ age & \text{if not immediate} \\ cover & \text{if not default} \\ picture & \text{if not default} \end{cases} \quad (2)$$

However, content-based features include temporal, contextual validation of user-generated data, grammatical quality, and emotional context of surfing nature as shown in Fig. 3.

Temporal taxonomy comprises time interval between tweets( $t_g$ ), retweets ( $rt_g$ )and its frequency( $t_f, rt_f$ ). Contextual content includes term and document frequency of user tweets, Whereas linguistics feature reflects the standard of language script and sensitivity incorporate susceptibility of the user while tweets.

$$t_f = \begin{cases} t_g & = time \\ rt_g & = time \\ t_f & = number \\ rt_f & = number \end{cases} \quad (3)$$

However, graph-based features include validation of structural and relational nature of end-user such as number of friends, follower, friend distribution, etc.

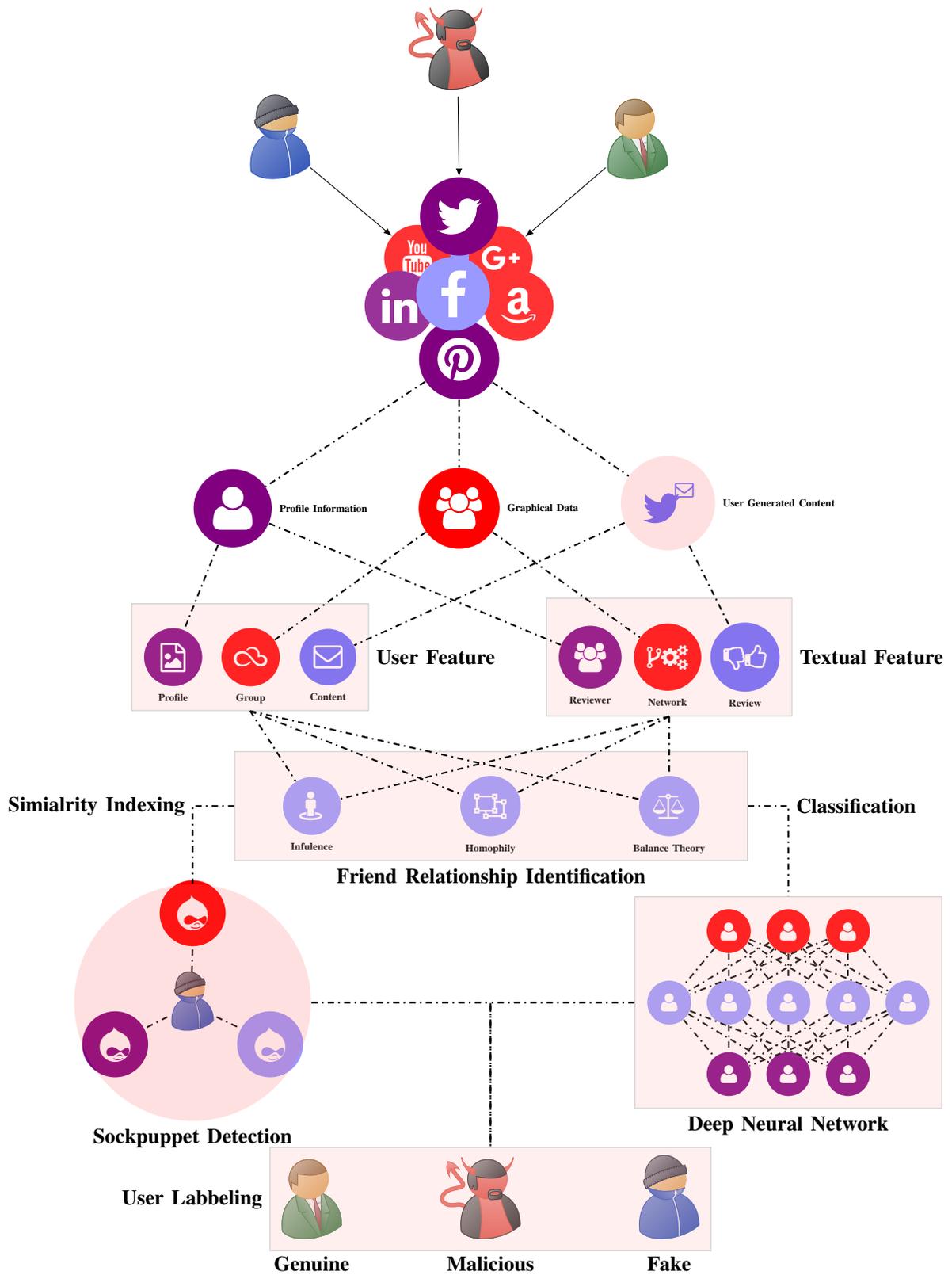


Fig. 1. Proposed Relationship Identification (RIF) Framework for Fake User Identification.

TABLE I. ARTICLE SUMMARY:FAKE ACCOUNT DETECTION

R	Task	Approach	Algo	Data Set	Research Gap
[8]	Cross-Platform Fake account identification	Friend Relationship-Based User Identification	Graph Based	Crude Data Set	Multiple Dimensions Profile Information
[9]	Anomalous Compromised Account Detection	Statistical Anomaly Detection Techniques	Graph Based	Twitter Dataset	Discriminate weightage of features
[10]	Sybil Attacks detection Via Fake profile	Deep-Regression	Graph Based	USA Election Tweeter data set	Handling noisy and malicious data
[11]	Sybil Attacks detection Via Fake profile	Pairing-based Cryptography	Graph Based	Twitter and YouTube dataset	Handling optimized defensive features
[12]	Mining Fake Account	Social Media Mining	Machine Learning	Deceptive Accounts Dataset	Detection of identity deception
[13]	Contextual long short-term memory architecture to detect bots	Deep Neural Network	Machine Learning	Cresci and Collaborators Dataset	Scrutinize social media Conversation in different contexts
[14]	Location labeling for Spam Account detection	Similarity based Social Media Mining	Machine Learning	Twitter API Dataset	Handle dynamic information
[15]	Detection of malicious profiles	Petri net structure analyzes	GB-Machine Learning	Crude dataset	Optimization of irrelevant features



Fig. 2. User Feature over Social Media.

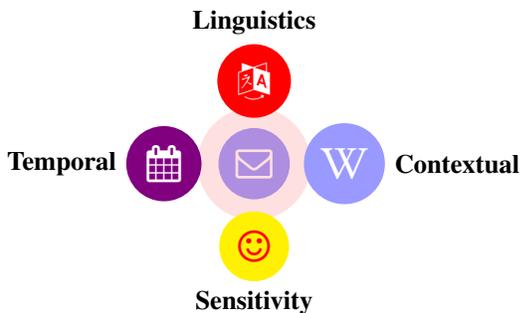


Fig. 3. Content Based Feature over Social Media.

### C. Textual Feature

Textual feature of social media user generated content are classified into three class behalf of content, reviewer profile and network dimension as shown in Fig. 4. RIF framework examine and correlate following Review, Reviewer and Network centric feature.

#### (a) Reviewer Centric Feature [16], [17], [18]

- Number of reviews

- Number of Shared/helpful votes
- Time interval between reviews
- Percentage of positive and negative reviews
- Ratio of verified purchase
- Verified stay flag
- Rating deviation
- Review length

#### (b) Review Centric Feature[19], [20], [21], [22], [23], [17], [18], [24], [25]

- Content Similarity Score (Nearly Duplicates)
- Percentage of Pronouns/ Nouns/ Adjective / Verbs
- Lexical Validity
- Lexical Diversity
- Content Diversity
- Syntactical Diversity
- Active and Passive Voice
- Picture and Links
- Emotivenss
- Content Relevancy
- Sentiment Score
- Linguistic inquiry and Word Count
- Product Information Matching
- First Review Flag

#### (c) Network Centric Feature (NCF) [26], [27]

- IP address
- GPS Information
- Timestamp
- Traffic Patterns (IP density )
- Device Information

### D. Relationship Identification

After identifying profile and textual feature of end-user as seed profile , relationship identification employed balance theory to extracts hidden relationships of other similar profile with seed profile as implicit link relationship. For instance, consider  $g(v,r_e)$  as a social media graph having 11 users nodes and 9 relationship edges, as shown in Fig. 5. Then



Fig. 4. Textual Feature over Social Media Post.

after applying the balance theory of SMM, two hidden implicit relationships are extracted over graph  $g(v, r_e)$ , as shown in Fig. 6 by the red line.

After extracting the secret relationship, nodes are hierarchically differentiated according to their implicit status derived through the status theory. After applying the status theory, node colour over the clique are changed. The Degree of the brightness of node color has shown its hidden implicit statuses over the clique, as shown in Fig. 7.

Simultaneously, the graph transmit effects as explicit characteristics extracted through Influence, Homophily, and Confounding correlation theory. Higher status communal node changes the belongingness of its lower status node into their respective community through the Influence theory. Whereas, homophily builds the belongingness of similar characteristics node over the same community. However, any online forum creates an environment to make individuals similar, as confounding.

After extracting implicit information from social media through social theory, NCF generates vertex degree vector and reachability matrix, as shown in equation 6.16 and 6.17.

$$n_d^v = \{n_d^1, n_d^2, n_d^3, \dots, n_d^m\} \forall m \leq n - 1 \quad (4)$$

Where,  $n_d^v$  is represent node degree vector and  $n_d^i$  is the number of node having degree  $i$  in desire clique structure. Whereas,  $node_{rm}$  represent node reachability square matrix having  $n \times n$  dimension and  $r_{v_i, v_j}$  is the modular distance between node  $v_i$  and  $v_j$

$$node_{rm} = [r_{v_i, v_j}]_{n \times n} \quad (5)$$

After extracting node feature vector and matrix, multiplication of vertex degree vector and node reachability matrix return  $A_{i,j}$  as the highest influence node. Simultaneously, the K-means algorithm builds the community of similar nodes with a similarity index of the Jaccard coefficient over the initial point  $A_{i,j}$ .

#### IV. ENVIRONMENTAL SETUP AND RESULT ANALYSIS

The comparative analysis is present interesting and useful facts regarding the state-of-the-art of malicious account classification technique. For performance evaluation of DNN based RIF framework with basic stand-alone classifiers such as Random Forest (RF), Bagging Classifier, J48 Classifier, Random Tree, and Logistic Regression has been carried out over two different interaction and structural anomalies social media data set, namely Crude and Cresci Collaborators (CCDS) data

set. Crude dataset [10] has 6824 profile data(Fake+ Genuine), 59153788 tweets, 4899493 followers, 16236669 Likes, 67976 listed count 1367 URL Shared. Simultaneously, CCDS [11] has 3474 genuine accounts, 8377522 genuine tweets, 991 fake account, and 1610176 fake tweets.

Performance evaluation of Random Forest (RF) for malicious account classification with and without user feature and social theory is described in Table I.

The RF algorithm acquires 67.09%, 66.98%, 68.12% and 80.21% 78.45%, 81.78% precision with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table II and Fig. 8(a). The RF algorithm's performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The RF algorithm acquires 1.53%, 1.36%, 3.09% and 33.02%, 30.10%, 35.62% improvement over the precision with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 8(b).

Whereas, RF algorithm acquires 67.34%, 66.14%, 68.92% and 78.41% 74.24%, 79.12% recall with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table II and Fig. 8(c). The RF algorithm's performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The RF algorithm acquires 3.09%, 1.26%, 5.51% and 41.15%, 33.65%, 35.62% improvement over the recall with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 8(d).

Simultaneously, RF algorithm acquires 67.84%, 65.91%, 69.46% and 78.9% 76.14%, 79.98% F1-Score with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table II and Fig. 8(e). The RF algorithm's performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The RF algorithm acquires 4.19%, 1.23%, 6.68% and 38.37%, 33.53%, 40.27% improvement over the F1-Score with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 8(f).

However, RF algorithm acquires 92.94%, 92.1%, 93.45% and 95.78%, 94.56%, 96.2% Accuracy with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table II and Fig. 8(g). The RF algorithm's performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The RF algorithm acquires 1.41%, .49%, 1.96% and 5.46%, 4.12%, 5.92% improvement over the Accuracy with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 8(h).

The Bagging algorithm acquires 66.59%, 65.19%, 67.82% and 75.22%, 74.61%, 76.15% precision with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table III and Fig. 9(a). The RF algorithm's performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Bagging acquires 3.43%, 1.26%, 5.34% and 42.25%, 41.09%, 44.01% improvement over the precision with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 9(b).

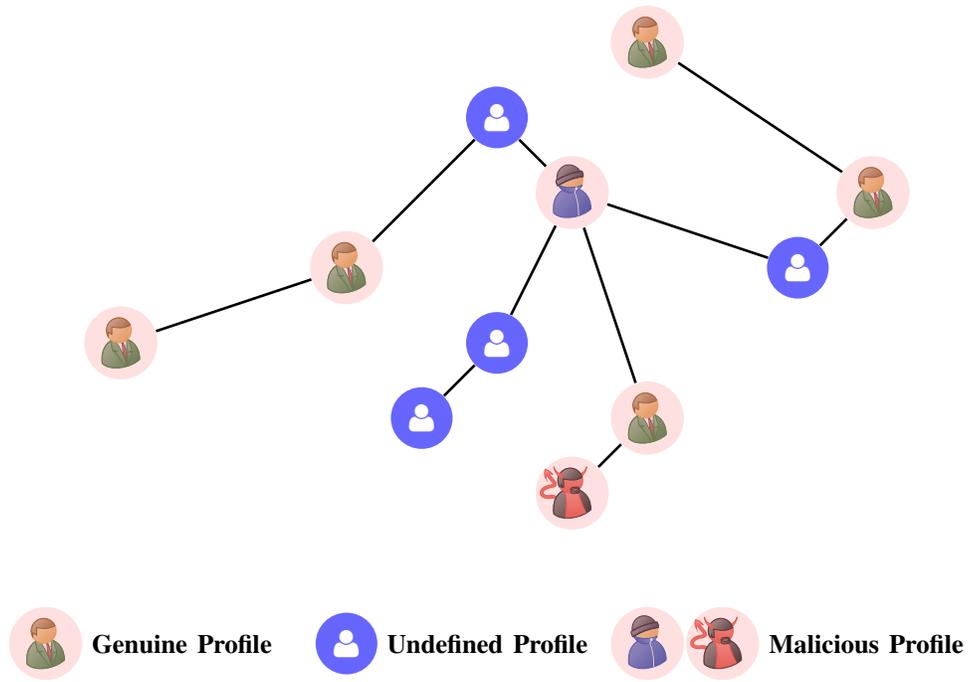


Fig. 5. Structure of user Community.

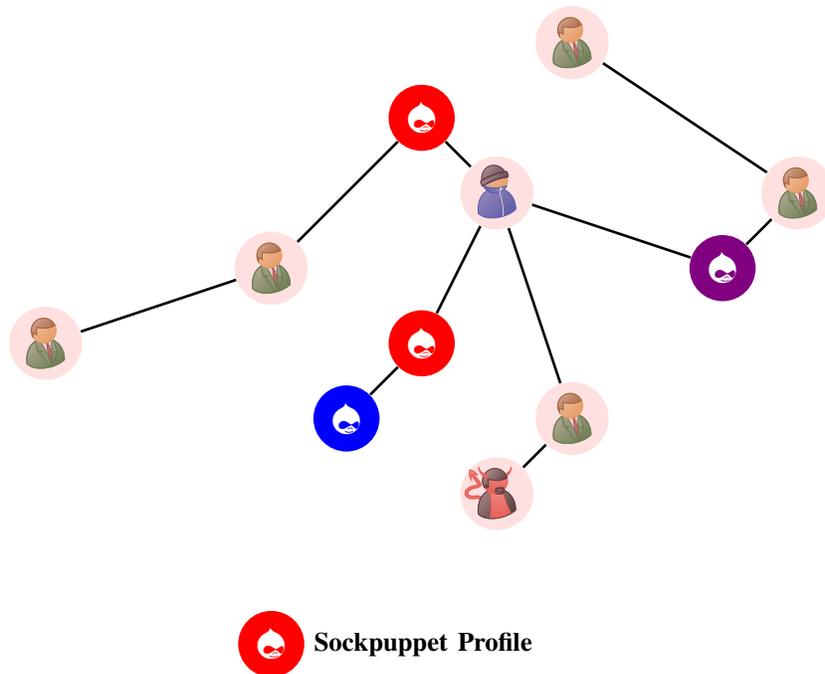


Fig. 6. Identify Status of Profile Via Balance Theory.

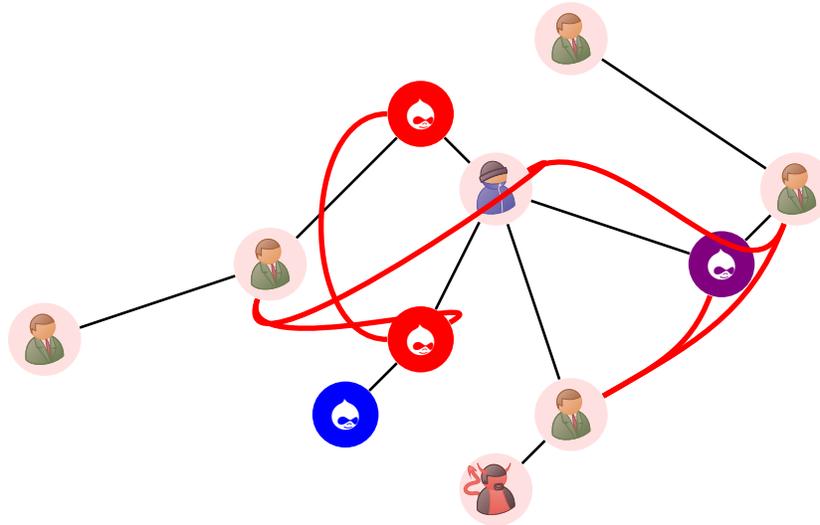


Fig. 7. Implicit Link Structuring via Influence and Homophily.

TABLE II. MALICIOUS ACCOUNT CLASSIFICATION THROUGH RANDOM FOREST

Data Set	Evaluation Parameter	Standalone	User Feature	Social Theory	Fusion
Crude	Precision	66.08	67.09	66.98	68.12
	Recall	65.32	67.34	66.14	68.92
	F1-Score	65.11	67.84	65.91	69.46
	Accuracy	91.65	92.94	92.10	93.45
CCSD	Precision	60.30	80.21	78.45	81.78
	Recall	55.55	78.41	74.24	79.12
	F1-Score	57.02	78.90	76.14	79.98
	Accuracy	90.82	95.78	94.56	96.20

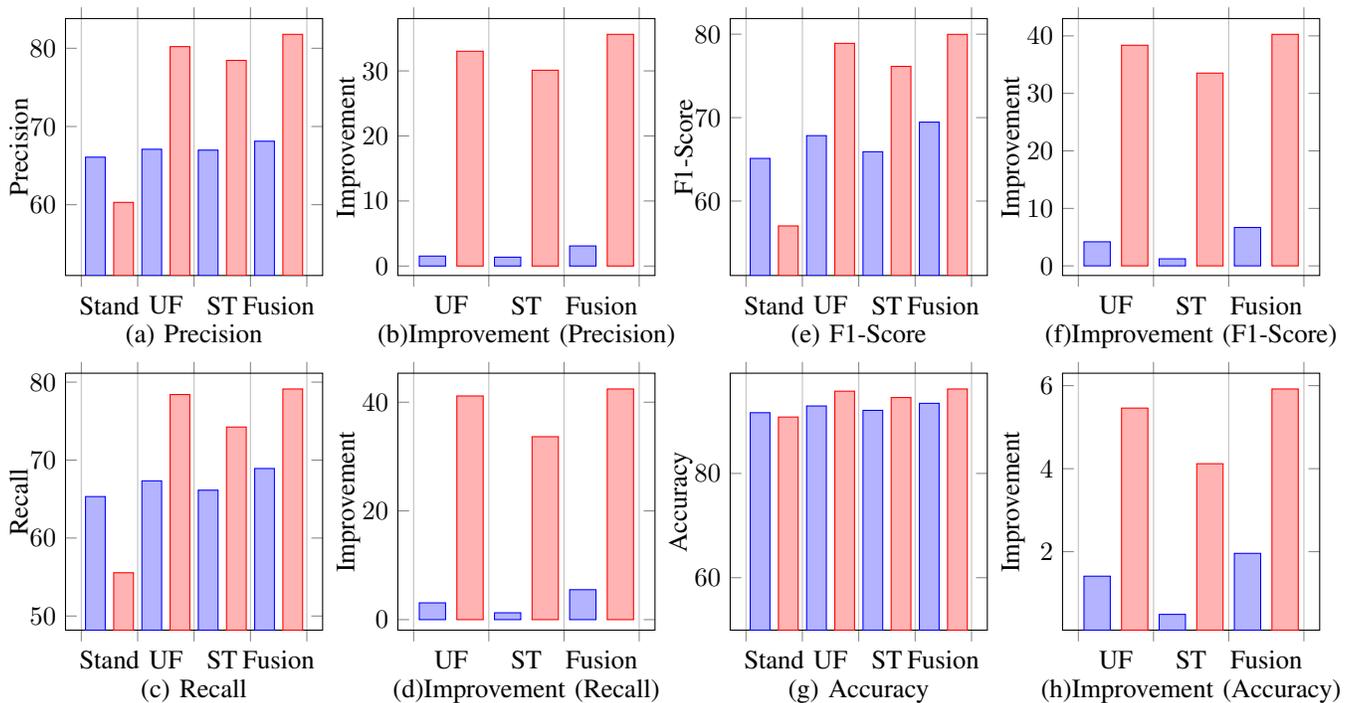


Fig. 8. Performance Evaluation of Malicious Account Classification Through Random Forest.

TABLE III. MALICIOUS ACCOUNT CLASSIFICATION THROUGH BAGGING

Data Set	Evaluation Parameter	Standalone	User Feature	Social Theory	Fusion
Crude	Precision	64.38	66.59	65.19	67.82
	Recall	63.04	66.69	64.85	67.98
	F1-Score	55.36	65.24	64.12	68.72
	Accuracy	90.94	92.74	90.42	93.14
CCDS	Precision	52.88	75.22	74.61	76.15
	Recall	48.84	73.16	70.58	73.89
	F1-Score	49.83	73.65	71.25	75.28
	Accuracy	89.44	95.55	92.18	95.98

Whereas, Bagging acquires 66.69%, 64.85%, 67.98% and 73.16%, 70.58%, 73.89% recall with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table III and Fig. 9(c).The Bagging performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The RF algorithm acquires 5.79%, 2.87%, 7.84% and 49.80%, 44.51%, 51.29% improvement over the recall with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 9(d).

Simultaneously, Bagging acquires 65.24%, 64.12%, 68.72% and 73.65%, 71.25%, 75.28% F1-Score with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table III and Fig. 9(e). The Bagging performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Bagging acquires 17.85%, 15.82%, 24.13% and 47.80%, 42.99%, 51.07% improvement over the F1-Score with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 9(f).

However, Bagging acquires 92.74%, 91.42%, 93.14% and 95.55%, 92.18%, 95.98% Accuracy with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in table 3 and figure 9(g).The Bagging performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Bagging acquires 1.98%, .53%, 2.42% and 6.83%, 3.06%, 7.31% improvement over the Accuracy with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 9(h).

The J48 algorithm acquires 63.52%, 62.78%, 64.15% and 70.6%, 64.52%, 72.82% precision with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table IV and Fig. 10(a). The J48 performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Bagging acquires 4.75%, 3.53%, 5.79% and 52.19%, 39.08%, 56.97% improvement over the precision with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 10(b).

Whereas,J48 acquires 62.02%, 59.69%, 62.84% and 69.23%, 65.82%, 71.56% recall with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in table 4 and figure 10(c).The J48 performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The J48 acquires 5.14%, 1.19%, 6.53% and 64.52%, 56.42%, 70.06%

improvement over the recall with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 10(d).

Simultaneously, J48 acquires 61.73%, 58.36%, 62.84% and 69.19%, 66.58%, 70.69% F1-Score with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table IV and Fig. 10(e).The J48 performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The J48 acquires 19.68%, 13.14%, 21.13% and 58.73%, 52.74%, 62.17% improvement over the F1-Score with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 8(f).

However, J48 acquires 91.87%, 91.25%, 93.14% and 93.95%, 92.56%, 94.64% Accuracy with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table IV and Fig. 8(g).The J48 performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The J48 acquires 1.77%, 1.09%, 3.18% and 6.50%, 4.92%, 7.28% improvement over the Accuracy with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 10(h).

The Random tree algorithm acquires 64.67%, 64.08%, 65.84% and 72.76%, 70.28%, 73.58% precision with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table V and Fig. 11(a). The J48 performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Random tree acquires 1.57%, 0.64%, 0.41% and 41.04%, 36.23%, 42.62% improvement over the precision with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 11(b).

Whereas, Random tree acquires 65.13%, 64.56%, 66.18% and 50.86%, 49.86%, 52.69% recall with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table V and Fig. 11(c). The Random tree performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Random tree acquires 4.59%, 3.68%, 6.28% and 7.48%, 5.37%, 11.35% improvement over the recall with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 11(d).

Simultaneously, Random tree acquires 63.78%, 62.86%, 64.27% and 54.15%, 52.85%, 55.28% F1-Score with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table V and Fig.

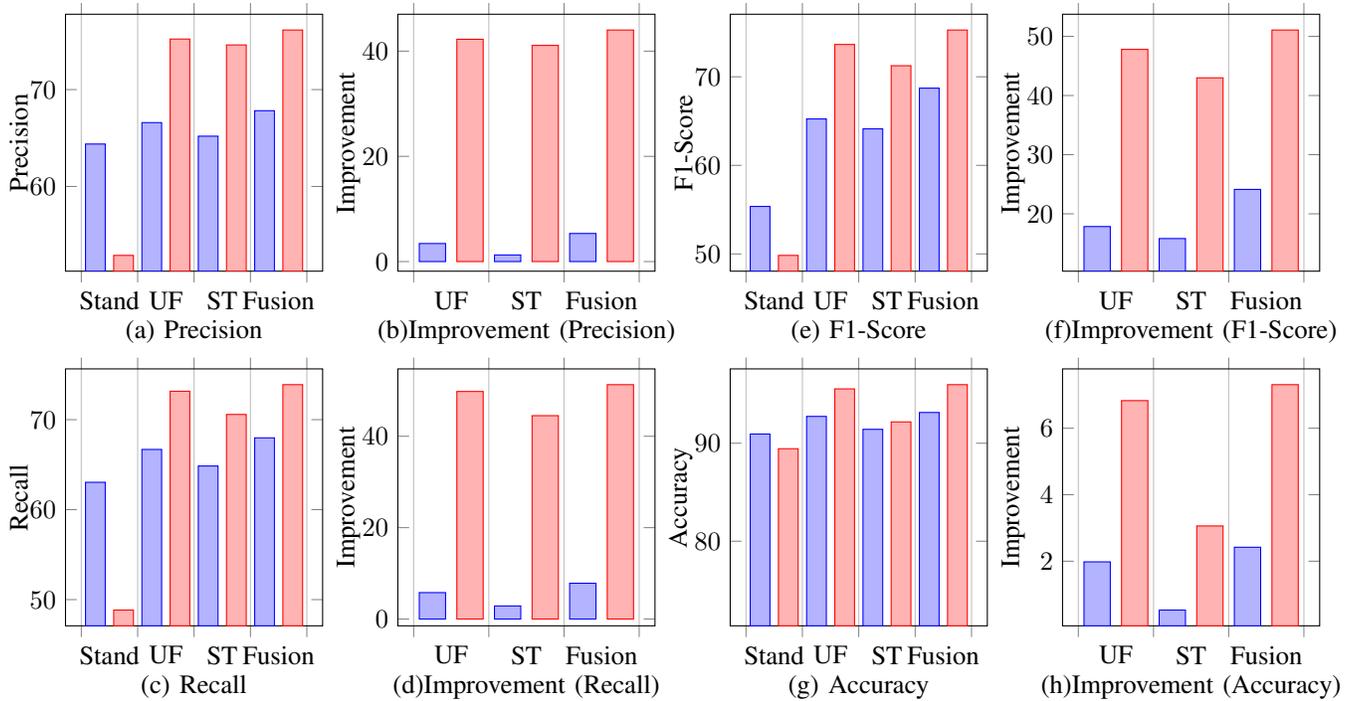


Fig. 9. Performance Evaluation of Malicious Account Classification Through Bagging.

TABLE IV. MALICIOUS ACCOUNT CLASSIFICATION THROUGH J48

Data Set	Evaluation Parameter	Standalone	User Feature	Social Theory	Fusion
Crude	Precision	60.64	63.52	62.78	64.15
	Recall	58.99	62.02	59.69	62.84
	F1-Score	51.58	61.73	58.36	62.48
	Accuracy	90.27	91.87	88.25	92.14
CCSD	Precision	46.39	70.6	64.52	72.82
	Recall	42.08	69.23	65.82	71.56
	F1-Score	43.59	69.19	66.58	70.69
	Accuracy	88.22	93.95	92.56	94.64

TABLE V. MALICIOUS ACCOUNT CLASSIFICATION THROUGH RANDOM TREE

Data Set	Evaluation Parameter	Standalone	User Feature	Social Theory	Fusion
Crude	Precision	63.67	64.67	64.08	65.84
	Recall	62.27	65.13	64.56	66.18
	F1-Score	54.61	63.78	62.86	64.27
	Accuracy	90.65	91.54	91.05	92.47
CCSD	Precision	51.59	72.76	70.28	73.58
	Recall	47.32	50.86	49.86	52.69
	F1-Score	48.36	54.15	52.85	55.28
	Accuracy	89.06	94.84	92.42	95.58

TABLE VI. MALICIOUS ACCOUNT CLASSIFICATION THROUGH LOGISTIC REGRESSION

Data Set	Evaluation Parameter	Standalone	User Feature	Social Theory	Fusion
Crude	Precision	52.97	60.92	59.85	62.56
	Recall	53.42	61.54	60.21	63.08
	F1-Score	53.13	61.11	60.48	62.46
	Accuracy	88.31	90.17	88.23	91.47
CCSD	Precision	57.21	63.18	61.56	64.58
	Recall	46.03	92.54	89.95	94.12
	F1-Score	56.44	92.72	90.56	93.86
	Accuracy	76.75	84.67	83.41	85.98

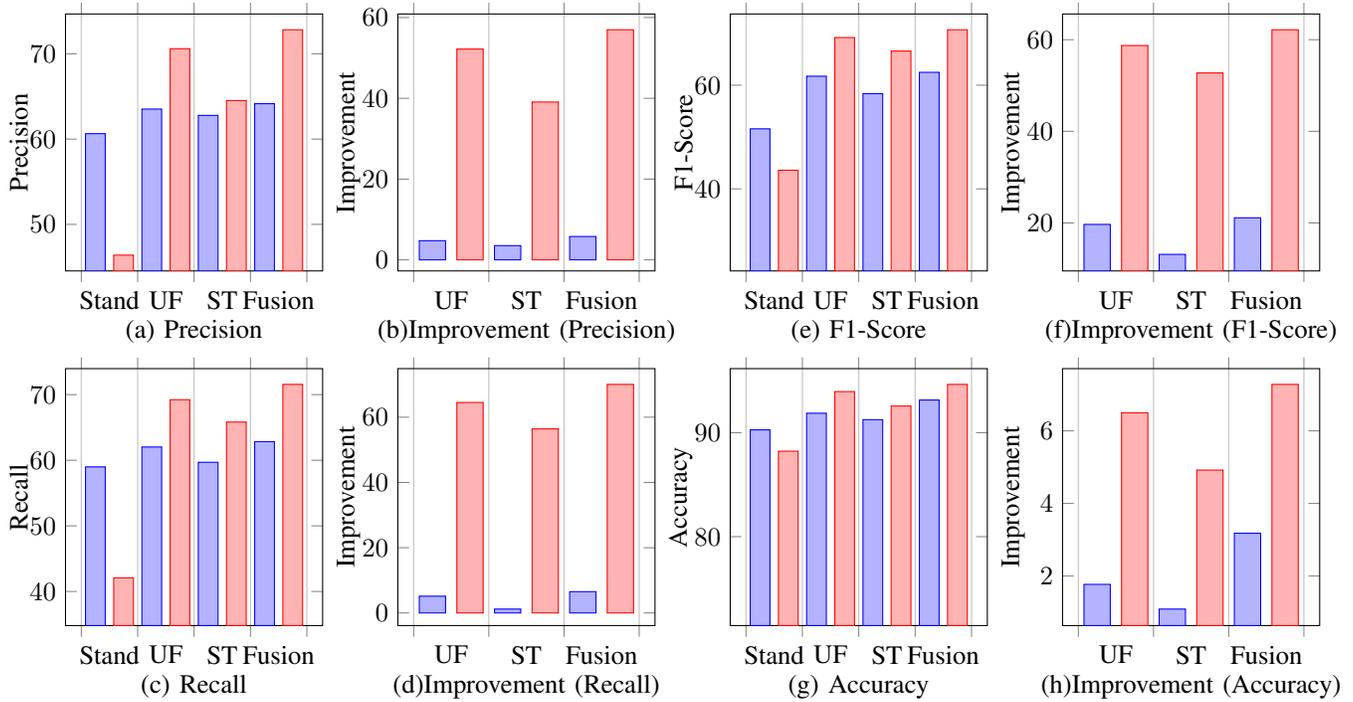


Fig. 10. Performance Evaluation of Malicious Account Classification Through J48.

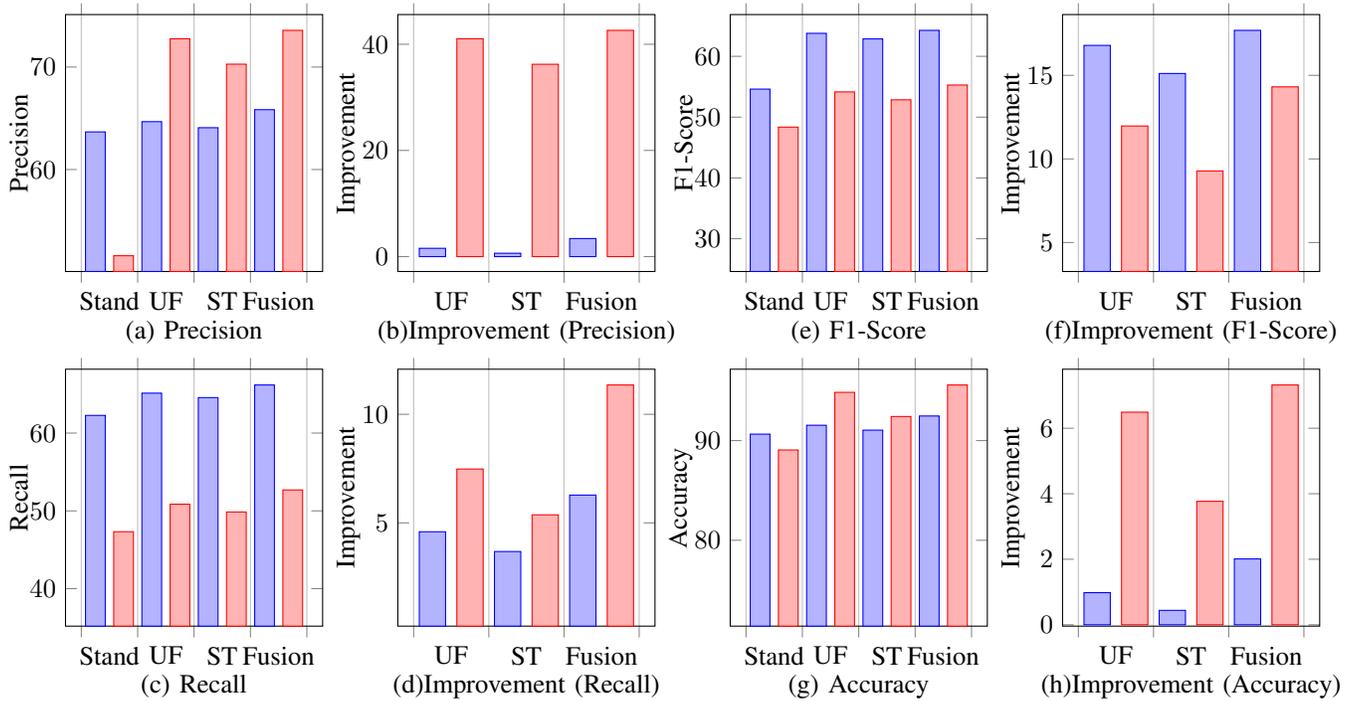


Fig. 11. Performance Evaluation of Malicious Account Classification Through Random Tree.

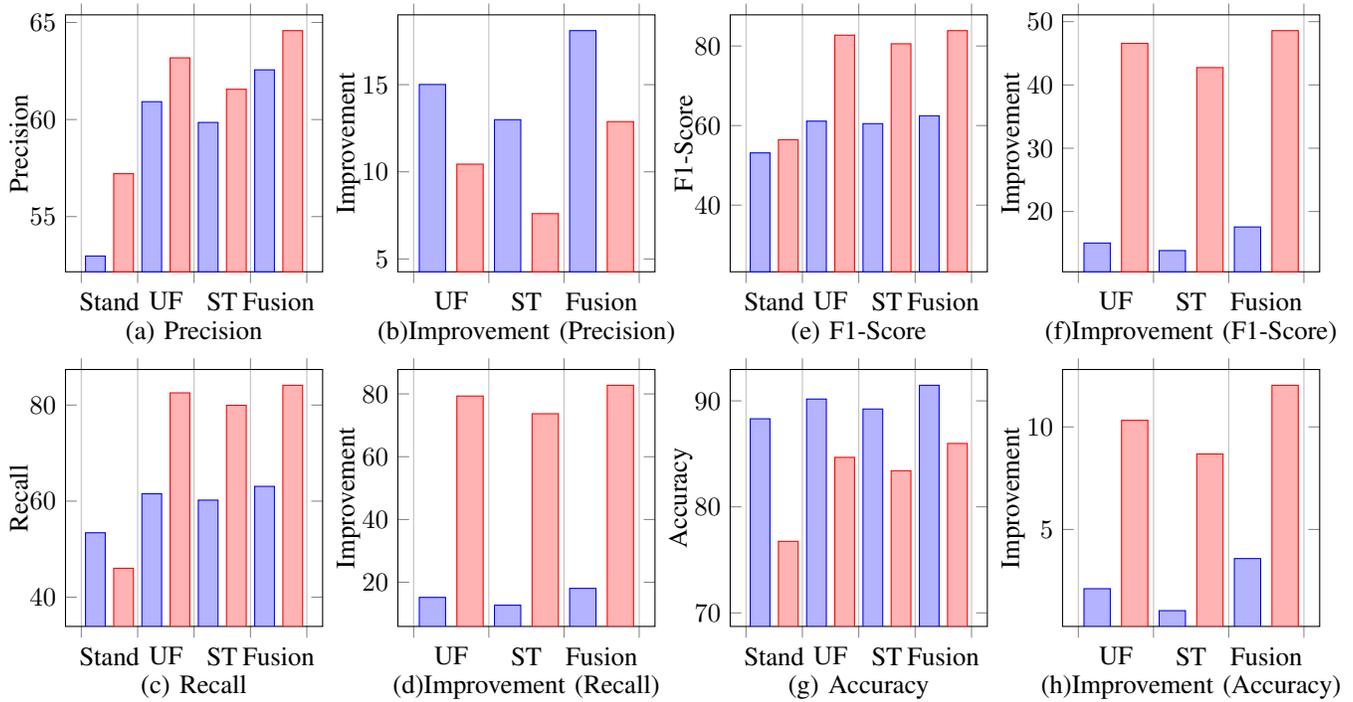


Fig. 12. Performance Evaluation of Malicious Account Classification Through Logistic Regression.

TABLE VII. MALICIOUS ACCOUNT CLASSIFICATION THROUGH PROPOSED WORK

Data Set	Evaluation Parameter	Random Forest	Bagging	J48	Random Tree	Logistic Regression	Proposed Work
Crude	Precision	68.12	67.82	64.15	65.84	62.56	75.89
	Recall	68.92	67.98	62.84	66.18	63.08	76.42
	F1-Score	69.46	68.72	62.48	64.27	62.46	77.52
	Accuracy	93.45	93.14	93.14	92.47	91.47	95.89
CCSD	Precision	81.78	76.15	72.82	73.58	64.58	82.49
	Recall	79.12	73.89	71.56	52.69	84.12	87.76
	F1-Score	79.98	75.28	70.69	55.28	83.86	86.19
	Accuracy	96.2	95.98	94.64	95.58	85.98	98.54

11(e). The Random tree performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Random tree acquires 16.79%, 15.11%, 17.69% and 11.97%, 9.28%, 14.31% improvement over the F1-Score with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 11(f).

However, Random tree acquires 72.76%, 70.28%, 73.78% and 94.84%, 92.42%, 95.58% Accuracy with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table V and Fig. 11(g). The Random tree performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Random tree acquires .98%, .44%, 2.01% and 6.49%, 3.77%, 7.32% improvement over the Accuracy with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 11(h).

The Logistic algorithm acquires 60.92%, 59.85%, 62.56% and 63.18%, 61.56%, 64.58% precision with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table VI and Fig. 12(a). The Logistic performance is significantly boosted up after

rectifying network information by user feature, social theory, and fusion of both. The Logistic acquires 15.01%, 12.99%, 18.10% and 10.44%, 7.60%, 12.88% improvement over the precision with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 12(b).

Whereas, Logistic regression algorithm acquires 61.54%, 60.21%, 63.08% and 82.54%, 79.95%, 84.12% recall with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table VI and Fig. 12(c). The Logistic performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The J48 acquires 15.20%, 12.71%, 18.08% and 79.32%, 73.69%, 82.75% improvement over the recall with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 12(d).

Simultaneously, Logistic regression algorithm acquires 61.11%, 60.48%, 62.46% and 82.72% 80.56%, 83.86% F1-Score with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table VI and Fig. 12(e). The Logistic performance is significantly boosted up after rectifying network information by user fea-

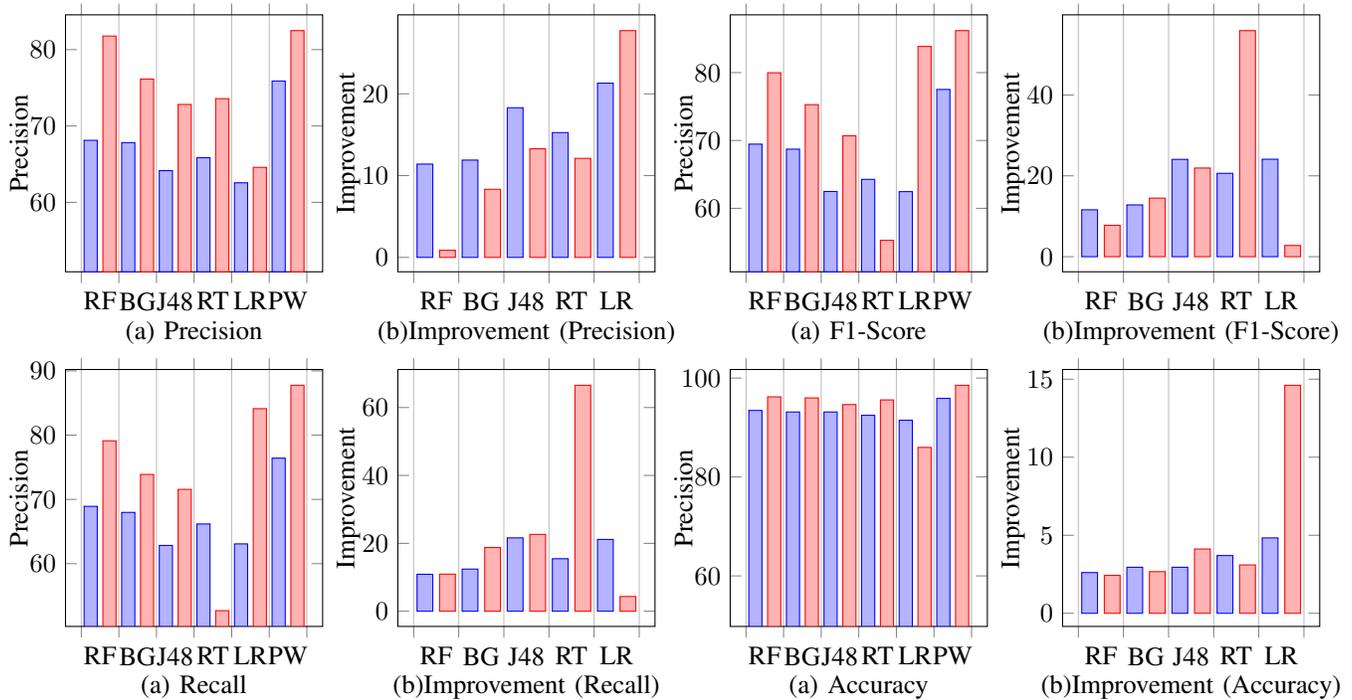


Fig. 13. Performance Evaluation of Malicious Account Classification Through Proposed Work.

ture, social theory, and fusion of both. The Logistic acquires 15.02%, 13.83%, 17.56% and 46.56%, 42.74%, 48.58% improvement over the F1-Score with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 12(f).

However, Logistic regression algorithm acquires 90.17%, 89.23%, 91.47% and 84.67% ,83.41%, 85.98% Accuracy with user feature, social theory, and fusion of both respectively over Crude and CCDS data set as shown in Table VI and Fig. 12(g).The Logistic performance is significantly boosted up after rectifying network information by user feature, social theory, and fusion of both. The Logistic acquires 2.11%, 1.04%, 3.58% and 10.32%, 8.68%, 12.03% improvement over the Accuracy with user feature, social theory, and fusion of both over Crude and CCDS data set, as shown in Fig. 12(h).

Whereas Proposed work acquire 75.89% , 82.49% precision, 76.42% , 87.76% recall, 77.52%, 86.19% F1-Score, and 95.89%, 98.54% Accuracy respectively over Crude and CCDS data set as shown in Table VII and Fig. 13. However its gain 11.41% - 21.31% and 0.87% - 27.73% improvement in precision, 10.88% - 21.61% and 10.92% - 66.56% improvement in recall, 11.60% - 24.11% and 2.78% - 55.92% improvement in F1-Score, and 2.61% - 4.83% and 2.43% - 14.61% improvement in Accuracy over Crude and CCDS data set, as shown in Fig. 13.

## V. CONCLUSION

Online Social Network (OSN) is a network hub where people with similar interests or real world relationships interact. As the popularity of OSN is increasing, the security and privacy issues related to it are also rising. Fake and Clone profiles are creating dangerous security problems to social network users. Cloning of user profiles is one serious

threat, where already existing userâ€™s details are stolen to create duplicate profiles and then it is misused for damaging the identity of original profile owner. They can even launch threats like phishing, stalking, spamming, etc. Fake profile is the creation of profile in the name of a person or a company which does not really exist in social media, to carry out malicious activities. In this paper graphical, linguistics and social theory based relationship identification (RIF) framework is developed to identify malicious end-user over social media. This framework amalgamates linguistics, temporal and contextual ethics of user-generated content with profile and graphical information. The RIF framework extract feature vector to delineate user behaviors and similarity index over social media. Classifying identical profile concerning to similar user via Jaccard coefficient over linguistics pattern of tweets and provide linguistics, temporal and contextual meaning to develop a mathematical model for classifying identical profile as sockpuppet over social media. RIF framework achieve maximum 82.49% precision, 87.76% recall, 86.19% F1-Score, and 98.54% Accuracy. However its gain maximum 27.73% improvement in precision, 66.56% improvement in recall, 55.92% improvement in F1-Score, and 14.61% improvement in Accuracy.

## REFERENCES

- [1] N. K. Singh, D. S. Tomar, and A. K. Sangaiah, "Sentiment analysis: a review and comparative analysis over social media," *Journal of Ambient Intelligence and Humanized Computing*, May 2018.
- [2] G. D. Domenico, J. Sit, A. Ishizaka, and D. Nunan, "Fake news, social media and marketing: A systematic review," *Journal of Business Research*, vol. 124, pp. 329–341, 2021.
- [3] N. Singh and D. Tomar, "Comprehensive analysis of scope of negation for sentiment analysis over social media," *Journal of Theoretical and Applied Information Technology*, vol. 97, pp. 1704–1719, 03 2019.

- [4] N. K. Singh and D. S. Tomar, "Feature fusion for negation scope detection in sentiment analysis: Comprehensive analysis over social media," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, 2019.
- [5] S. Cresci, M. Petrocchi, A. Spognardi, and S. Tognazzi, "On the capability of evolved spambots to evade detection via genetic engineering," *Online Social Networks and Media*, vol. 9, pp. 1–16, 2019.
- [6] J. Pastor-Galindo, M. Zago, P. Nespola, S. López Bernal, A. Huertas Celdrán, M. Gil Pérez, J. A. Ruipérez-Valiente, G. Martínez Pérez, and F. Gómez Mármol, "Twitter social bots: The 2019 spanish general election data," *Data in Brief*, vol. 32, p. 106047, 2020.
- [7] J. Rodríguez-Ruiz, J. I. Mata-Sánchez, R. Monroy, O. Loyola-González, and A. López-Cuevas, "A one-class classification approach for bot detection on twitter," *Computers and Security*, vol. 91, p. 101715, 2020.
- [8] X. Zhou, X. Liang, H. Zhang, and Y. Ma, "Cross-platform identification of anonymous identical users in multiple social media networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 28, pp. 411–424, Feb 2016.
- [9] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Towards detecting compromised accounts on social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, pp. 447–460, July 2017.
- [10] M. Al-Qurishi, M. Alrubaian, S. M. M. Rahman, A. Alamri, and M. M. Hassan, "A prediction system of sybil attack in social network using deep-regression model," *Future Generation Computer Systems*, vol. 87, pp. 743 – 753, 2018.
- [11] M. Al-Qurishi, S. M. M. Rahman, M. S. Hossain, A. Almogren, M. Alrubaian, A. Alamri, M. Al-Rakhami, and B. Gupta, "An efficient key agreement protocol for sybil-precaution in online social networks," *Future Generation Computer Systems*, vol. 84, pp. 139 – 148, 2018.
- [12] E. Van Der Walt and J. Eloff, "Using machine learning to detect fake identities: Bots vs humans," *IEEE Access*, vol. 6, pp. 6540–6549, 2018.
- [13] S. Kudugunta and E. Ferrara, "Deep neural networks for bot detection," *Information Sciences*, vol. 467, pp. 312 – 322, 2018.
- [14] M. Celik and A. S. Dokuz, "Discovering socially similar users in social media datasets based on their socially important locations," *Information Processing and Management*, vol. 54, no. 6, pp. 1154 – 1168, 2018.
- [15] S. R. Sahoo and B. Gupta, "Hybrid approach for detection of malicious profiles in twitter," *Computers and Electrical Engineering*, vol. 76, pp. 65 – 81, 2019.
- [16] Y. Liu and B. Pang, "A unified framework for detecting author spamicity by modeling review deviation," *Expert Systems with Applications*, vol. 112, pp. 148 – 155, 2018.
- [17] R. Barbado, O. Araque, and C. A. Iglesias, "A framework for fake review detection in online consumer electronics retailers," *Information Processing and Management*, vol. 56, no. 4, pp. 1234 – 1244, 2019.
- [18] Y. Liu, B. Pang, and X. Wang, "Opinion spam detection by incorporating multimodal embedded representation into a probabilistic review graph," *Neurocomputing*, vol. 366, pp. 276 – 283, 2019.
- [19] J. K. Rout, A. K. Dash, and N. K. Ray, "A framework for fake review detection: Issues and challenges," in *2018 International Conference on Information Technology (ICIT)*, pp. 7–10, 2018.
- [20] L. Li, B. Qin, W. Ren, and T. Liu, "Document representation and feature combination for deceptive spam review detection," *Neurocomputing*, vol. 254, pp. 33 – 41, 2017. Recent Advances in Semantic Computing and Personalization.
- [21] W. Liu, J. He, S. Han, F. Cai, Z. Yang, and N. Zhu, "A method for the detection of fake reviews based on temporal features of reviews and comments," *IEEE Engineering Management Review*, vol. 47, pp. 67–79, Fourthquarter 2019.
- [22] M. Petrescu, K. O'Leary, D. Goldring, and S. B. Mrad, "Incentivized reviews: Promising the moon for a few stars," *Journal of Retailing and Consumer Services*, vol. 41, pp. 288 – 295, 2018.
- [23] E. F. Cardoso, R. M. Silva, and T. A. Almeida, "Towards automatic filtering of fake reviews," *Neurocomputing*, vol. 309, pp. 106 – 116, 2018.
- [24] L. You, Q. Peng, Z. Xiong, D. He, M. Qiu, and X. Zhang, "Integrating aspect analysis and local outlier factor for intelligent review spam detection," *Future Generation Computer Systems*, vol. 102, pp. 163 – 172, 2020.
- [25] S. Noekhah, N. binti Salim, and N. H. Zakaria, "Opinion spam detection: Using multi-iterative graph-based model," *Information Processing & Management*, vol. 57, no. 1, p. 102140, 2020.
- [26] S. Shehnepoor, M. Salehi, R. Farahbakhsh, and N. Crespi, "Netspam: A network-based spam detection framework for reviews in online social media," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 1585–1595, July 2017.
- [27] J. K. Rout, A. Dalmia, K. R. Choo, S. Bakshi, and S. K. Jena, "Revisiting semi-supervised learning for online deceptive review detection," *IEEE Access*, vol. 5, pp. 1319–1327, 2017.

# A Parameter-free Clustering Algorithm based K-means

Said Slaoui<sup>1</sup>, Zineb Dafir\*<sup>2</sup>

Faculty of Science of Rabat, Mohammed V University  
Rabat, Morocco

**Abstract**—Clustering is one of the relevant data mining tasks, which aims to process data sets in an effective way. This paper introduces a new clustering heuristic combining the E-transitive heuristic adapted to quantitative data and the k-means algorithm with the goal of ensuring the optimal number of clusters and the suitable initial cluster centres for k-means. The suggested heuristic, called PFK-means, is a parameter-free clustering algorithm since it does not require the prior initialization of the number of clusters. Thus, it generates progressively the initial cluster centres until the appropriate number of clusters is automatically detected. Moreover, this paper exposes a thorough comparison between the PFK-means heuristic, its diverse variants, the E-Transitive heuristic for clustering quantitative data and the traditional k-means in terms of the sum of squared errors and accuracy using different data sets. The experiments results reveal that, in general, the proposed heuristic and its variants provide the appropriate number of clusters for different real-world data sets and give good clusters quality related to the traditional k-means. Furthermore, the experiments conducted on synthetic data sets report the performance of this heuristic in terms of processing time.

**Keywords**—Data mining; clustering; overlapping clustering; k-means; cluster centre initialization

## I. INTRODUCTION

In the last few years, the digital world has been facing rapid and unprecedented global evolutions due to the emergence of various concepts such as the development of the connected objects market, known as the internet of things, the continued growth of social networks, the strong use of the large e-commerce sites, as well as other factors. Therefore, this digital explosion presents a serious challenge for researchers to find appropriate techniques and efficient algorithms to analyze and process the considerable amount of data arising from those sources, and thus extract relevant information and facilitate decision-making.

Clustering is one of the relevant data mining tasks, which aims to process data sets effectively. Indeed, it proceeds by gathering the data objects the most similar into the same group, and the dissimilar ones into different groups, so that the similarity between data objects of the same group is the highest while the similarity between two data objects of different groups is the lowest [1]. The purpose is then to form disjoint groups, called clusters. The notion of similarity mainly depends on the attribute values describing the data objects and generally implies a distance measure. Accordingly, different clustering algorithms can make different clustering results for the same data set.

This paper suggests a parameter-free clustering algorithm

combining the E-transitive heuristic [2] and the traditional k-means algorithm [3] [4]. Indeed, the proposed heuristic does not require the prior initialization of the number of clusters. It generates progressively the initial cluster centres until the appropriate number of clusters is automatically detected. Hence, the improvements achieved through this heuristic concern primarily two major weaknesses of the k-means algorithm. The first one consists of fixing the number of clusters  $k$ , and the second one focuses on the determination of the initial cluster centres. Moreover, an overall comparison was established between the parameter-free clustering algorithm based k-means, its diverse variants, the E-transitive heuristic [2] adapted to quantitative data, the iterative k-means minus-plus [5] and the traditional k-means [3] [4] in terms of the sum of squared errors and accuracy measures using different UCI data set [6]. The experiment results reveal that, in general, the proposed heuristic and its variants provide the appropriate number of clusters for different real-world data set and give good clusters quality compared to the traditional k-means. Furthermore, the experiments conducted on synthetic data sets report the performance of this heuristic in terms of processing time.

The major contributions of this paper are as follows:

- Develop a new parameter-free clustering heuristic combining the E-transitive heuristic and the k-means algorithm to automatically determine the initial cluster centres and the number of clusters.
- Provide different variants of the PFK-means algorithm focusing on the initialization process applied with different approaches (Overlapping PFK-means and Hard PFK-means).
- Establish a comparison between the suggested heuristic, its variants, the E-transitive adapted to quantitative data, the traditional k-means, and the iterative k-means minus-plus algorithm.

The remainder of this paper is organized as follows: Section 2 fully describes the different steps of the proposed heuristic, its different variants, and the E-transitive heuristic adapted to quantitative data. Section 4 provides the experiment results on real-world and synthetic data sets. And finally, Section 5 covers the conclusion and future perspectives.

## II. LITERATURE REVIEW

Several clustering algorithms have been developed with the goal of ensuring optimal solutions for different clustering problems [7] [8] [9] [10] [11]. K-means is one of the popular partitioned clustering algorithms [3] [4], which aims to cluster

a set of data objects into  $k$  clusters by minimizing the sum of squared errors over these clusters. Despite its popularity, efficiency, and facility of implementation, the major difficulty encountered with the k-means algorithm is primarily related to its sensitivity to the initialization conditions including the selection of the initial clustering centres, the determination of the number of clusters  $k$ , and the possibility to converge on a local optimum [12] [1]. All these aspects influence the quality of clustering. To deal with these issues, researchers devote continuously great efforts to find adequate techniques able to provide suitable initialization parameters, so then ensure a higher clustering quality. Diverse initialization improvements were suggested over the years such as [13] [12] [14][15] [16] [17] [5] [18] [19] [20].

Among these enhancements, the global k-means [13] which is considered as a global search procedure aiming to find an optimal solution for a clustering problem. Indeed, this proposed technique proceeds by adding dynamically one cluster centre at a time using a series of local searches based on fast computed bound on the clustering error. Moreover, it consists of splitting the data space using a k-d tree structure to improve the performance of clustering.

Another initialization strategy represented in cluster center initialization algorithm (CCIA) [12], which intends to perform clustering using two major steps. The first one consists of generating clusters whose number may exceed the number of clusters  $k$ . In such a case the second step is employed by merging the similar clusters using a density-based multi-scale data condensation, and then the merged clusters are treated as the initial cluster centres of the k-means algorithm.

In the same context, the k-means ++ algorithm [14] aims to select the initial cluster centre uniformly at random, then choose the next cluster centres based on a determined probability until the total number of clusters is reached. The next step consists of applying the standard k-means algorithm.

Further enhancement regarding the k-means initialization strategies manifested in the modified global k-means algorithm [15] intends to compute clusters incrementally and determine the k-partition of the data set used based on the previous iterations. Thereby, the algorithm calculates the starting points by minimizing an auxiliary cluster function.

In a similar vein, the authors in [17] develop a new canopy clustering: a pre-processing method for the k-means algorithm, which aims to determine appropriate initial clustering centers and thus attains an optimal number of clusters  $k$ . The proposed algorithm covers the pre-processing density canopy method as well as the main k-means processes.

More recently, an entropy-based initialization method [18] for the k-means algorithm was developed to obtain an optimal number of clusters. Indeed, it determines the initial point using the maximization of Shannon's entropy-based objective function, then it aims to detect the best number of clusters based on the optimal cluster detection algorithm for faster convergence.

Another recent work represents the random initialization method [21] merging the bootstrap technique with the data depth concept. Thereby, this method employs k-means with bootstrap replications to find the cluster centres in the original

data space. Moreover, it aims to identify a good separation among clusters using depth computation.

### III. A PARAMETER-FREE CLUSTERING ALGORITHM BASED K-MEANS

#### A. Basic Concepts

Suppose a data set  $X = \{x_1, \dots, x_n\}$ , containing  $n$  data objects in Euclidean space,  $x_i \in \mathbb{R}^d$ ,  $i=1 \dots n$ . The aim is to partition  $X$  into  $k$  clusters  $C_1, C_2, \dots, C_k$ , that is,  $\bigcup_{j=1}^k C_j = X$  and  $C_i \cap C_j = \emptyset$  for  $1 \leq i \neq j \leq k$ .  $c_1, c_2, \dots, c_k$  are the centres of clusters  $C_1, C_2, \dots, C_k$  respectively and  $c_j = \frac{1}{|C_j|} \sum_{x_i \in C_j} x_i$ .

The difference between  $c_i$ , a centre of cluster  $C_j$  and a data object  $x$  is measured by  $dist(x, c_i)$ , where  $dist(x, y)$  is the Euclidean distance between two data objects  $x$  and  $y$ . The quality of cluster  $C_j$  can be measured by the sum of squared error between all data objects  $x_i$  in  $C_j$  and the cluster centre  $c_j$ , defined as:

$$E = \sum_{i=1}^n \sum_{j=1}^k dist(x_i, c_j)^2, x_i \in C_j \quad (1)$$

The average distance of all data objects in the data set  $X$  is defined as follows:

$$MeanDist(X) = \frac{2}{n(n-1)} \sum_{i=1}^n \sum_{j=i+1}^n dist(x_i, x_j) \quad (2)$$

A new cluster centre  $c_{new} \in X$  corresponds to the data object defined by:

$$dist(c_{new}, c_j) = Max(dist(x_i, c_j)) \quad (3)$$

where  $1 \leq j \leq p$ ,  $p \leq k$ ,  $x_i \in X$ ,  $p$  is the number of the existing cluster centres  $\{C_1, \dots, C_p\}$  and  $c_j$  corresponds to the  $j$ th cluster centre.

#### B. The PFK-means Heuristic

The proposed heuristic is a parameter-free clustering algorithm, named PFK-means, combining the E-transitive heuristic [2] adapted to quantitative data and the traditional k-means [3][4]. Indeed, PFK-means does not require any initial parameters and generates progressively the cluster centres until the appropriate number of clusters is automatically detected. More specifically, the PFK-means consists of two major stages: the first stage includes the construction of the initial cluster centres and thus discovers the number of clusters  $k$ . The second stage consists of applying the traditional k-means algorithm by taking the cluster centres of the first stage as well as the number of clusters detected in the previous stage.

1) *The initialization stage:* This stage aims to establish the cluster centres without specifying the number of clusters  $k$ . In that respect, it starts by calculating the average distance of all data objects using the equation 2. Then, it selects the first cluster centre randomly from the data set containing  $n$  data objects. The next step consists of calculating the distance between the selected centre and each data object in the data set, using the Euclidean distance. In the case where the distance value is less than the average distance value, the corresponding data object is added to the overlapping cluster, which is being formed. Otherwise, no changes will be applied.

The selection of the other cluster centres follows another strategy. In such a case, the selection is decided during the construction of the forgoing overlapping cluster. The data object the least similar to the foregoing cluster centres is defined as the cluster centre of the current overlapping cluster. In other words, the new cluster centre corresponds to the data object defined in equation 3. From the second iteration, after the determination of the cluster centre, the construction of the other overlapping clusters is made similarly to the first step. This process continues until all data objects are processed and thus the initial clusters, as well as the overlapping clusters, are obtained. The steps above-mentioned are described in the algorithm 1.

---

**Algorithm 1** Construction of initial clusters

---

**Input:**A set of  $n$  data objects  $X$

**Output:**The initial cluster centres  $T_{c_{next}}$ . The number of clusters automatically computed

**begin**

```
1: compute  $MeanDist(X)$  or  $MeanDist(SampleX)$ 
2: select the first cluster centre  $c_{new}$  randomly from  $X$ 
3: initialize  $Next \leftarrow true$ 
4:  $T_{c_{next}} \leftarrow null$ 
5: add  $c_{new}$  to  $T_{c_{next}}$ 
6: while  $Next$  do
7:    $c_{next} \leftarrow null$ 
8:   for  $i \leftarrow 0$  to  $|X|$  do
9:     calculate  $dist(x_i, c_{new})$ 
10:    if  $dist(x_i, c_{new}) < MeanDist(X)$  then
11:      assign  $x_i$  to the current cluster
12:    else if  $c_{next}$  is null then
13:       $c_{next} \leftarrow x_i$ 
14:    else if  $dist(x_i, c_{new}) > dist(c_{next}, c_{new})$  for all
15:       $c_{next}$  in  $T_{c_{next}}$  then
16:         $c_{next} \leftarrow x_i$ 
17:    end if
18:  end for
19:   $c_{new} \leftarrow c_{next}$ 
20:  add  $c_{new}$  to  $T_{c_{next}}$ 
21:  if  $c_{next}$  is null then
22:     $Next \leftarrow false$ 
23:  end if
24: end while
25: end begin
```

---

2) *The second stage:* The purpose of the initialization stage is to provide the initial cluster centres and detect the number of clusters  $k$  automatically. These parameters are the input settings of the traditional k-means executed in this stage. In that respect, the procedure starts by browsing the whole data set and thereafter scrolls through the list of cluster centres provided from the initialization stage and finally assign each data object to the appropriate cluster according to the Euclidean distance. After assigning all data objects to the appropriate clusters, the cluster centres are updated by calculating the mean of the data objects contained in each cluster. The process reiterates until there is no change in the cluster centres values. It should be noted that using the initial cluster centres obtained in the initialization stage as input settings of the traditional k-means allows a rapid convergence and an optimum solution. The pseudo-code of the traditional k-means is described in

Algorithm 2.

---

**Algorithm 2** The traditional k-means

---

**Input:** a set of  $n$  data objects  $X$ , the list of initial clusters  $T_{c_{next}}$ , the number  $k$  automatically computed

**Output:** the data objects in  $X$  partitioned in  $k$  clusters  
**begin**

```
1: repeat
2:   for  $i \leftarrow 0$  to  $|X|$  do
3:     for  $j \leftarrow 0$  to  $k$  do
4:       calculate  $dist(x_i, c_j)$ 
5:       if  $dist(x_i, c_j) < MeanDist(X)$  then
6:         assign  $x_i$  to the current cluster
7:       end if
8:     end for
9:   end for
10:  update the cluster centres
11: until Convergence criteria are met
12: end begin
```

---

### C. Different Variants of PFK-means

In order to fully explore the suggested heuristic, several variants of PFK-means have been proposed. These variants mainly focus on the initialization process applied with different approaches: overlapping PFK-means and hard PFK-means.

1) *Overlapping PFK-means variant:* In the initialization stage, each data object can belong to several clusters and thus the obtained distribution contains overlapping clusters. In that respect, there is one suggested solution with overlapping clusters.

In order to obtain the initial clusters and the number of clusters, the first variant of PFK-means consists of applying the initialization procedure, which is above-explained as a first stage. Thereafter, the second stage starts by browsing the achieved cluster centres and the whole data set and for each data object, calculates the distance between this data object and the current cluster centre based on the Euclidean distance. In the case where the distance value is less than the average distance of all data objects (equation 2), the data object being processed is added to the overlapping cluster which is being formed. After scanning the whole cluster centres, each cluster centre value is updated by calculating the mean value of all data objects belonging to its corresponding cluster. This iterative procedure is repeated until no changes occur on the cluster centres values. After the completion of this process, the data set processed is partitioned into  $k$  overlapping clusters. The algorithm 3 shows the details of this iterative procedure.

2) *The hard PFK-means version I:* This solution consists of applying the initialization process ((Algorithm 1) presented in the PFK-means heuristic as a first stage. Then, similarly to the steps explained on the iterative procedure (Algorithm 3) assign each data object to the appropriate cluster and in parallel remove the intersections between the constructed overlapping clusters. In other words, when the data object which is being processed is not clustered, it is added immediately to the cluster being formed. Otherwise, when the data object is already clustered, the distance between the current cluster centre and the data object is calculated then compared with

---

**Algorithm 3** The iterative procedure

---

**Input:** a set of  $n$  data objects  $X$ , the  $k$  initial cluster centres  $C, k$

**Output:** the data objects in  $X$  partitioned in  $k$  clusters  
**begin**

```
1: repeat
2:   for  $r \leftarrow 0$  to  $k$  do
3:     for  $i \leftarrow 0$  to  $|X|$  do
4:       calculate  $dist(x_i, c_r)$ 
5:       if  $dist(x_i, c_r) < MeanDist(X)$  then
6:         assign  $x_i$  to the current cluster
7:       end if
8:     end for
9:   end for
10:  update the cluster centres  $C$ 
11: until Convergence criteria are met
end begin
```

---

the distance between the same data object and the centre of the cluster containing this data object. In the case where the data object is most similar to the current cluster, it will be removed from the old cluster and added to the overlapping cluster being formed. Thus, the cluster centres are updated after each iteration by calculating the mean value of the data objects assigned to each cluster. The Algorithm 4 illustrates the steps of this hard iterative procedure.

---

**Algorithm 4** The hard iterative procedure

---

**Input:** a set of  $n$  data objects  $X$ , the  $k$  initial cluster centres  $C, k$

**Output:** the data objects in  $X$  partitioned in  $k$  clusters  
**begin**

```
1: repeat
2:   for  $r \leftarrow 0$  to  $k$  do
3:     for  $i \leftarrow 0$  to  $|X|$  do
4:       if  $x_i$  is not clustered then
5:         calculate  $dist(x_i, c_r)$ 
6:         if  $dist(x_i, c_r) < MeanDist(X)$  then
7:           assign  $x_i$  to the current cluster
8:         end if
9:       else if  $x_i$  is clustered in the cluster whose centre
10:      is  $c_m$  then
11:        calculate  $dist(x_i, c_r)$  and  $dist(x_i, c_m)$ 
12:        if  $dist(x_i, c_r) < dist(x_i, c_m)$  then
13:          add  $x_i$  to the current cluster, remove  $x_i$ 
14:          from the cluster represented by  $c_m$ 
15:        end if
16:      end if
17:    end for
18:  end for
19:  update the cluster centres  $C$ 
20: until Convergence criteria are met
end begin
```

---

3) *The hard PFK-means version II* : The process of this variant is similar to that of the first version of the hard PFK-means (Algorithm 1+ Algorithm 4), the only difference is that the last stage of this solution consists of applying the traditional k-means at the end of the process. In that regard, the

second version of the hard PFK-means consists of three major stages. The first stage aims to discover the initial clusters by applying the initialization phase as presented in the PFK-means (Algorithm 1). Then, the second stage consists of executing the hard iterative procedure as explained in the above variant (Algorithm 4). Finally, in the last stage, the traditional k-means is applied by taking the cluster centres and the number of clusters, obtained from the second stage, as input parameters (Algorithm 2).

4) *The hard PFK-means version III*: In a similar vein, this solution starts by applying the initialization stage (Algorithm 1). Secondly, it executes the iterative procedure (Algorithm 3). At last stage, it runs the traditional k-means algorithm taking as input settings the output parameters of the second stage, which are the initial cluster centres of the obtained overlapping clusters and the number of overlapping clusters automatically computed (Algorithm 2).

#### D. The E-transitive Heuristic Adapted to Quantitative Data

The E-transitive heuristic [2] is an improved version of the *Transitive* heuristic [22] which aims to cluster categorical data sets using the benefits of the Relational Analysis [23]. In fact, the principal purpose of this heuristic is to perform a clustering without specifying the number of clusters by adopting a specific cluster structure and then reduce the computational time. Thus, the E-transitive heuristic adapted to quantitative data consists of applying exclusively the initialization stage (Algorithm 1) presented in the PFK-means heuristic by removing intersections between the overlapping clusters. In that regard, the process is similar to that of the initialization stage, the only difference is that each data object must be checked before being added to the appropriate cluster. Thus, at the beginning of the process, all data objects are noted as not clustered and each data object added to a cluster is noted clustered. Accordingly, there are two possibilities. In the case where the data object being processed is not clustered, it will be added to the cluster being formed immediately. Otherwise, in the first step, the distance between the current cluster centre and the data object is calculated and then compared with the distance between the same data object and the centre of the cluster containing this data object. In the case where the data object is most similar to the current cluster, the data object will be removed from the old cluster and added to the overlapping cluster being formed. The cluster centres are updated after each modification. The Algorithm 5 presents the instructions of this solution.

## IV. EXPERIMENTS

This section provides the results obtained by implementing the PFK-means heuristic, its different variants, the E-transitive heuristic [2] adapted to quantitative data, and the traditional k-means [3] [4] using real-world data sets, retrieved from the UCI Machine Learning Repository [6]. In order to measure the clustering effect, these algorithms are evaluated based on the accuracy and the sum of squared errors described by equation 1. The experiments include also the simulation tests which have been performed to evaluate the performance of PFK-means heuristic in terms of running time with distinct synthetic data sets generated using a data mining generator, called weka [24].

**Algorithm 5** The E-transitive heuristic adapted to quantitative data

---

**Input:** A set of  $n$  data objects  $X$   
**Output:** The initial cluster centres  $T_{c_{next}}$ . The number of clusters automatically computed

---

**begin**

- 1: compute  $MeanDist(X)$  or  $MeanDist(SampleX)$
- 2: select the first cluster centre  $c_{new}$  randomly from  $X$
- 3: initialize  $Next \leftarrow true$
- 4:  $T_{c_{next}} \leftarrow null$
- 5: add  $c_{new}$  to  $T_{c_{next}}$
- 6: **while**  $Next$  **do**
- 7:      $c_{next} \leftarrow null$
- 8:     **for**  $i \leftarrow 0$  to  $|X|$  **do**
- 9:         calculate  $dist(x_i, c_{new})$
- 10:         **if**  $dist(x_i, c_{new}) < MeanDist(X)$  **then**
- 11:             **if**  $x_i$  is not clustered **then**
- 12:                 assign  $x_i$  to the current cluster
- 13:                 update the current cluster
- 14:             **else if**  $x_i$  is clustered in the cluster whose centre is  $c_m$  **then**
- 15:                 calculate  $dist(x_i, c_r)$  and  $dist(x_i, c_m)$
- 16:                 **if**  $dist(x_i, c_r) < dist(x_i, c_m)$  **then**
- 17:                     add  $x_i$  to the current cluster, remove  $x_i$  from the cluster represented by  $c_m$
- 18:                     update the current cluster and cluster represented by  $c_m$
- 19:                 **end if**
- 20:             **end if**
- 21:             **else if**  $c_{next}$  is null **then**
- 22:                  $c_{next} \leftarrow x_i$
- 23:             **else if**  $dist(x_i, c_{new}) > dist(c_{next}, c_{new})$  for all  $c_{next}$  in  $T_{c_{next}}$  **then**
- 24:                  $c_{next} \leftarrow x_i$
- 25:             **end if**
- 26:             **end for**
- 27:      $c_{new} \leftarrow c_{next}$
- 28:     add  $c_{new}$  to  $T_{c_{next}}$
- 29:     **if**  $c_{next}$  is null **then**
- 30:          $Next \leftarrow false$
- 31:     **end if**
- 32: **end while**

**end begin**

---

#### A. Data Sets Description

Table I gives a brave description of seven real-world data sets, retrieved from the UCI machine learning [6], used to evaluate the performance of the proposed heuristic, namely, Iris, Wine, Seeds, Pima Indian Diabetes, Soybean-small, Segmentation, Musk, and Letter-Recognition (LR). As shown in Table I, each data set is described by a specified number of clusters, many data objects, and each data object is described by a vector of attributes. The simulated data sets are generated by varying the size of the data sets, the number of clusters, and the number of attributes. Indeed, the first experiment consists of generating data sets with different sizes: 1000, 1500, 2000, 2500, 3000, 3500, and 4000. Each of these data sets is described by three clusters and five attributes. In the second experiment, the data set size is fixed at 1000, the number of attributes at 5, and the size of the cluster is varied

TABLE I. DESCRIPTION OF THE REAL-LIFE DATA SETS USED IN THE EXPERIMENTS.

data set	Data size	Attributes	Cluster number
Iris	150	4	3
Wine	178	13	3
Soybean-small	47	35	4
Pima Indian Diabetes	768	8	2
Seeds	210	7	3
Musk	6598	168	2
Letter-Recognition(LR)	20000	16	26

as follows: 2, 3, 4, 5, 6, 7, 8, 9, and 10. Finally, the last experiment use data sets with a different number of attributes: 5, 10, 15, 20, 25, 30, 35, 40, and fix the data set size and the number of clusters at 1000 and three respectively. Besides, two-dimensional synthetic data sets [25] were used for comparing the suggested heuristic and the iterative k-means minus-plus [5]. These data sets contain 5000 data points and 15 clusters: S1, S2, S3, and S4.

#### B. Clustering Evaluation Measures

Clustering validation is an important aspect to evaluate the quality of clustering results. Indeed, it depends on some parameters such as the similarity measure, the implementation of the clustering algorithm used, and the capacity to catch some or all of the hidden patterns. In order to measure the clustering effect of the proposed heuristic, the following parameters are involved: the time required for completing the procedure of clustering, the sum of squared errors (equation 1), the accuracy, and the entropy clustering measure.

#### C. Results on Real-world Data Sets

In order to evaluate the performance of the developed heuristic and its variants, these heuristics have been programmed using java. The results presented are the best values obtained from five runs for each proposed heuristic, except for the second version of the hard PFK-means which produces stable results. Concerning the traditional k-means algorithm, the initial centres were generated randomly. Table II provides the sum of squared errors for PFK-means, the E-transitive heuristic [2] adapted to quantitative data and its variants on real-world data sets. Clearly, the second version of the hard PFK-means exceeds the other proposed heuristics in terms of the sum of squared errors for all data sets except the soybean data set. In this case, the PFK-means and the second version of the hard PFK-means give the best results. The performance of the E-transitive heuristic comes back to the fact that this variant makes it possible to detect outliers. Absolutely, since in the iterative procedure applied as the second stage of this heuristic, the data objects which are very far from the cluster centres are not assigned imperatively to these clusters. Therefore, the E-transitive heuristic adapted to quantitative data provides the minimal values of SSE. Additionally, the second version of the hard PFK-means produces stable results. Finally, it should be noted that PFK-means and its variants lead to finding the right number of clusters for all tested data sets as described in Table IV. Furthermore, regarding the PFK-means heuristic and its hard variants, all inputs are clustered.

In the figures (Fig. 1, Fig. 2, Fig. 3), a comparison of the clustering results of PFK-means, the E-transitive heuristic

TABLE II. THE SUM OF SQUARED ERRORS OF THE CLUSTERING RESULTS ON REAL-WORLD DATA SETS.

data set	PFK-means	E-transitive	Hard PFK-means1	Hard PFK-means2	Hard PFK-means3
Iris	78.94	<b>76.46</b>	82.86	78.94	78.94
Soybean	<b>205.96</b>	207.49	220.05	207.49	207.05
Wine	2.63E+06	<b>2.31E+06</b>	2.97E+06	2.37E+06	2.37E+06
Pima	5.18E+06	<b>4.31E+06</b>	5.68E+06	5.12E+06	5.14E+06
Seeds	<b>587.31</b>	<b>587.31</b>	630.78	<b>587.31</b>	588.43

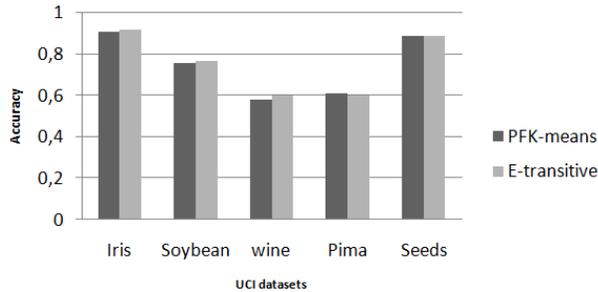


Fig. 1. The Accuracy of PFK-means and E-transitive on Real-world Data Sets.

adapted to quantitative data, its variants, and the traditional K-means on real-world data sets in term of accuracy is illustrated. Fig. 1 presents a comparison between the PFK-means and the E-transitive heuristic. Based on this result, it is clear that the accuracy of these heuristics is closed to each other. Moreover, Fig. 2 describes the accuracy of PFK-means and its variants for the above-mentioned real-world data sets. As can be seen, the accuracy of PFK-means and its variants are closed to each other for iris, Pima Indian Diabetes, seeds, and soybean data sets, yet for wine data set the second version of the hard PFK-means and the third version of the hard PFK-means outperform the PFK-means heuristic and the first version of the hard PFK-means. The last Fig. (3) describes the accuracy of the PFK-means heuristic and the k-means algorithm with UCI data sets [6]. From this figure, it can be shown that the PFK-means outperforms the k-means algorithm for Pima Indian Diabetes and seeds data set. However, for wine and soybean data sets, the k-means algorithm achieves an accuracy superior to the accuracy of PFK-means.

Table III presents a comparison between the PFK-means heuristic and the traditional k-means Algorithm [3] [4], in terms of a sum of squared errors, accuracy, and entropy measure based on real-world data sets. Regarding the sum of squared errors and the entropy clustering measure, the smaller their values, the better the result. The highest value provided by the entropy clustering measure is one while the lowest one is 0. The PFK-means heuristic exceeds the traditional k-means algorithm in terms of the sum of squared errors for all data sets except the Pima data set. Concerning the accuracy, the PFK-means heuristic gives the best results for Iris, Pima, and Seeds data sets. Furthermore, the values obtained by the entropy clustering measure are the best for the PFK-means heuristic. In addition to that since the suggested heuristic doesn't require the number of clusters as an input parameter, it shows important results compared to the traditional k-means. Thus, the results

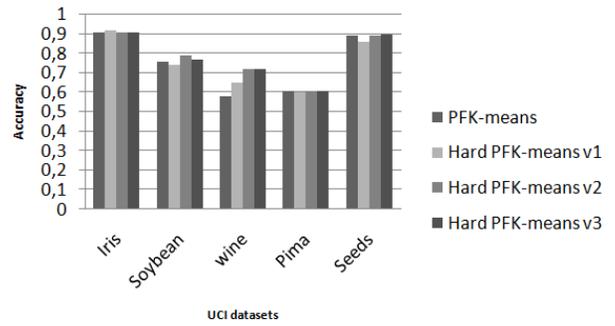


Fig. 2. The Accuracy of PFK-means and its Variants on Real-world Data Sets.

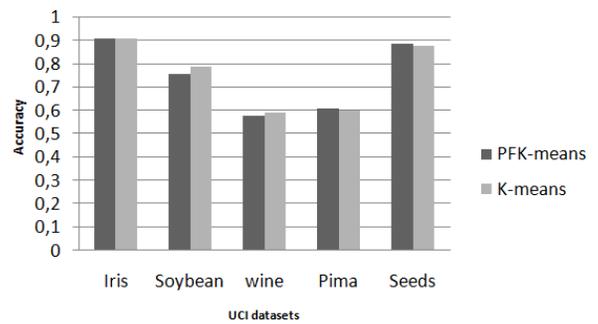


Fig. 3. The Accuracy of PFK-means and the Traditional k-means on Real-world Data Sets.

exposed in Table III demonstrate the efficiency of the PFK-means heuristic and its ability to find the appropriate number of clusters for all data sets. Table IV presents the number of clusters found after executing the PFK-means as well as the exact number of clusters for the real-world data sets used.

TABLE III. COMPARISON OF PFK-MEANS AND K-MEANS ON REAL-WORLD DATA SETS.

	K-means			PFK-means		
	SSE	Accuracy	Entropy	SSE	Accuracy	Entropy
Iris	78.94	0.91	0.39	78.94	0.91	0.39
Soybean	208.15	<b>0.79</b>	0.56	<b>205.96</b>	0.76	<b>0.55</b>
Wine	2.66E+06	<b>0.59</b>	0.98	<b>2.63E+06</b>	0.58	<b>0.95</b>
Pima	<b>5.13E+06</b>	0.60	0.91	5.18E+06	<b>0.61</b>	<b>0.77</b>
Seeds	593.50	0.88	0.46	<b>587.31</b>	<b>0.89</b>	<b>0.44</b>

TABLE IV. THE NUMBER OF CLUSTERS OBTAINED AFTER EXECUTING PFK-MEANS AND ITS VARIANTS.

data set	Exact Cluster number	Cluster number found
Iris	3	3
Wine	3	3
Soybean-small	4	4
Pima Indian Diabetes	2	2
Seeds	3	3
Musk	2	2
Letter-Recognition(LR)	26	26

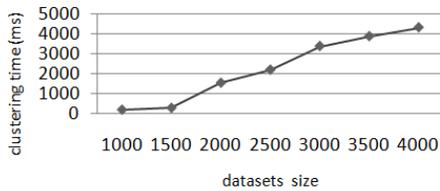


Fig. 4. Clustering Time of Synthetic Data Sets for Different Sizes.

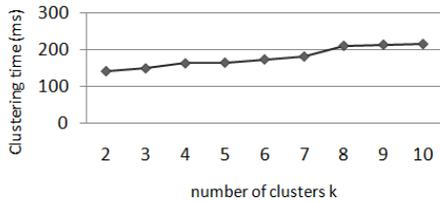


Fig. 5. Clustering Time of Synthetic Data Sets for Different Clusters.

#### D. Results on Synthetic Data Sets

For the purpose of testing the performance of the proposed heuristic in terms of processing time, different synthetic data sets were generated based on different clustering criteria namely, the size of the data sets, the number of clusters, and the number of attributes.

The first experiment (Fig. 4) describes the performance of the proposed heuristic when increasing the size of the data sets, which varies from 1000 to 4000 while setting the number of clusters at 3 and the number of attributes at 5. As shown in Fig. 4 the running times of the proposed heuristic vary from 188 to 4321 milliseconds which are nearly linear against the size of the data sets. The next experiment (Fig. 5) depicts the suggested heuristic behavior by increasing the number of clusters from 2 to 10 with the data set size set to 1000 instances and the number of attributes fixing to 5. It is clear from Fig. 5 that the clustering time scales linearly from 141 to 217 milliseconds while increasing the number of clusters. Additionally, the proposed heuristic can detect the adequate number of clusters of each generated data set. The last experiment (Fig. 6) illustrates the processing times in milliseconds while increasing the number of attributes from 5 to 40 with the number of clusters fixing to 3 and the size of the data set setting in 1000. This Fig. (6) shows clearly that the variation of the running times of the proposed heuristic from 169 to 489 milliseconds while increasing the number of attributes is quite linear.

#### E. Results of PFK-means Compared to the Iterative k-means Minus-plus

The PFK-means heuristic was compared to the iterative k-means minus-plus [5], which is an iterative approach to improve the quality of the k-means algorithm by removing one cluster (minus), dividing another one (plus), and applying re-clustering again, for each iteration. The results of the iterative k-means minus-plus and the traditional k-means were presented as in the original paper describing the iterative k-means [5]. Table V presents a comparison between the PFK-

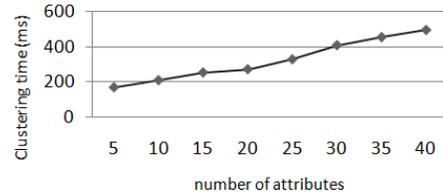


Fig. 6. Clustering Time of Synthetic Data Sets by Varying the Number of Attributes.

TABLE V. COMPARISON OF PFK-MEANS, THE ITERATIVE K-MEANS-+, AND THE K-MEANS ALGORITHM ON DIFFERENT DATA SETS.

	maximum of partial SSE			SSE		
	KM	IKM-+	PFKmeans	KM	IKM-+	PFKmeans
Iris	6.53E+01	3.98E+01	3.98E+01	9.95E+01	7.89E+01	7.89E+01
Musk	4.61E+09	4.35E+09	4.35E+09	6.09E+09	5.92E+09	5.92E+09
LR	4.17E+04	3.93E+04	3.93E+04	6.20E+05	6.16E+05	6.16E+05
S1	6.59E+12	8.54E+11	8.54E+11	1.85E+13	8.92E+12	8.91E+12
S2	5.78E+12	1.33E+12	1.33E+12	2.01E+13	1.33E+13	1.32E+13
S3	3.41E+12	1.56E+12	2.97E+12	1.94E+13	1.69E+13	2.06E+13
S4	2.56E+12	1.79E+12	2.77E+12	1.70E+13	1.57E+13	1.98E+13

means heuristic, the iterative k-means minus-plus, and the traditional k-means algorithm, in terms of a sum of squared errors, and maximum of partial SSE for three real-world data sets and four synthetic data sets. The PFK-means heuristic and the iterative k-means minus-plus algorithm outperforms the traditional k-means, except for S3 and S4 data sets when the iterative k-means -+ outperforms the proposed heuristic.

#### V. CONCLUSIONS AND PERSPECTIVES

The purpose of this research is to present a new clustering algorithm namely a parameter-free clustering algorithm based on k-means. This hybrid solution combines the E-transitive heuristic adapted to quantitative data and the k-means algorithm to deal with the major issue encountered with k-means, which is the determination of the number of clusters and the initial cluster centres. The PFK-means and its variants were explained according to the clustering approaches. Also, this paper covers a detailed comparison between the PFK-means heuristic, its different variants, the revisited version of the E-transitive heuristic, the iterative k-means minus-plus, and the k-means algorithm in terms of the sum of squared errors and accuracy.

From the experiments that have been conducted on real-world data sets, it has been proven that the suggested heuristics can to detect the appropriate number of clusters independently of any initial conditions. Accordingly, these heuristics can be successfully used for unsupervised learning. Furthermore, the examination conducted on synthetic data sets demonstrates that the proposed heuristic finds the appropriate number of clusters in reasonable processing time against the variation of the size of the data sets, the number of clusters, and the number of attributes. In future work, we will be concentrating on clustering big data using the parallel programming [26] to improve the efficiency and the complexity of the proposed heuristic. Additionally, we will focus on the implementation

of the proposed heuristic using other similarity measures.

#### REFERENCES

- [1] J. Han, J. Pei, and M. Kamber, *Data mining: concepts and techniques*. Elsevier, 2011.
- [2] S. C. Slaoui, Z. Dafir, and Y. Lamari, "E-transitive: an enhanced version of the transitive heuristic for clustering categorical data," *Procedia Computer Science*, vol. 127, pp. 26–34, 2018.
- [3] J. MacQueen *et al.*, "Some methods for classification and analysis of multivariate observations," in *Proceedings of the fifth Berkeley symposium on mathematical statistics and probability*, vol. 1, no. 14. Oakland, CA, USA, 1967, pp. 281–297.
- [4] S. Lloyd, "Least squares quantization in pcm," *IEEE transactions on information theory*, vol. 28, no. 2, pp. 129–137, 1982.
- [5] H. Ismkhan, "Ik-means+: An iterative clustering algorithm based on an enhanced version of the k-means," *Pattern Recognition*, vol. 79, pp. 402–413, 2018.
- [6] A. Asuncion and D. Newman, "Uci machine learning repository," 2007.
- [7] P. Berkhin, "A survey of clustering data mining techniques," in *Grouping multidimensional data*. Springer, 2006, pp. 25–71.
- [8] L. Rokach, "A survey of clustering algorithms," in *Data mining and knowledge discovery handbook*. Springer, 2009, pp. 269–298.
- [9] A. K. Jain, "Data clustering: 50 years beyond k-means," *Pattern recognition letters*, vol. 31, no. 8, pp. 651–666, 2010.
- [10] H. Zhang, T. W. Chow, and Q. J. Wu, "Organizing books and authors by multilayer som," *IEEE transactions on neural networks and learning systems*, vol. 27, no. 12, pp. 2537–2550, 2015.
- [11] H. Zhang, S. Wang, X. Xu, T. W. Chow, and Q. J. Wu, "Tree2vector: learning a vectorial representation for tree-structured data," *IEEE transactions on neural networks and learning systems*, no. 99, pp. 1–15, 2018.
- [12] S. S. Khan and A. Ahmad, "Cluster center initialization algorithm for k-means clustering," *Pattern recognition letters*, vol. 25, no. 11, pp. 1293–1302, 2004.
- [13] A. Likas, N. Vlassis, and J. J. Verbeek, "The global k-means clustering algorithm," *Pattern recognition*, vol. 36, no. 2, pp. 451–461, 2003.
- [14] D. Arthur and S. Vassilvitskii, "k-means++: The advantages of careful seeding," in *Proceedings of the eighteenth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, 2007, pp. 1027–1035.
- [15] A. M. Bagirov, "Modified global k-means algorithm for minimum sum-of-squares clustering problems," *Pattern Recognition*, vol. 41, no. 10, pp. 3192–3199, 2008.
- [16] M. E. Celebi, H. A. Kingravi, and P. A. Vela, "A comparative study of efficient initialization methods for the k-means clustering algorithm," *Expert systems with applications*, vol. 40, no. 1, pp. 200–210, 2013.
- [17] G. Zhang, C. Zhang, and H. Zhang, "Improved k-means algorithm based on density canopy," *Knowledge-based systems*, vol. 145, pp. 289–297, 2018.
- [18] K. Chowdhury, D. Chaudhuri, and A. K. Pal, "An entropy-based initialization method of k-means clustering on the optimal number of clusters," *Neural Computing and Applications*, pp. 1–18, 2020.
- [19] S. Xia, D. Peng, D. Meng, C. Zhang, G. Wang, E. Giem, W. Wei, and Z. Chen, "A fast adaptive k-means with no bounds," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020.
- [20] S. Wang, X. Liu, and L. Xiang, "An improved initialisation method for k-means algorithm optimised by tissue-like p system," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 36, no. 1, pp. 3–10, 2021.
- [21] A. Torrente and J. Romo, "Initializing k-means clustering by bootstrap and data depth," *Journal of Classification*, pp. 1–25, 2020.
- [22] S. C. Slaoui and Y. Lamari, "Clustering of large data based on the relational analysis," in *2015 Intelligent Systems and Computer Vision (ISCV)*. IEEE, 2015, pp. 1–7.
- [23] J. Ah-Pine and J.-F. Marcotorchino, "Overview of the relational analysis approach in data-mining and multi-criteria decision making," in *Web intelligence and intelligent agents*. IntechOpen, 2010.
- [24] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The weka data mining software: an update," *ACM SIGKDD explorations newsletter*, vol. 11, no. 1, pp. 10–18, 2009.
- [25] P. Fränti and S. Sieranoja, "K-means properties on six clustering benchmark datasets (2018)," URL: <http://cs.uef.fi/sipu/datasets>.
- [26] Z. Dafir, Y. Lamari, and S. C. Slaoui, "A survey on parallel clustering algorithms for big data," *Artificial Intelligence Review*, pp. 1–33, 2020.

# Arabic Tweets Sentiment Analysis about Online Learning during COVID-19 in Saudi Arabia

Asma Althagafi<sup>1</sup>, Ghofran Althobaiti<sup>2</sup>, Hosam Alhakami<sup>3</sup>, Tahani Alsubait<sup>4</sup>  
College of Computer and Information Systems  
Umm Al-Qura University  
Makkah, Saudi Arabia

**Abstract**—The COVID-19 pandemic can be considered as the greatest challenge of our time and is defining and reshaping many aspects of our life such as learning and teaching, especially in the academic year of 2020. While some people could adapt quickly to online learning, others consider it to be inefficient. The re-opening of schools and universities is currently under consideration. However, many experts in many countries suggested that at least one semester should be online, during the pandemic. Understanding the public's emotional reaction to online learning has become significant. This paper studies the attitude of people of Saudi Arabia towards online learning. We have used a collection of Arabic tweets posted in 2020, collected mainly via hashtags that originated in Saudi Arabia. Our sentiment analysis has shown that people have maintained a neutral response to online learning. This study will allow scholars and decision makers to understand the emotional effects of online learning on communities.

**Keywords**—Social media analytics; sentiment analysis; online learning; Arabic tweets

## I. INTRODUCTION

The COVID-19 pandemic has pushed educators towards adopting online learning, starting from the academic year 2020. Looking back at history, the COVID-19 CORONA virus was discovered in the last month of 2019, in Wuhan of China. In March 2020, the Director General of the World Health Organization (WHO)<sup>1</sup> announced COVID-19 as a pandemic, after evaluating the accelerated dissemination and magnitude of the lethal virus across the globe, with an additional declaration of social distancing as a way of halting the spread of the pandemic. This pandemic has prompted a worldwide physical shutdown of businesses, sporting events and schools by forcing all institutions to switch to online channels. As a result, pupils cannot attend schools or institutions physically. Around the same time, though, they need to learn to deal with this condition and to continue their studies. While some people could adapt quickly, others considered it to be inefficient. The re-opening of schools and universities is currently under consideration. However, most experts suggested that at least one semester should be online. So, in this research we explore what people think about online learning via exploring tweets related to online learning to understand people's opinions and attitudes.

People openly share their thoughts and views in no more than 280-characters tweets, making Twitter one of the most popular social networking sites in the world. In this research,

we focus on sentiment analysis of people's posts in Twitter. We argue that tweeting is a good way of raising public opinion about online learning, as the platform is widespread in Saudi Arabia.

At present, sentiment analysis or opinion mining has been considered to be one of the most emerging fields of study sparked by social networks. Sentiment analysis is the job of recognizing optimistic and negative views, feelings, and evaluations. The aim of sentiment analysis is to decide a writer's attitude to some subject or the overall document's tonality [1]. The purpose of Sentiment Analysis is to find views, define the conveyed emotions, then describe their polarity [2]. Sentiment analysis can be conducted at several levels: document level, sentence level and subject level [3]. In this research, we are interested in the sentence level sentiment analysis of Arabic tweets to assess the tweet polarity; whether it is positive, negative or neutral. We are interested in sentiment classification in the Arabic language at the sentence level in which the aim is to classify tweets about online learning in Saudi Arabia to determine people's opinions related to this topic and classify the tweets to positive, negative or neutral.

The remainder of this article is arranged as follows: Section II presents a background to Sentiment Analysis in Arabic. Section III introduces related work. Section IV introduces methods and materials used in this research. Section V exposes our results and discussions. Finally, Section VI lays forth the conclusion and future work.

## II. BACKGROUND

### A. Sentiment Analysis in the Arabic Language

In recent years, social media sentiment analysis has become a hot subject for opinion mining in many social networking applications [4]. Sentiment analysis-based opinion mining may be done by evaluating a subject's feelings and actions about an occurrence or a particular subject. Arabic sentiment analysis is one of the most challenging social media sentiment analysis techniques, owing to the casual noisy content and the rich morphology of the Arabic language. The Arabic opinion analysis approaches are gaining more popularity and significance by rising the rate of feedback and comments by Arabic users on numerous social media platforms [5]. Arabic is a Semitic language that is spoken in the Middle East and North Africa by more than 250 million individuals. It is one of the United States' six official dialects and the language of the Holy Quran. It is additionally the language that a portion of the world's most

<sup>1</sup><https://www.who.int/en>

prominent scholarly, science and chronicled works have been written in. There are three principle types of Arabic [6]:

- 1) Classic Arabic (CA)  
That is the kind of Arabic that the Mushaf (Holy Quran) is written in. The grammar of today's Arabic is significantly different, as Mushaf was written in the 6th century CE. CA is based on the medieval dialects of Arab tribes.  
CA special symbols are used to indicate proper pronunciation and to deliver words. Such written Arabic symbols are almost exclusively found in the Quran or alrecitation [7].
- 2) Modern Standard Arabic (MSA)  
In today's Arabic-speaking countries, it is the most common form of Arabic used. In virtually every media medium, MSA is used in TV, documentaries, papers, and radio broadcasts. Most written papers in seminars and politicians' speeches are in the MSA [6].
- 3) Colloquial Arabic (Arabic)  
It is the Arabic dialect unique to each region, the Arabic language that is utilized to communicate thoughts fundamentally in the WWW, generally in sites, discussions, and conversational posts. While much of its vocabulary and grammatical origins come from the MSA, it still incorporates its own lexicon [6].

### B. Challenges of using Arabic Language in Sentiment Analysis

There are many challenges facing Arabic, some of which are particular to the sentiment analysis activities, and the rest are due to the complexities of the Arabic language. A big challenge is the unavailability of colloquial Arabic sentiment lexicons and the limited availability of MSA lexicons, relative to those constructed in the English language, while most people in social Media platforms use colloquial Arabic to write their opinions and feelings [8]. The use of Latin characters to represent Arabic words is a recent social media theme, which is referred to as Arabizi. Arabic social media users often prefer to switch languages in their writings between Arabic and English, making it impossible to detect whether a phrase written with Latin characters is Arabizi or English [8]. Sarcasm is a kind of speech act in which there's something good a person says when something negative is actually meant, or vice versa [9]. Sarcasm is very difficult to detect, with just a few attempts in English for sarcasm detection using supervised and semi-supervised approaches to learning [9]. No research that deals with sarcasm identification has been found in Arabic sentiment analysis, to the best of our knowledge.

### III. RELATED WORK

Since people and consumers express their thoughts and feelings more freely than ever before, sentiment analysis is becoming an important method for tracking and understanding these feelings. A lot of research has been done on developing methods of sentiment analysis and defining the process of detecting sentiment for different languages around the world.

Heikal et al. [3] examine sentiment analysis of Arabic tweets utilizing Deep Learning. They utilized a troupe model

for investigation. The complexity of the Arabic language has urged them to investigate diverse profound learning models that have not examined to improve the accuracy of Arabic language examination. They use a mix of Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) models. They applied the model to a collection of Arabic tweets. The model accomplishes a 64.46% F1 score, which surpasses the F1 score of the cutting edge profound learning model fusing Convolutionary Neural Network (CNN) and Long Short-Term Memory (LSTM) models, to anticipate a 53.6% inclination on the Arabic Sentiment Tweets Dataset (ASTD).

Aldayel and Azmi [10] present a further investigation on the subject of getting the feeling from Arabic tweets with an attention on those starting in Saudi Arabia. There are numerous hindrances to the act of utilizing dialectical Arabic in tweets; the engendering of spelling mistakes; and the enormous variety of Twitter spaces, to name a few. To depict the extremity of Arabic tweets, they propose a cross breed arrangement that mixes semantic direction with an AI approach. A lexical classifier is utilized to characterize tweets in a solo manner, for example to manage plain tweets, and the SVM classifier further fortifies the result of the lexical classifier. The tests demonstrate that neither the lexical nor SVM classifiers will get the impact of the half breed approach. The normal execution of the crossover classifier regarding F-estimation and accuracy is 84.01% and 84.01% separately, respectively.

Duwairi et al. [11] present another study on Arabic tweets, discussing sentiment analysis. About 350,000 tweets have been collected for this purpose. In order to label 25000+ tweets, crowd sourcing was used. A label like Positive, Negative or Neutral is assigned to each tweet. Majority voting was used with every tweet to determine the final label. There are many novel contributions to this work, such as managing negations, Arabizi and Arabic dialects. The system was tested using three built-in classifiers in Rapid miner. The results obtained are promising.

Zhou et al. [12] present a study about a Tweets Sentiment Analysis Model (TSAM). Their research has shown that it is feasible and can be very useful to develop an intelligent lexicon-based sentiment analysis framework. However the opinion analysis method, in its current form, has not yet achieved its full potential. A variety of study problems must be worked out in order to boost the existing TSAM, such as distinguishing between parts of speech. The opinion terms are extracted in the current model as the features. The accuracy of the part of speech tagging has been found to affect the overall sentiment ratings. Therefore to enhance the existing technique, advanced NLP methods must be implemented. Taking into account the study of emotions, the method identifies positive and negative thoughts, experiences and feelings. It measures a person's feeling in the sense of positivity or negativity. However, the study of text emotions moves beyond the positive-negative dimension to the discreet forms of emotions such as joy, sadness, etc. Moreover, text-based mood analysis, such as text grouping and clustering, poses numerous obstacles beyond conventional text analysis. With the analysis carried out above, the TSAM model will yield even more accurate performance, with the use of more specific entity recognition approaches.

Larkey et al. [13] present one more examination utilizing

an assortment of word references that store positive, negative and neutral roots. A stemmer was used to translate words into roots in order to evaluate the sentiment or class of a sentence. On the chance that the subsequent root shows up in the positive/negative/neutral root word reference, it is called positive/negative/impartial. In the event that the word isn't in the word reference, the user is asked to choose its extremity and afterward to add its source to the relating word reference.

#### A. Comparison of Related Work

Overall, we reviewed several recent studies highly related to ours. Some of these studies, as shown in Table I, applied Sentiment Analysis on tweets to extract the sentiments by using many methods, as we detail in the table.

TABLE I. COMPARISON OF RELATED WORK

Studies	Main Method	Accuracy%
Heikal et al. [3]	Convolutional Neural Network(CNN)	64.46%
Heikal et al. [3]	Long Short-Term Memory(LSTM)	53.6%
Aldayel et al. [10]	Support Vector Machines (SVM)	84.01%

### IV. METHODOLOGY

#### A. Tweets Extraction

Firstly, we got a Twitter Developer Account<sup>2</sup> that helps you to access the Twitter API. By using our API information we collected tweets in Arabic only related to online learning. We searched for the following hashtags in the tweets:

- #التعليم\_عن\_بعد (Online teaching)
- #الدراسة\_عن\_بعد (Online learning)
- #البلاكبورد (Blackboard)
- #تيمز (Teams)
- #التعليم\_الالكتروني (E-Learning)

And the keywords that follow:

- التعليم عن بعد (Online teaching)
- الدراسة عن بعد (Online learning)
- البلاكبورد (Blackboard)
- تيمز (Teams)
- التعليم الالكتروني (E-Learning)

By using the get\_tweets function, we got 10445 tweets that also include venue, username, retweet count, favorite count, and time of tweet.

#### B. Data Pre-Processing

The first stage of pre-processing is getting rid of duplicate tweets. There were 2269 duplicate tweets, so the number of tweets was decreased to 8176. Then, we need to get rid of stop words, punctuation, hashtags, comparisons, links, and one or two-letter words as follow:

- Tokenize tweets into words and punctuation marks. The sentence "البلاكبورد اليوم معلق." can be tokenized like ["البلاكبورد", "اليوم", "معلق.", "."]
- Remove URLs from tweets because the URLs are pointed to extra information that was not a prerequisite for sentiment analysis in our approach. We also removed numbers, punctuation marks and extra white spaces because they do not contain emotions.
- Remove stop words. Removing stop words from text helps to recognize the most relevant words. Here we delete terms like: (who, whom, whose, not) الذي, التي, التي, الذي, ليس and الذين, by using the stop words from the nltk library.
- Finally we apply stemming which is a natural language processing technique that solves the issue of vocabulary mismatch [14] and keeps only the origin of each word.

#### C. Sentiment Analysis

Once the tweets were pre-processed, the second stage is sentiment analysis. In this step, we can focus on our main aim in this project which is to measure sentimental characteristics of tweets, such as polarity and subjectivity, using TextBlob<sup>3</sup>. Polarity is a variation in value between '-1' and '1'. It shows us how positive or negative the statement is. Subjectivity is another difference of value between '0' and '1' which shows whether the statement is an opinion or statement. Textblob comes with the core features of natural-language processing essentials; this approach classifies the polarity of textual data in positive, neutral and negative groups as '1', '0' and '-1'. We divided sentiments into three groups, namely positive, negative and neutral, based on their polarity, as seen in Table II.

TABLE II. POLARITY CLASSIFICATION

Value of Polarity	Sentiment
>0	Positive
0	Neutral
<0	Negative

#### D. Evaluation

To evaluate our results, we split our data into 80% train and 20% test sets. To classify the texts, a variety of machine learning algorithms have been implemented. We used the Naive Bayes, Random Forest and K-nearest neighbor Classifiers.

<sup>2</sup><https://developer.twitter.com/en>

<sup>3</sup><https://textblob.readthedocs.io/en/dev/>

Naive Bayes is a simple but fast classification algorithm. It is a commonly used algorithm for classifying documents [15]. Multinomial classifier Naive Bayes is widely used in the case of text categorization. It depends on three assumptions: documents are generated by a mixture model, between each mixture component and class there is a one-to-one correspondence, and each mixture component is a multinomial distribution of terms [16]. Theorem of Bayes offers a way to measure the posterior likelihood by equation 1.

$$P(c | x) = \frac{P(x | c)P(c)}{P(x)} \quad (1)$$

Where:

- $P(c | x)$  is the posterior probability of the attribute given by the class.
- $P(c)$  is a prior probability of class.
- $P(x)$  is a prior probability of attribute.
- $P(x | c)$  is the probability of attribute given class.

Random Forest (RF) classifiers excel in a number of automated sorting functions, such as categorization and emotion analysis. It is ideal for treating high dimensional noise data in text classification [17]. The phases of the Random Forest algorithm are as follows: The first step is to conclude that  $n$  samples and  $T$  classification attributes are found in the training set.  $N$  samples are collected using the bootstrap sampling process to get a new sample collection. In the second step, the  $t(T \leq t)$  attributes are selected at random from the  $t$  attributes given. The optimal classification node is chosen by using the optimal feature norm of a decision tree such that all the sub samples are leaf nodes. Repeat the second step of  $K$  in the third step, create  $K$  decision trees, and get the final random forest. In the fourth step, the function model of the classifier is  $H(x)$ , the decision tree is  $h_i$ , the classification label is  $y$ , and the indicator function is  $I(h_i(x) = Y)$ . The random-forest decision-making formula is as equation 2 [18]:

$$H(x) = \operatorname{argmax} \sum_{i=1}^k I(h_i(x) = Y) \quad (2)$$

K-nearest neighbor (KNN) is a standard example based classifier that does not make a clear, declarative description of the category, but depends on the category labels attached to the training documents identical to the test text [19]. KNN is classified by a majority vote of its neighbors, with the case assigned to the most common class of its nearest K-neighbors, determined by a distance function in equation 3. For  $K = 1$ , the case is simply assigned to the class of its closest neighbor.

$$\sqrt{\sum_{i=1}^k (X_i - Y_i)^2} \quad (3)$$

## V. RESULTS AND DISCUSSIONS

To have a better understanding of the public opinion towards online learning, we studied the sentiment people expressed in social media in the first academic term of 2020 in Saudi Arabia by tweets in the Twitter platform. We got the

results as Fig. 1 shows. That most tweets were expressing a neutral sentiment that might have happened because most of the tweets contained sentences that do not express negative, or positive emotions, the rest are due to the complexities of the Arabic language, such as having no sentiment lexicon available for colloquial Arabic, while MSA lexicons are limited relative to those constructed for the English language, and most peoples in social Media platforms use colloquial Arabic to write their opinions and feelings.

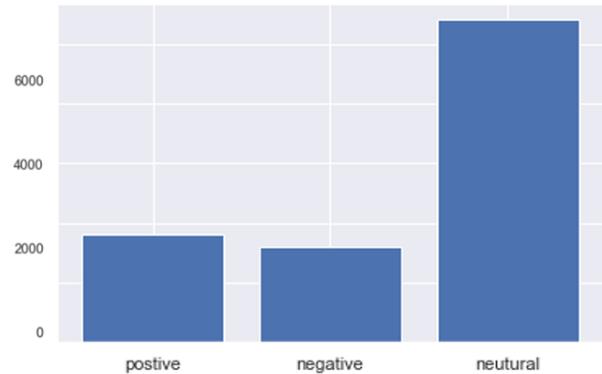


Fig. 1. Distribution of Sentiment.

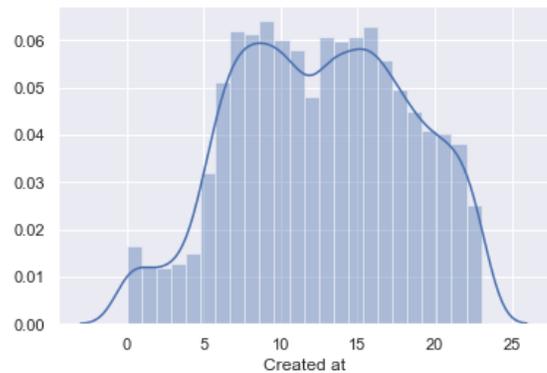


Fig. 2. Hourly Distribution of Tweets.

We also obtained the hourly distribution of tweets as shown in Fig. 2. We can see that the amount of tweets during the day is increased in the period from 6am until 3pm. This period has the most activity because these times are the times of lectures and courses for students in Saudi Arabia.

Moreover, after using TextBlob we can get words clouds for each label. Let us look at the positive and negative tweets words as seen in Fig. 3 and 4. Apparently, in negative words, people whose tweets are negative finds online learning tedious, terrible, and stressful. On the other hand, some positive people prefer online learning opportunities.

To evaluate our results the algorithm performance review experimental environment is supported by the Windows 10 operating system, Intel(R) Core(TM) i7-4710HQ CPU 2.50

## VI. CONCLUSION

Our research was centered on Twitter's opinion mining and sentiment analysis about online learning during COVID-19 pandemic, which bifurcates tweets based on three categories: positive, negative and neutral. Our goal was to get a better understanding of the feelings and opinions of tweeters about online learning. To do so, we collected about 10445 tweets. After that we applied sentiment analysis to these tweets and measured sentimental characteristics of tweets, such as polarity and subjectivity, using TextBlob. We got that most tweets were expressing a neutral sentiment, that might have happened because most of the tweets contained sentences that does not express negative nor positive emotions. One of the key challenges, however, is the lack of resources to be able to analyze the Arabic language, especially that each country has different colloquial Arabic. As for future work, we plan to understand people's attitudes towards different platforms of online learning via sentiment analysis of the feelings shared by the public about these platforms.



Fig. 3. Positive WordCloud.



Fig. 4. Negative WordCloud.

GHz cpu and 16.0 GB memory as support for the whole experiment and we used Python as the language of programming. We used a machine learning model by Naive Bayes, RF and KNN Classifiers. We split our data into 80% train and 20% test sets. We got 77% of Naive Bayes, 84% of RF and 67% of KNN Classifier.

The comparison of Naive Bayes, RF and KNN classifiers for multi-class text classification is also presented in this research. The findings indicate that the RF multi-class classification method achieved the highest classification accuracy in comparison with Naive Bayes and KNN classifiers because it works well with high-dimensional data such as a text classification compared to the other classifiers model.

## REFERENCES

- [1] A. Shouky and A. Rafea, "Sentence-level arabic sentiment analysis," in *2012 International Conference on Collaboration Technologies and Systems (CTS)*, pp. 546–550, 2012.
- [2] W. Medhat, A. Hassan, and H. Korashy, "Sentiment analysis algorithms and applications: A survey," *Ain Shams engineering journal*, vol. 5, no. 4, pp. 1093–1113, 2014.
- [3] M. Heikal, M. Torki, and N. El-Makky, "Sentiment analysis of arabic tweets using deep learning," *Procedia Computer Science*, vol. 142, pp. 114–122, 2018.
- [4] S. Ahmad, M. Z. Asghar, F. M. Alotaibi, and I. Awan, "Detection and classification of social media-based extremist affiliations using sentiment analysis techniques," *Human-centric Computing and Information Sciences*, vol. 9, no. 1, p. 24, 2019.
- [5] H. AlSalman, "An improved approach for sentiment analysis of arabic tweets in twitter social media," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1–4, IEEE, 2020.
- [6] 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*, 2020.
- [7] A. A. Khrisat and Z. A. Alharthy, "Arabic dialects and classical arabic language," *Advances in Social Sciences Research Journal*, vol. 2, no. 3, 2015.
- [8] N. Al-Twairsh, H. Al-Khalifa, and A. Al-Salman, "Subjectivity and sentiment analysis of arabic: trends and challenges," in *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, pp. 148–155, IEEE, 2014.
- [9] B. Liu, "Sentiment analysis and opinion mining," *Synthesis lectures on human language technologies*, vol. 5, no. 1, pp. 1–167, 2012.
- [10] H. K. Aldayel and A. M. Azmi, "Arabic tweets sentiment analysis—a hybrid scheme," *Journal of Information Science*, vol. 42, no. 6, pp. 782–797, 2016.
- [11] R. M. Duwairi, R. Marji, N. Sha'ban, and S. Rushaidat, "Sentiment analysis in arabic tweets," in *2014 5th International Conference on Information and Communication Systems (ICICS)*, pp. 1–6, IEEE, 2014.
- [12] X. Zhou, X. Tao, J. Yong, and Z. Yang, "Sentiment analysis on tweets for social events," in *Proceedings of the 2013 IEEE 17th international conference on computer supported cooperative work in design (CSCWD)*, pp. 557–562, IEEE, 2013.
- [13] N. Farra, E. Challita, R. Abou Assi, and H. Hajj, "Sentence-level and document-level sentiment mining for arabic texts," in *2010 IEEE international conference on data mining workshops*, pp. 1114–1119, IEEE, 2010.

- [14] L. S. Larkey, L. Ballesteros, and M. E. Connell, "Improving stemming for arabic information retrieval: light stemming and co-occurrence analysis," in *Proceedings of the 25th annual international ACM SIGIR conference on Research and development in information retrieval*, pp. 275–282, 2002.
- [15] P. Melville, W. Gryc, and R. D. Lawrence, "Sentiment analysis of blogs by combining lexical knowledge with text classification," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 1275–1284, 2009.
- [16] K. P. Nigam, "Using unlabeled data to improve text classification," tech. rep., CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE, 2001.
- [17] T. Salles, L. Rocha, and M. Gonçalves, "A bias-variance analysis of state-of-the-art random forest text classifiers," *Advances in Data Analysis and Classification*, pp. 1–27, 2020.
- [18] Y. Sun, Y. Li, Q. Zeng, and Y. Bian, "Application research of text classification based on random forest algorithm," in *2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE)*, pp. 370–374, IEEE, 2020.
- [19] S. Tan and J. Zhang, "An empirical study of sentiment analysis for chinese documents," *Expert Systems with applications*, vol. 34, no. 4, pp. 2622–2629, 2008.

# A Framework for Data Research in GIS Database using Meshing Techniques and the Map-Reduce Algorithm

Abdoulaye SERE<sup>1</sup>, Jean Serge Dimitri OUATTARA<sup>2</sup>, Didier BASSOLE<sup>3</sup>,  
José Arthur OUEDRAOGO<sup>4</sup>, Moubaric KABORE<sup>5</sup>

Network of Computer Science Teachers  
and Scientists of Faso

Bobo-Dioulasso, Burkina Faso

**Abstract**—Everywhere, centers, laboratories, hospital and pharmacy have faced many challenges to delivery quality of health service due to constraints related to limited availability of resources such as drugs, places, equipments and specialists, often in health deficit with increasing number of patients, for instance during COVID-19 pandemic. Late information on these constraints from health service centers will play negatively on service quality because of time delayed between requesting service on place and the response to delivery safe service. All these problems don't strengthen prevention or fighting against diseases in a region. This paper proposes a data research framework in a NoSQL database based on GIS data, containing an abstract table that could be inherited or specialized to any adopted GIS solution leading to a central data management instead of installing several database sites. The central database accepts data updated in back office by data owner and allows data research based on meshing Techniques and the map-reduce algorithm in front office. Variant meshing techniques have been presented to clustering GIS data with associated definitions of the content of map-reduce in order to improve processing time. In application in health service, the experimental results reveal that this system contributes to improve drug management in pharmacies and could be also used in others fields such as Finance, Education and Shopping through agencies spread over the territory, to strengthen national information systems and harmonised data.

**Keywords**—Map-reduce; big data; digital health; classification; Geographic Information System (GIS); COVID-19; Spark; MongoDB; NewSQL; NoSQL

## I. INTRODUCTION

The Sustainable Development Goals (SDG) reaffirm international commitment to achieve Universal Health Coverage (UHC) by 2030. The quality of health services is a global imperative in view universal health coverage, according to World Health Organization (WHO) in [12] and OCDE in [13]. Thus, a framework to measure quality of health service has been proposed by Arah, and others in [14]. Quality of Health Services provided by Hospital, pharmacies, Health Centers has played essential roles in fighting and prevention of diseases.

Health centers, Governments have faced many challenges due to many constraints related to availability of resources such as specialists, equipments, places, drugs during diseases. Among the need of human capacity building, materials for radiography contribute to improve Health services. For instance, according to Abdulrahman M. Qahtani and others in

[11], since the beginning of the COVID-19 in 2019, WHO also faced many challenges in increasing the global healthcare and Hygiene awareness to overcome COVID-19 pandemic. Thus, the needing of noze cover and washing hands regularly have been strongly recommended by Governments to prevent the COVID-19 disease.

The question is why going to a saturated clinic for health care and leaves others unsaturated. Information on available resources from Health centers might be opened somewhere and should indicate to patients, the way to follow in order to take the best decisions related to safe health. That will reduce forward death rate.

Today's technologies indicate the scale and speed at which technology is transforming traditional socio-economic sectors such as Health to reach digital Health.

Thus, digital transformation through software based on processing data related to Health has been proposed by engineers and scientists. For instance, applications based on disease diagnostic have contributed to support specialists in disease research.

Classification techniques are used in Big Data to identify groups in order to accelerate data processing and to take best decisions in smart system.

In classification, criteria can be taken into account to have data in the same groups. In Machine Learning, classification techniques such as supervised classification or not supervised classification, support Vector Machine (SVM), Decision Tree, Fuzzy Classification, Multi-Label Classification [1] could be used to establish relations between data.

Many techniques of tiling a space have been also developed by scientists to obtain cells in different grids such as Voronoi diagrams, Triangulation Delaunay, quasi-affine transformations, presented in [2], [3] and [15]. Fortune's algorithm also gives a way to build voronoi diagrams with a given set of continuous points. All these methods allows to get either regular grids or irregular grids in the image space, leading to data classification.

In a regular grid, each cell has the same geometric shape and the same size while in the irregular grid, the cells have different sizes or shapes. For instance, Vacavant's thesis in [4] presents different techniques of mesh generation used in

simulation, that lead to irregular grids. Several tools as in [16] and [17] generate meshing models.

The Map-Reduce framework in [6], [7], [8], [10] performs speedily a large volume of data, in using the parallelism of map and reduce. For instance, a survey on performance comparisons of different frameworks such as Hadoop, Spark, Phoenix++, Marissa, Mariane, Sasreduce, Bitdew, Mr4c and Themis, has been presented by Zeba Khanam and others in [9]. An application of the map-reduce algorithm to improve the Hough Transform method processing has been introduced by SERE and others in [5]. It has been extended by Mateus Coelho and others in [19] to deal with circle recognition. SERE and others in [18] have also used the map-reduce algorithm to extract speedily posts from social networks.

Our work concerns with the problem to find out a particular data in Big Data distributed on different clusters. The proposed method is represented by an architecture that searches a data in a grid of clusters with algorithms introduced into the functions map and reduce. The generated clusters takes the concept of classification based on k-neighborhood into account.

This paper is organized as follows: The Section II named preliminaries introduces the problem specification and the concepts related to meshing techniques and the map-reduce algorithm. The Section III explains the proposed method with the applications of meshing techniques and the map-reduce algorithm. Experimental results deal with the case study of drug management in pharmacies, illustrated by the Section IV.

## II. PRELIMINARIES

This section brings informations on the problem specification, the description of the map-reduce algorithm and the meshing techniques used in Discrete Geometry.

### A. Problem Statement

Let  $W$  be the universal set of database sites distributed in a space. Let  $S$  be a subset of database sites such as  $S \subset W$ . Suppose that  $S = \{S_1, S_2, \dots, S_{n-1}, S_n\}$  where  $S_i$  is a database site. All the data in database site  $S_i \in S$ , together possesses the characteristics of Big Data through data volumetric.

Consider  $d$  as a specific data such as  $d \in u$  and  $u \in W$ .  $u$  could be a member of  $S$  or not. Let  $M$  be a point. The problem is to find out database sites  $S_i \in S$  where database sites  $S_i$  must be the neighbors of the point  $M$  and  $d \in S_i$ . That leads to a decisional problem in calculability.

There are two manners to verify if the data  $d$  is in the database  $S_i$ . That means if  $d \in S_i$  ?

- the first one is to search data sequentially in each  $S_i \in S$  in going from 1 to  $n$ .
- the second one is to proceed by a parallel verification with research in each group of  $S_i$ .

Our hypotheses is that the parallel verification is speedier than the first one. Suppose that  $\alpha$  is the time taken to perform  $S_i$ .

In the first case, the effective execution time will be  $n\alpha$  in the worst case. The worst case corresponds to the conditions ( if  $d \in S_n$  or if  $d$  is not a member of any  $S_i$  ).

In the second case, let  $\beta$  be the number of group of  $S_i$ . That means clearly  $\beta \leq n$ .  $\alpha$  will be also considered as the execution time to perform each group. The global execution time will be  $\beta\alpha$ . We obtain  $\beta\alpha \leq n\alpha$  because  $\beta \leq n$ .

Thus, our analysis will focus on two axes : firstly, before searching data, we classify data into clusters; secondly, we accelerate data research in using the map-reduce algorithm on limited clusters.

Furthermore, the following sections will deal with an analysis of the map-reduce framework and meshing techniques that generate different groups to make data research speedier in the Big Data context.

### B. Mesh Generation

There are also many techniques in discrete geometry to create regular or irregular grid which allows forward detection of the nearest sites. For instance, Vacavant's thesis in [4] study possible applications of regular grids and irregular grids in simulation, illustrated by the Fig. 1.

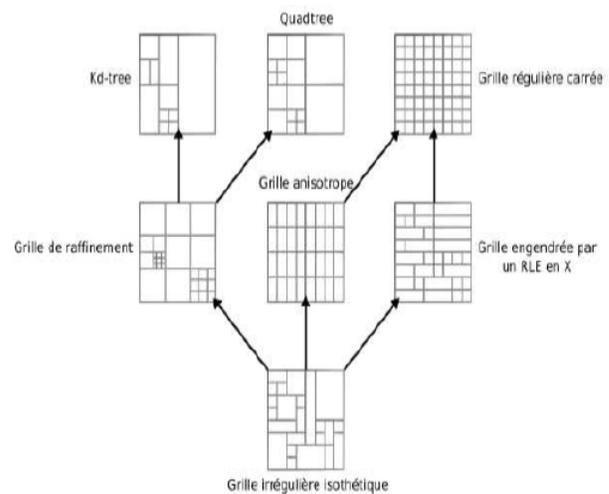


Fig. 1. Irregular Grids and Regular Grids in Vacavant's Thesis in [4].

K-neighborhood is very used in Discrete Geometry. It follows from meshing technique application and corresponds to 4-neighborhood and 8-neighborhood in a two dimensional space :

**Definition 1 (4-neighborhood in [3], [15])** Let A and B be two pixels with integer coordinates respectively  $(X_A, Y_A)$  and  $(X_B, Y_B)$ .

$$(A \text{ and } B \text{ are in 4-neighborhood}) \iff |X_A - X_B| + |Y_A - Y_B| = 1$$

4-neighborhood uses the distance of Manhattan based on  $D(A, B) = |X_A - X_B| + |Y_A - Y_B|$  in 2D.

Figure 2 shows an example of 4-neighborhood between the central pixel A and the pixels B, C, D, E.

**Definition 2 ( 8-neighborhood in [3], [15] )** Let A and B be two pixels with integer coordinates respectively  $(X_A, Y_A)$  and  $(X_B, Y_B)$ .

$$(A \text{ and } B \text{ are in 8-neighborhood}) \iff \max(|X_A - X_B|, |Y_A - Y_B|) \leq 1$$

But, 8-neighborhood implements the distance of Tchebychev which is defined by  $D(A, B) = \max(|X_A - X_B|, |Y_A - Y_B|)$  in 2D.

Fig. 3 shows an example of 8-neighborhood between the central pixel A and the pixels B, C, D, E, F, G, H, I.

Euclidian distance and K-nearest neighbor are another alternatives to define neighborhood, to build clusters and to reach classification.

Manhattan distance, Tchebychev distance and Euclidean distance lead respectively to several geometry shapes such as lozenges, squares and circles, used in computing neighbors.

These above definitions are necessary in computing nearest database sites. Others information related to Geographic Information System (GIS) might be integrated in this way.

The following sections will explain how meshing techniques can be useful in classification in order to speed up the processing through the map reduce algorithm.

### C. Map-reduce Concepts

Map-Reduce content defines two important tasks, namely Map and Reduce. It describes the parallelism of the map functions followed by the parallelism of the reduce functions, as explained by Dean and others in [10] and SERE and others in [18]. The shuffle phase is executed automatically by the system, between both the map function and the reduce function.

The map function defines a transformation of pairs that accepts as inputs a single key and a value, noticed  $(k, v)$  pair and produces as outputs a set of intermediate (key, value) pairs  $(k_i, v_i)$ . At the end of all the map functions, several pairs  $(k_i, v_i)$  are produced by the map functions. For instance the map function transforms the pairs  $(k, v)$  as input and produces the set of pairs  $(k_1, v_1), (k_2, v_2)$ .

The shuffle phase starts after all the map functions ended and before starting the reduce functions. The shuffle phase consists of having together the value of the pairs  $(k_i, v_i)$  produced by all the map functions : it produces the pairs that have the same key. It also sort keys into correct order to prepare next computation. For instance, for the following pairs  $(k_1, v_1), (k_1, v_2), (k_2, v_2), (k_2, v_3)$  produced by all the map functions, the shuffle phase returns the pairs  $(k_1, \langle v_1, v_2 \rangle), (k_2, \langle v_2, v_3 \rangle)$ . Thus, the shuffle phase carry out data classification where each class referenced by a key.

The reduce function takes as an input a (key, list of values) pair that contains a intermediate key and a set of values for that key. The reduce function produces a pair (key, result of a list of values). The key in the input is the same in the output. For instance, the pairs  $(k_1, \langle v_1, v_2 \rangle)$  and  $(k_2, \langle v_2, v_3 \rangle)$  become  $(k_1, \langle v_1 + v_2 \rangle), (k_2, \langle v_2 + v_3 \rangle)$ .

Reduce functions could start before the end of all the map functions. Mixing map and reduce will reach an improvement of processing time : That will be studied in perspectives, with synchronization control between each others.

The map-reduce model consists of the parallelism of map function followed respectively by the shuffle phase and reduce functions: there is a master node that controls all the processes tasks, distributed on secondary nodes with distributed memory.

Thus, the map function, the shuffle phase and the reduce function have summarized successively in 1, 2, 3, 4, 5, 6 and 7 as follows:

$$Map(k, v) \longrightarrow \{(k_1, v_1), (k_1, v_2)\} \quad (1)$$

$$Map(k', v') \longrightarrow \{(k_2, v_2), (k_2, v_3)\} \quad (2)$$

$$\{(k_1, v_1), (k_1, v_2)\} \xrightarrow{shuffle} (k_1, \langle v_1, v_2 \rangle) \quad (3)$$

$$\{(k_2, v_2), (k_2, v_3)\} \xrightarrow{shuffle} (k_2, \langle v_2, v_3 \rangle) \quad (4)$$

$$Reduce(k_1, \langle v_1, v_2 \rangle) \longrightarrow (k_1, \langle v_1 + v_2 \rangle) \quad (5)$$

$$Reduce(k_2, \langle v_2, v_3 \rangle) \longrightarrow (k_2, \langle v_2 + v_3 \rangle) \quad (6)$$

Generally the reduce function is defined by :

$$Reduce(k_i, \langle v_1, \dots, v_j \rangle) \longrightarrow (k_i, v_k) \quad (7)$$

Where  $v_k = v_1 + \dots + v_j$ , being the result of the operator + applied to the members of the list  $\langle v_1, \dots, v_j \rangle$ .

The map-reduce framework has applied to problems of counting the number of word in a document, computing the average of numbers, doing data selection and to sort dataset.

### III. METHOD DESCRIPTION

This section is focusing on the application of meshing techniques very used in discrete geometry, database structure description, Data research algorithms and the content of map-reduce algorithm.

Due to the size of all the database sites reaching Big Data size as presented in problem statement, it will be better to have different clusters of database sites, linked by an unique structure of database in a central NoSQL database. In this manner, the central nosql database has connected on different sites in the same network : these sites, as data owners have the right to update data in back office. Users request to read data from the system in front office through their mobile phone or online with a desktop connected on the network provided by mobile operators for instance.

The network will contribute to improve the map-reduce algorithm according to the execution time, in giving easily data accessibility through data research.

Meshing techniques will define the central database structure in giving a relation between GPS references and related data. They also creates the clusters of database sites that must be together (in the same cluster) in order to improve data research with the map- reduce algorithm.

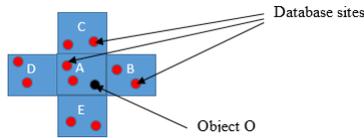


Fig. 2. 4-Neighborhood.

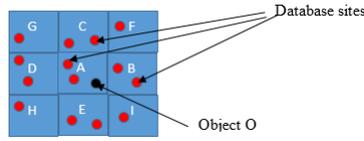


Fig. 3. 8-Neighborhood.

### A. Meshing Application

Through the problem specification, all the database sites are referenced by the coordinates corresponding to its GPS reference. They have been distributed into different cells, called clusters. The center of each cluster is also referenced by the coordinates associated to its GPS reference.

A central database is introduced to take all the data of all the database sites into account. The Section III-B will discuss about database structure and the network architecture used.

The concept of k-neighborhood in discrete geometry uses the notion of distance. It determines the neighbor cells around a central cell.

4-neighborhood and 8-neighborhood are the particular cases of k-neighborhood in a two dimensional space. Fig. 2 shows an example of a regular grid with different pixels in 4-neighborhood, where A is the central pixel : there are four (04) pixels in 4-neighborhood with the pixel A, such as B, C, D, E.

While, Fig. 3 also presents an example of 8-neighborhood: the pixel A has eight (8) pixels as its neighbors such as B, C, D, E, F, G, H, I.

The pixels A, B, C, D, E, F, G, H, I indicate different clusters which contain database sites (as presented by red points in Fig. 2 and in Fig. 3). All the database sites represented by red points together has the characteristics of Big Data as illustrated in the problem statement. The problem is to find out the nearest database sites of an object O (a black point in Fig. 2 and in Fig. 3) that verify some conditions about the item d.

There exist many techniques to generate meshing grids. For instance, Quasi-affine applications leads to establish a grid on an image, to overcome pixels, called in our study, as clusters. For instance let  $(D_i)$  and  $(D'_i)$  be straight lines, respectively defined by  $ax+by = w_i$  and  $cx+dy = w'_i$  in a two dimensional space. Fig. 4 shows clusters, resulting of the intersection of the straight lines  $(D_i)$  and  $(D'_i)$ .

Each cluster is referenced by  $idc_k$ . It contains the database sites. Each database site is referenced by  $idc_{k,l}$  where  $k$  is an integer in  $\{1, 2, \dots, n-1, n\}$  and  $l$  is an integer in  $\{1, 2, \dots, m-1, m\}$ .  $n$  is the number of clusters in all the GIS area while  $m$  corresponds to the maximal number of database

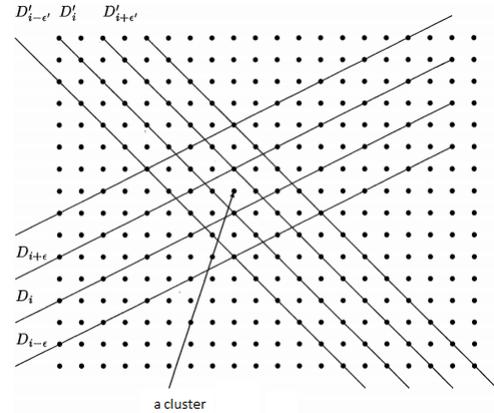


Fig. 4. Clusters Resulting of Crossing Parallel Straight Lines.

sites in each cluster. Then the number of database sites in the GIS area defined by an image is then determined by the value  $n.m$ .

In others ways, let  $nbd(x)$  be a function that allows to get easily the number of database sites in the cluster referenced by the index  $x$ . Then, the number of database sites in all the area will become  $\sum_{k=1}^{k=n} nbd(ic_k)$ .

That means :

$$\sum_{k=1}^{k=n} nbd(ic_k) \leq n.m \quad (8)$$

Moreover, if each database site has a maximal size, named  $s$ , the size of all the data named big data will be either  $s.n.m$  or  $s. \sum_{k=1}^{k=n} nbd(ic_k)$  where obviously

$$s. \sum_{k=1}^{k=n} nbd(ic_k) \leq s.n.m \quad (9)$$

Our purpose concerns time reduction in using the map-reduce algorithms for data research and to localize the data as inputs to these algorithms.

Then, we have:

$$s. \sum_{k=1}^{k=t} nbd(ic_k) \leq s. \sum_{k=1}^{k=n} nbd(ic_k) \leq s.n.m \quad (10)$$

where  $t < n$ .

Only a limited number of clusters defined by the value  $t$ , will be processed by the map-reduce algorithm.

### B. Database Structure and Architecture

The proposed solution for data control is a network between different sites, connected on the central nosql database with permissions of data updating and data selection to each others.

Database structure takes into account the relation between database sites referenced by GPS coordinates distributed into the same cluster.

Thus, a cluster referenced by a pair  $(u_i, v_i)$  contains a set of pairs  $(m_i, n_i)$  representing database site references. For instance, the Table I shows a NoSQL database table.

TABLE I. A DATABASE TABLE

cluster references	database site references	data in sites	data in sites
$(u_1, v_1)$	$(m_1, n_1)$	Data	Data
$(u_2, v_2)$	$(m_2, n_2)$	Data	Data
$(u_3, v_3)$	$(m_3, n_3)$	Data	Data

We introduce a dynamic table to save clusters references corresponding exactly to the regular grid, associated to a region. This grid is resulting of the meshing technique application. But, to overcome the problem of empty clusters having no data inside that might happen in the central database, the solution is to establish for instance, an adapted irregular grid in following the technique of Delaunay triangulation or Voronoi diagram. Another possibility is to accept empty clusters being inserted into the nosql database Table I. The future works will focus on the strategies to transform a regular grid to an irregular grid to avoid empty clusters.

The Table II is useful for neighbor detection to get the next clusters as inputs to the entity “data research” in the following section.

TABLE II. A MEMORY TABLE OF CLUSTER REFERENCES GENERATED BY A MESHING TECHNIQUE

(0,0)	(0,1)	(0,2)	(0,3)	(0,4)
(1,0)	(1,1)	(1,2)	(1,3)	(1,4)
(2,0)	(2,1)	(2,2)	(2,3)	(2,4)
(3,0)	(3,1)	(3,2)	(3,3)	(3,4)
(4,0)	(4,1)	(4,2)	(4,3)	(4,4)
(5,0)	(5,1)	(5,2)	(5,3)	(5,4)
(6,0)	(6,1)	(6,2)	(6,3)	(6,4)

The first column named “cluster references” of the table I contains the same data as the cell values of the Table II. While the second column named “database site reference” presents site references. Fig. 5 provides more details on the relation between the Table I and the Table II with  $(u_1, v_1)$  and  $(u_2, v_2)$  as cluster references.

There are three layers in the architecture: the layer “database”, the layer “map-reduce algorithm” and the layer “application” as presented in the Table III.

### C. Data Research

In a two dimensional space, a quasi-affine application is defined by the function  $F_0(x, y)$  which returns the coordinates of the central cluster that contains the initial object  $O$  of coordinates  $(x_O, y_O)$ . That means  $F_0(x_O, y_O) = (u, v)$  where  $(u, v)$  is the coordinates of the central cluster.

In 4-neighborhood, we'll obtain the couples  $(u, v - 1), (u, v + 1), (u - 1, v), (u + 1, v)$  of the central clusters  $(u, v)$ .

But, in following 8-neighborhood, the first package of neighbors around the central cluster  $(u, v)$  gives the following

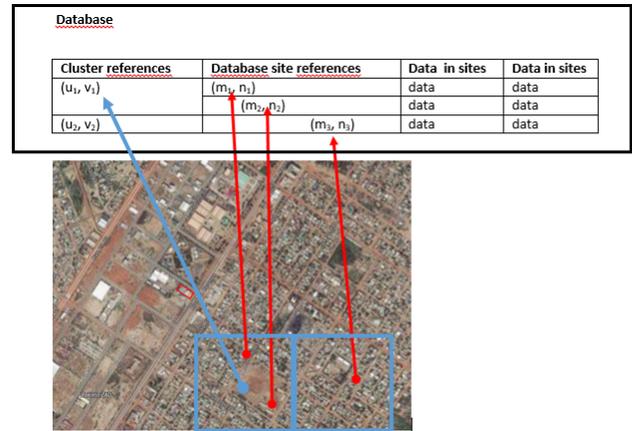


Fig. 5. Link Between an Image and a Database.

TABLE III. THREE LAYERS IN THE ARCHITECTURE

Layer 3 : Application
Layer 2 : Map-reduce algorithms
Layer 1 : Database

set of clusters  $\{(u, v - 1), (u, v + 1), (u - 1, v), (u + 1, v), (u - 1, v - 1), (u - 1, v + 1), (u + 1, v + 1), (u + 1, v - 1)\}$ .

Our method will study 8-neighborhood in a regular grid, constituted of squares. Let  $I_1$  be the set  $\{-1, 0, +1\}$ . It is obvious that  $\text{card}(I_1)=3$ . The first package contains clusters referenced by the set  $\{(u + k, v + l) \text{ where } (k, l) \in I_1\}$ .

Finally, the number of clusters in the first package is determined by  $\text{card}(I_1^2)$ .

As  $\text{card}(I_1^2)=9$ , there are nine clusters in the package 1, used for data research.

For generalization, suppose that

$$I_i = \{-i, -(i - 1), \dots, -1, 0, +1, \dots, +(i - 1), +i\} \quad (11)$$

The following Table IV summarizes the packages with their cluster references inside that may be used step by step in data research.

TABLE IV. PACKAGES

Packages	$I_n$	cluster references	$\text{card}(I_n^2)$
Package 1	$I_1 = \{-1, 0, +1\}$	$\{(u + k, v + l) / (k, l) \in I_1^2\}$	9
Package 2	$I_2 = \{-2, -1, 0, +1, +2\}$	$\{(u + k, v + l) / (k, l) \in I_2^2\}$	25
Package 3	$I_3 = \{-3, -2, -1, 0, +1, +2, +3\}$	$\{(u + k, v + l) / (k, l) \in I_3^2\}$	49
Package i	$I_i = \{-i, -(i-1), \dots, -1, 0, +1, \dots, +(i-1), +i\}$	$\{(u + k, v + l) / (k, l) \in I_i^2\}$	$(2i + 1)^2$

Data research deals with the processing of the package i. It begins initially with the package 1. If the value d is not found in the package i, then the next package i+1 will be processed: in fact, as  $(\text{package } i) \subset (\text{package } i+1)$ , we are interested precisely in cluster references in the package i+1, not already performed in the package i, as illustrated in Fig. 6 by colored layers successively with the numbers 1, 2, 3, 4, and 5.

As we know that:

$$I_{i-1} \subset I_i \quad (12)$$

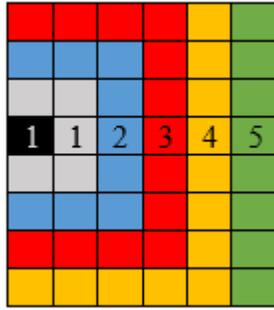


Fig. 6. Clusters Sent Respectively to the Map Functions for Analysis in the Order of Colored Packages 1, 2, 3, 4 and 5.

We have precisely:

$$I_i = I_{i-1} \cup \{-i, +i\} \quad (13)$$

That means generally:

$$I_n = I_1 \cup \left( \bigcup_{i=2}^n \{-i, +i\} \right) \quad (14)$$

Consider

$$D_i = I_i - I_{i-1} \quad (15)$$

We conclude then

$$D_i = \{-i, +i\} \quad (16)$$

Suppose that

$$R_i = (D_i \times I_i) \cup (I_i \times D_i) \quad (17)$$

As

$$(D_i \times I_i) \cap (I_i \times D_i) = \{(-i, -i), (-i, +i), (+i, -i), (+i, +i)\} \quad (18)$$

We have

$$\text{card}(R_i) = [(2 \times (2i + 1)) + ((2i + 1) \times 2)] - 4 \quad (19)$$

That means

$$\text{card}(R_i) = 8i + 4 - 4 \quad (20)$$

Finally

$$\text{card}(R_i) = 8i \quad (21)$$

As  $\text{card}(R_i)=8i$ , 8i new clusters have been performed by data research, for each iteration i. For instance:

- if  $i=2$ , data research will run on 16 clusters referenced by:
  - \*  $\{(u-2, v-2), (u-1, v-2), (u, v-2), (u+1, v-2), (u+2, v-2)\}$
  - \*  $\{(u-2, v+2), (u-1, v+2), (u, v+2), (u+1, v+2), (u+2, v+2)\}$
  - \*  $\{(u-2, v-1), (u-2, v), (u-2, v+1)\}$
  - \*  $\{(u+2, v-1), (u+2, v), (u+2, v+1)\}$
- if  $i=3$ , data research will deal with 24 clusters referenced by:

- \*  $\{(u-3, v-3), (u-2, v-3), (u-1, v-3), (u, v-3), (u+1, v-3), (u+2, v-3), (u+3, v-3)\}$
- \*  $\{(u-3, v+3), (u-2, v+3), (u-1, v+3), (u, v+3), (u+1, v+3), (u+2, v+3), (u+3, v+3)\}$
- \*  $\{(u-3, v-2), (u-3, v-1), (u-3, v), (u-3, v+1), (u-3, v+2)\}$
- \*  $\{(u+3, v-2), (u+3, v-1), (u+3, v), (u+3, v+1), (u+3, v+2)\}$

- finally if  $i=a$ , data research will take in entry 8a clusters referenced by:

- \*  $\{(u-a, v-a), (u-(a-1), v-a), \dots, (u, v-a), (u+1, v-a), \dots, (u+(a-1), v-a), (u+a, v-a)\}$
- \*  $\{(u-a, v+a), (u-(a-1), v+a), \dots, (u, v+a), (u+1, v+a), \dots, (u+(a-1), v+a), (u+a, v+a)\}$
- \*  $\{(u-a, v-(a-1)), (u-a, v-(a-2)), \dots, (u-a, v), (u-a, v+(a-2)), (u-a, v+(a-1))\}$
- \*  $\{(u+a, v-(a-1)), (u+a, v-(a-2)), \dots, (u+a, v), (u+a, v+(a-2)), (u+a, v+(a-1))\}$ .

The coordinates  $(u, v)$  of any cluster localized in a region must verify the constraints  $\begin{cases} x_{min} \leq u \leq x_{max} \\ y_{min} \leq v \leq y_{max} \end{cases}$  where  $x_{min}, x_{max}, y_{min}$  and  $y_{max}$  are constants corresponding to the coordinates of clusters in the extremities of the region.

We have introduced an algorithm to create a list of cluster as follows in Algorithm 2. This algorithm takes as parameters an integer and the Table II which has its extremities coordinates defined by the constraints  $\begin{cases} x_{min} \leq u \leq x_{max} \\ y_{min} \leq v \leq y_{max} \end{cases}$

The global algorithm illustrated in Algorithm 1 shows more details on the main steps of data research: it generates in each iteration a list of cluster through the method `getClusterofPackage(i, m)` which content is given by the Algorithm 2.

We recall that in both Algorithms 1 and 2 the coordinates  $(u, v)$  verify  $F_0(x_0, y_0) = (u, v)$ .

Thus, the clusters in entry to the map-reduce algorithm have been analyzed successively by iterations, as presented in Algorithm 1. Each iteration is associated to a new package.

As a conclusion, we have studied the neighbors packages, in considering 8-neighborhood based on the distance of Tchebychev. But others distances such as the Euclidean distance leading to digital disks, should be explored precisely in perspectives.

But, the concepts of distance are limited in analysis of the nearest database sites, because they might be influenced by barriers or obstacles in the environment, depending on effective presence of roads described in Geographic Information System (GIS). In reality, the distance between a point M and a database site may be short and separated by a mountain. The future works will study on how to take the presence of roads into account.

Now, the remaining question is to search precisely data in the content of each cluster.

#### D. Map-Reduce Algorithm and Application

This section concerns the definitions of map-reduce content, in explaining how to extract data of database sites through

---

**Algorithm 1:** GlobalAlgorithm(Object O, Table m)

---

**Result:** a list of data found in the form list  $\langle data \rangle$   
d : Data ;  
i : integer ;  
b: boolean ;  
l: list $\langle Cluster \rangle$  ;  
r: list $\langle Data \rangle$  ;  
l.add(Cluster(u, v));  
l.addList(getClusterofPackage(1, m));  
i=1;  
b=False;  
**while** (not empty(l) and b==False) **do**  
    r =Map-reduceAlgorithm(l);  
    **if** not empty(r) **then**  
        b=True ;  
    **end**  
    **else**  
        i=i+1;  
        l.clean();  
        l.addList(getClusterofPackage(i, m));  
    **end**  
**end**  
**if** (b==True) **then**  
    return r ;  
**end**  
**else**  
    return NULL ;  
**end**

---

a restricted list of cluster instead of taking all the clusters in the region.

The reference of a cluster is giving by the pair  $(u, v)$  that corresponds to the coordinates of its center or its GPS coordinates, transformed.

Firstly, the entries of the function map are the clusters of the package 1 represented, respectively by  $(u, v)$ ,  $(u_1, v_1)$ ,  $(u_2, v_2)$ ,  $(u_3, v_3)$ ,  $(u_4, v_4)$ ,  $(u_5, v_5)$ ,  $(u_6, v_6)$ ,  $(u_7, v_7)$ ,  $(u_8, v_8)$  in relation in 8-neighborhood.

Due to the image size and then the cluster size, each cluster reference must verify the constraints:  $\begin{cases} x_{min} \leq u_i \leq x_{max} \\ y_{min} \leq v_i \leq y_{max} \end{cases}$

For new data research, regarding to the value 8i increasing, the number of map function could change dynamically to face scalability with more users connected on the system.

Moreover, due to using a regular grid, the database will present empty clusters which contain data from any database sites: that means no database sites in these clusters. But, these empty clusters give information about the need of installing database sites in these regions.

Our method considers each map function taking one cluster in entry. Algorithm 3 shows exactly the content of the map function.

But the future works might concern the case of several clusters or the whole package as entries, being analyzed by one map function.

---

**Algorithm 2:** getClusterofPackage(Int a, Table m)

---

**Result:** a list of Cluster as in the form list  $\langle Cluster \rangle$   
c : Cluster ;  
j : integer ;  
l: list $\langle Cluster \rangle$  ;  
l.clean() ;  
**for** (j=-a; j ≤ a; j++) **do**  
    **if** ( $x_{min} \leq u + j \leq x_{max}$  and  $y_{min} \leq v - a \leq y_{max}$ ) **then**  
        c=new Cluster(u+j, v-a);  
        l.add(c);  
    **end**  
**end**  
**for** (j=-a; j ≤ a; j++) **do**  
    **if** ( $x_{min} \leq u + j \leq x_{max}$  and  $y_{min} \leq v + a \leq y_{max}$ ) **then**  
        c=new Cluster(u+j, v+a);  
        l.add(c);  
    **end**  
**end**  
**for** (j=-a+1; j ≤ a-1; j++) **do**  
    **if** ( $x_{min} \leq u - a \leq x_{max}$  and  $y_{min} \leq v + j \leq y_{max}$ ) **then**  
        c=new Cluster(u-a, v+j);  
        l.add(c);  
    **end**  
**end**  
**for** (j=-a+1; j ≤ a-1; j++) **do**  
    **if** ( $x_{min} \leq u + a \leq x_{max}$  and  $y_{min} \leq v + j \leq y_{max}$ ) **then**  
        c=new Cluster(u+a, v+j);  
        l.add(c);  
    **end**  
**end**  
return l ;

---



---

**Algorithm 3:** function map(Doc idcluster, Doc value)

---

**Result:** the pairs in the form  $(k, v)$   
d : Data ;  
**if** Verification(d, value ) **then**  
    information←getInformationSite(value) ;  
    emit(idcluster, information);  
**end**

---

The variable value represents the content of a cluster and contains on each line, the name and the data of a site, corresponding to the data of the column name “data in sites” in the table I. The output of a mapper is for instance the set of pairs  $(id, info_1)$ ,  $(id, info_2)$ , with the same  $id$  as a reference for a cluster. Each mapper works on different clusters.

The shuffle phase is automatic as illustrated in the Table V : it consists of putting together all the pairs issued by the map functions. That means:

- for the cluster  $id_1$  in entry: the pairs  $(id_1, info_{11})$ ,  $(id_1, info_{12})$  becomes  $(id_1, \langle info_{11}, info_{12} \rangle)$ ;
- for the cluster  $id_2$  in entry: the pairs

$(id_2, info_{21}), (id_2, info_{22})$  returns  $(id_2, < info_{21}, info_{22} >)$

- for the cluster  $id_3$  in entry: the pairs  $(id_3, info_{31}), (id_3, info_{32})$  becomes  $(id_3, < info_{31}, info_{32} >)$ .

TABLE V. THE SHUFFLE PHASE

Pairs issued by the map functions (in entry)	Results after the shuffle phase
$(id_1, info_{11}), (id_1, info_{12})$	$(id_1, < info_{11}, info_{12} >)$
$(id_2, info_{21}), (id_2, info_{22})$	$(id_2, < info_{21}, info_{22} >)$
$(id_3, info_{31}), (id_3, info_{32})$	$(id_3, < info_{31}, info_{32} >)$

The reduce functions will work on the pairs in the Table V resulting of the shuffle phase, as illustrated in Algorithm 4.

**Algorithm 4:** function reduce(Docid idCluster, Iterator value)

```

Result: the pairs in the form
       $(k, < v_1, v_2, \dots, v_{n-1}, v_n >)$ 
result : String ;
result ← "";
for each  $v_i$  in value do
  | result= result+""+ $v$  ;
end
emit(result);

```

Finally, the outputs of all the reduce functions will give three groups of data such as,  $info_{11} + info_{12}$ ,  $info_{21} + info_{22}$ ,  $info_{31} + info_{32}$ , representing information related to the presence of the value d.

#### IV. SIMULATION AND DISCUSSIONS

This section deals with method applications in referring to drugs management in pharmacies as the case study of the problem specification.

Consider data about drugs in pharmacies, spread over the territory. The question is to find out the nearest pharmacies (or drugstores) accordingly to the initial position of an Object O with coordinates  $(x_O, y_O)$ , requesting data research in a region.

The number of clusters  $8i$  will increase easily in each iteration  $i$  (for instance for  $i$  going 1 to  $n$ ): the value  $8i$  corresponds to a linear function that will lead to more clusters with  $i$  increasing. If the object O is localized in a cluster in one of the extremities of the region, the worst case will consist of finding out data related to the value d in the others extremities of the region. Consider  $F_0(x_O, y_O) = (0,0)$ , the corresponding cluster reference.

It will be better that the structure of cluster references in the database follows 8-neighborhood, to facilitate data research in the database and to allows speedily the response to any request. The relation of 8-neighborhood between two clusters is obviously reflexive and symmetric. Thus, two clusters linked by 8-neighborhood might be juxtaposed in the database structure. that will be of course difficult because the position of the object O is not definitively fixed for all the requests sent by users. But to overcome this, we have built a cluster list (precisely a

type list  $< Cluster >$ ), in doing research on cluster references in the memory Table II, as illustrated in Algorithm 1 with the function getClusterofPackage(i, m).

Moreover, there are several nosql databases such as MongoDB, Hbase, Cassandra, CouchDB, Couchbase, Neo4j, OrientDB, Oracle Graph, and Big table in [22] that might be used to store GIS data, as mentioned in the previous table I. But, here we have decided to use MongoDB as the database layer and to connect finally spark on MongoDB to realize implementation of the map-reduce algorithm.

Simulation considers a NoSQL database under the spark layer and is based on a computer with the following characteristics:

- the layers spark, NoSQL database (MongoDB) installed in localhost;
- memory: 3,7 GB
- processor: Intel® Celeron(R) CPU B830 1.80 GHz × 2
- graphic card: Intel® HD Graphics 2000
- operating system: Ubuntu 18,04 LTS 64 bits

Consider cluster references and site references in the Table VI, specializing the Table I, and saved in a MongoDB database.

Moreover, we establish a link between data in the Table VI and its associated region in the Table VII through the foreigner key "region name": the database will contain only two tables.

Cluster references and database sites references are obviously fixed, like the region name and its image.

Dataset is constituted by data extracted from the list of drugs from Hospitals in Cameroon in [21]. Generally, pharmacies provide the same drugs. Redundancy on the drugs names and its specification area will appear in the database. Then, we have decided to repeat data in the Table VI for different clusters to have more than 100 tuples: here, the Table VI is just a sample of real data in the database.

TABLE VI. TABLE OF DRUGS

Region name	Cluster Ref	Site Ref	Pharmacy	Drugs	Specif	quantity
belle-ville	(0, 0)	(0,1)	soudia	amoxiline	500mg	40
belle-ville	(0,0)	(0,1)	soudia	amoxiline	400mg	40
belle-ville	(0,0)	(0,1)	soudia	amoxiline	300mg	40
belle-ville	(0,0)	(0,1)	soudia	amoxiline	200mg	40
belle-ville	(0,0)	(0,1)	soudia	amoxiline	100mg	40

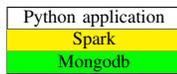
TABLE VII. TABLE OF REGIONS

Region name	images
belle-ville	image blob

The architecture used for implementation consists of three layers (mongodb, spark and python application) as defined by the Table VIII, specializing the layers, proposed in the Table III.

A spark connector allows connection between spark and mongodb to get dataframes from mongodb for visualisation in python application. A sample of codes in python is implemented in Fig. 7 and gives for instance the following results:

TABLE VIII. ARCHITECTURE WITH A NOSQL DATABASE



```

start_time = time.time()
def task1():
    # Map Function:
    start_t1 = time.time()
    mapper = Code("function(){ var skill =this.drugs ='Morphine';\
        if(this.quantity>0){\
            for(i in skill){emit({Information:{Pharmacy:this.pharmacy,Produits:this.drugs,\
                Specification:this.specif,Reference:this.cluster_ref}},\
                1)};\
            }\
        }")
    # Reduce:
    reducer = Code("function(key,values){return Array.sum(values);}")
    # Bringing it all together, creating an output file: 'ppl_skillCount'
    map_reduce = collection.map_reduce(mapper, reducer, 'ppl_skillCount')
    end_t1 = time.time()
    print("Le temps d'execution du task1()", end_t1 - start_t1)
    
```

Fig. 7. A Sample of Codes in Python

{{"Information": {"Pharmacy": "Escale", "Produits": "Morphine", "Specification": "500mg/ml", "Reference": "(0,1)"}, "value": 33.0}

We are interested in time evaluation between the sequential research step by step on selected clusters near the localized cluster and the parallelism research simultaneously on the same clusters. As mentioned in the data Table IX and its related Fig. 8, experimental results show a large difference between the curves of sequential execution and parallel execution in considering the time taken for data research and the number of clusters: The parallel execution of different clusters with the map-reduce algorithm brings interesting improvement of processing time, giving possibilities of speed responses to users.

We notice that, in Table IX and in Fig. 8, time is evaluated on each group, defined by the same drug name: that means each  $group_i$  corresponds to an unique  $(drugname)_i$ .

TABLE IX. TIME EVALUATION IN MILLISECOND (MS) WITH A NOSQL DATABASE

Group N°	1	2	3	4	5	6	7	8	9	10
Clusters found	10	20	30	40	50	60	70	80	90	100
Sequential	0.4994	0.524	0.5409	0.5879	0.7335	0.8577	0.9989	1.132	1.2859	3.5537
Parallel	0.4897	0.5294	0.565	0.5004	0.4906	0.4831	0.4898	0.5099	0.5205	0.5333

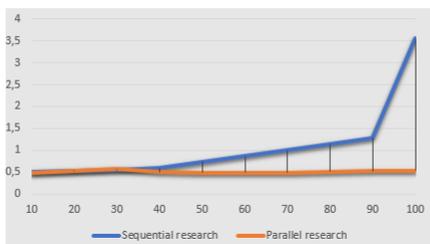


Fig. 8. Time Evaluation (in millisecond) Through the Curves of Sequential Research and Parallel Research with Spark

On the other hand, a nosql database could be substituted to a nosql database, to integrate performance of nosql databases

such as viz, VoltDB, MemSQL and NuoDB. Because, newsq databases conserve the power of nosql databases such as horizontally scalable, highly available and take into account ACID properties, SQL support for SQL databases, accordingly to Irina Astrova and others in [20]. In this case, implementation will consider the layers MemSQL, Spark and Python application: spark will be connected on MemSQL through a connector. Details on comparisons with time evaluation between MemSQL and MongoDB will be studied in perspectives.

## V. CONCLUSION AND PERSPECTIVES

A GIS database structure has been proposed in taking into account a meshing technique based on a quasi affine application in order to get a regular grid and to identify clusters. A NoSQL database table has been established as the implementation of data clustering. Proposed data research uses a limited number of clusters in entry to the map-reduce algorithm, to improve processing time.

Experimental results reveal effectively an improvement of processing time with the parallel execution on selected clusters around the central cluster through the map-reduce algorithm than the sequential execution on the same clusters.

In perspectives, the remaining questions will concern others meshing techniques to create new clusters and to undertake new concepts related to neighborhood through establishment of distance definitions and in taking others criteria such as modelization of presence of roads near the region.

The regular grid leads to empty clusters with no data inside. In the future works, as an alternative to alleviate this problem, we will study the case of irregular grids adapted to real data in the database sites to eliminate empty clusters in the central database. We will analyze strategies to transform a regular grid to an irregular grid to avoid empty clusters.

Comparisons between the layers MongoDB and MemSQL through spark connector and python application will be analyzed with time evaluation to determine the best alternative in data research.

The future works will explore in more details the applications of this framework to others fields such as Finance, Education and Shopping.

## ACKNOWLEDGMENT

The authors would like to thank the Ministry of Numeric Economy and Post (MDENP) for finding relevance in using big data opportunities for digital transformation of public administrations through several events such as FNDSI 2020 (Forum National des DSI) and SN 2020 (Semaine du Numérique 2020). These events focused on artificial intelligence, big data and cyber-security. This paper is regarding to these topics.

## REFERENCES

- [1] Yaya TRAORE, Malo SADOUANOUAN, Didier BASSOLE, Abdoulaye SERE, *Multi-Label Classification using an Ontology*, International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 10, No. 12, 2019
- [2] Marie-Andree and Jacob-Da Col, *Applications quasi-affines et pavages du plan discret*, Theoretical Computer Science vol 259 page 245-269, 2001

- [3] Abdoulaye SERE, *Transformations analytiques appliquées aux images multi-échelles et bruitées*, thèse de doctorat unique en informatique, Université de Ouagadougou, 2013
- [4] Antoine VACAVANT, *Géométrie discrète sur grilles irrégulières isothétiques*, thèse de doctorat en informatique, Université Lumière Lyon 2, 2007,
- [5] Abdoulaye SERE and Dario Colazzo and Oumarou SIE, *A Hough Transform based on a Map-Reduce Algorithm*, International Journal of Engineering Research and Applications (IJERA), 2016
- [6] Jimmy Lin, *MapReduce Algorithm Design*, Tutorial, Rio de Janeiro, 2013
- [7] Jairam Chandar, *Join Algorithms using Map-Reduce*, Master of Science, Computer Science School of Informatics, 2010
- [8] Jesus Camacho-Rodriguez and Dario Colazzo and Ioana Manolescu, *PAXQuery : Efficient Parallel Processing of Complex XQuery*, IEEE, 2015
- [9] Zeba Khanam and Shafali Agarwa, *Map-Reduce implementations : survey and performance comparison*, International Journal of Computer Science and Information Technology (IJCSIT), volume 7 , issue 4, 2015.
- [10] J. Dean and S. Ghemawat, *Map-reduce: simplified data processing on large clusters*, Commun. ACM, volume 51, issue 1, page 107-113, 2008.
- [11] Abdulrahman M. Qahtani, Bader M. Alouffi, Hosam Alhakami, Samah Abuayeid, Abdullah Baz, *Predicting Hospitals Hygiene Rate during COVID-19 Pandemic*, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 12, 2020.
- [12] World Health Organization (WHO), *la qualité des services de santé : Un impératif mondial en vue de la couverture santé universelle*, ISBN 978-92-4-251390-5 OMS.
- [13] OCDE, *Caring for quality in health: lessons learnt from 15 reviews of health care quality*, Éditions OCDE, Paris, <http://dx.doi.org/10.1787/9789264267787-en>, 2017.
- [14] Arah, O.A., G.P. Westert, J. Hurst et N.S. Klazinga, *A conceptual framework for the OECD Health Care Quality Indicators Project* , International Journal for Quality in Health Care, Suppl. 1, pp. 513, 2006.
- [15] David COEURJOLLY, *algorithmique et géométrie discrète pour la caractérisation des courbes et des surfaces*, thèse de doctorat en informatique, université Lumière Lyon2, 2002.
- [16] Zhi-Qiang Feng, Zhengqun Guan, Zhuowei Chen. *FER/Mesh: un logiciel de génération automatique de maillages*, 9e Colloque national en calcul des structures, CSMA, May 2009, Giens, France. hal- 01413781
- [17] Vincent François, *Méthodes de maillage et de remaillage automatiques appliquées à la modification de modèle dans le contexte de l'ingénierie simultanée*, thèse de doctorat, Université Henri Poincaré - Nancy 1, 1998
- [18] Abdoulaye SERE, José Arthur OUEDRAOGO, Boureima ZERBO, Oumarou SIE, *Post Classification in the Social Networks using the Map-reduce Algorithm*, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 12, 2020
- [19] Mateus Coelho ; Dylan Sugimoto ; Gabriel Melo ; Vitor Curtis and Juliana Bezerra, *A MapReduce based Approach for Circle Detection*, In Proceedings of the 14th International Conference on Software Technologies - Volume 1: ICSOFT, 454-459, Prague, Czech Republic, 2019.
- [20] Irina Astrova, Arne Koschel, Nils Wellermann, Philip Klostermeyer, *Performance Benchmarking of NewSQL Databases with Yahoo Cloud Serving Benchmark*, Springer Nature Switzerland AG 2021, K. Arai et al. (Eds.): FTC 2020, AISC 1289, pp. 271–281, 2021.
- [21] *Liste nationale des médicaments et autres produits pharmaceutiques essentiels*, Cameroun, 2017.
- [22] Moubaric KABORE, *Application du framework map-reduce à des groupes de données massives*, mémoire de master en Informatique, Université Joseph KI-ZERBO, 2017.

# Pitch Contour Stylization by Marking Voice Intonation

Sakshi Pandey<sup>1</sup>, Amit Banerjee<sup>2</sup>, Subramaniam Khedika<sup>3</sup>  
Computer Science Department  
South Asian University  
New Delhi, India

**Abstract**—The stylization of pitch contour is a primary task in the speech prosody for the development of a linguistic model. The stylization of pitch contour is performed either by statistical learning or statistical analysis. The recent statistical learning models require a large amount of data for training purposes and rely on complex machine learning algorithms. Whereas, the statistical analysis methods perform stylization based on the shape of the contour and require further processing to capture the voice intonations of the speaker. The objective of this paper is to devise a low-complexity transcription algorithm for the stylization of pitch contour based on the voice intonation of a speaker. For this, we propose to use of pitch marks as a subset of points for the stylization of the pitch contour. The pitch marks are the instance of glottal closure in a speech waveform that captures characteristics of speech uttered by a speaker. The selected subset can interpolate the shape of the pitch contour and acts as a template to capture the intonation of a speaker’s voice, which can be used for designing applications in speech synthesis and speech morphing. The algorithm balances the quality of the stylized curve and its cost in terms of the number of data points used. We evaluate the performance of the proposed algorithm using the mean square error and the number of lines used for fitting the pitch contour. Furthermore, we perform a comparison with other existing stylization algorithms using the LibriSpeech ASR corpus.

**Keywords**—Pitch contour; pitch marking; linear stylization; straight-line approximation

## I. INTRODUCTION

Speech prosody represents the pitch contour of a voice signal and can be used for the construction of linguistic models and their interaction with other linguistic domains, such as morphing and speech transformation [1]. In addition, the pitch contours are used for learning generative models for text-to-speech synthesis applications [2], language identification [3], emotion prediction and for forensics research [4]. Researchers have also used pitch and intensity of sound for predicting the mood of a speaker [5]. In order to remove the variability in the pitch contour, *stylization* is used to encode the contour into meaningful labels [6] or templates [7] for speech synthesis application. According to [8], stylization is a process of representing the pitch contour of the audio signal with a minimum number of line segments, such that the original pitch contour is auditorily indistinguishable from the re-synthesized pitch contour.

Broadly, the stylization of pitch contour either uses statistical learning or statistical analysis models. In *statistical analysis models*, the pitch contour is decomposed into a set of previously defined functions such as polynomial [9],

[10], parabolic [11], and B-splines [12]. In addition, low-pass filtering is also used for preserving the slow time variations in the pitch contours [6]. Recently, researchers have studied the *statistical learning models*, using hierarchically structured deep neural networks for modeling the F0 trajectories [13] and sparse coding algorithm based on deep learning auto-encoders [14]. In general, the statistical learning models require a large amount of data and uses complex machine learning algorithms for training purposes [13], [14]. On the other hand, the statistical analysis models decompose the pitch contours as a set of functions based on the shape and structure of the contour that requires further processing to capture voice intonations of the speaker [9]–[12], [15]. Table I summarizes the algorithms proposed for the stylization of pitch contour. Many successful speech applications use piecewise stylization of the pitch, including the study of sentence boundary [16], dis-fluency [17], dialogue act [18], and speaker verification [19].

In this paper, we use statistical analysis for piecewise decomposition of the pitch contour using the instance of glottal closure or pitch marks to stylize the pitch contour as well as capture the intonation of the speaker’s voice. As mentioned above, the previous works based on the statistical analysis approach [6], [9]–[12], mainly consider the shape and structure of the contour for stylization. For example, [12] use best-fit B-splines to define the segments of a pitch contour, and [11] uses parabolic functions to approximate the pitch contour. In contrary to these approaches, in this paper, we try to model the instances of glottal closure (pitch marks) of the source speaker. An advantage of the proposed approach is that the pitch marks can be used directly as templates for speech synthesis or speech morphing, making the approach suitable for various real-time applications.

The piecewise stylization approximates the pitch contour using  $K$  subset points. That is, if we let  $\{y_n\}_{n=1}^N$  to be the pitch at each instant of time in a speech signal then the piecewise stylization can be defined using function 1, where  $g(y)$  is the stylized pitch,  $a_i$  and  $b_i$  are the slope and intercept of each line at each  $y$  time instant and  $K$  is the subset size required for the stylization of the speech signal. In this paper, we select the pitch marks as a subset of points for the reconstruction of the pitch contour. These pitch marks are selected to fit the pitch contour for capturing large-scale variations. For this, we propose an algorithm using pitch marks as the subset points for the stylization of the pitch contour. The proposed algorithm can be used for retrieving the pitch marks from the voiced region of a pitch contour. In addition, it can

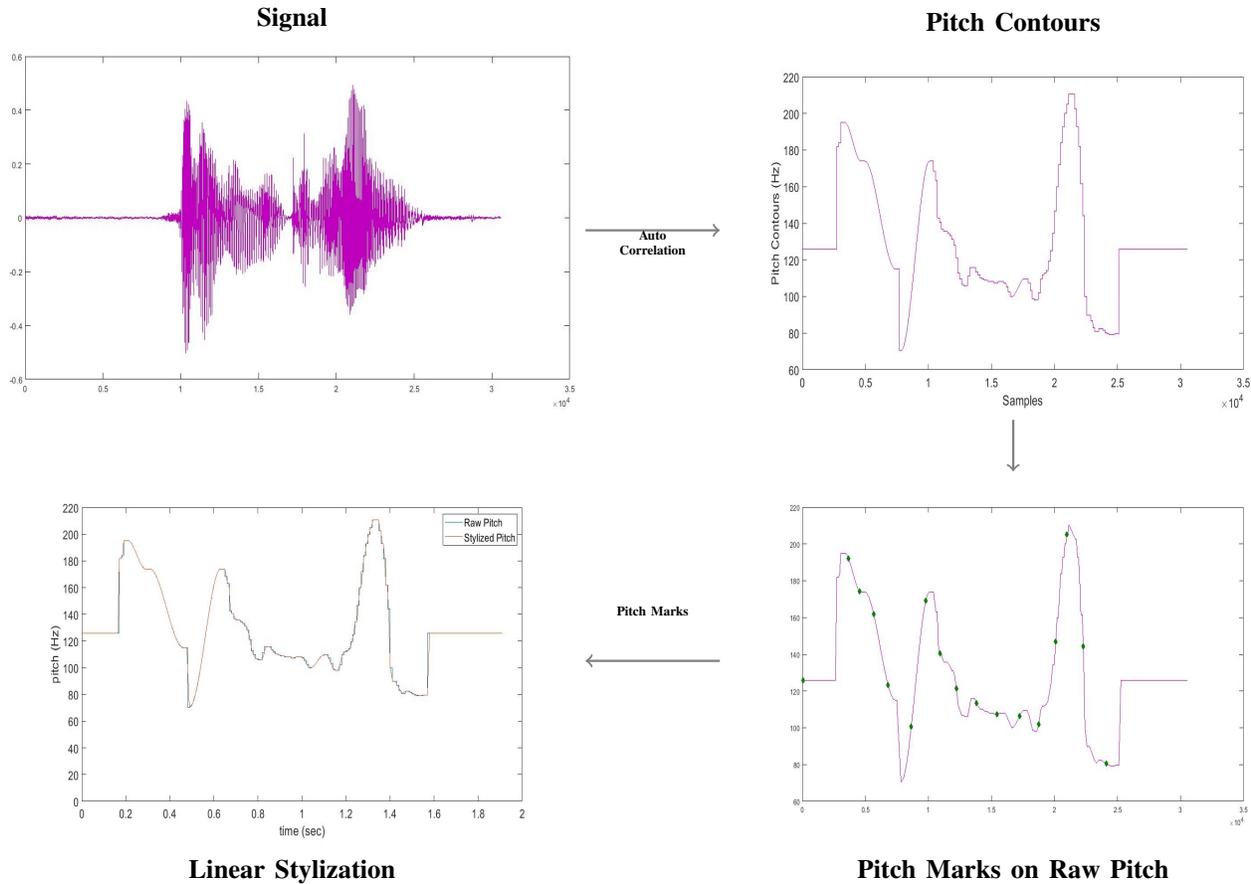


Fig. 1. Block Diagram of Proposed Method.

stylize the voiced and unvoiced region of the contours after pitch smoothing, which can be apt for applications mentioned above and for text-to-speech conversion [24], [25]. The general flow of the proposed methodology on a smoothed pitch contour is shown in Fig. 1. As shown in the figure, the approach uses auto-correlation to detect pitch and uses median filtering with length-3-window to remove sudden spikes to generate the corresponding pitch contour. This is used for extracting the pitch marks and to approximate the pitch contour using linear interpolation. The number of the linear segment depends on the number of pitch marks in the speech signal.

$$g(y) = \sum_{i=1}^{K-1} \sum_{j=i}^{i+1} (a_i y_j + b_i) \quad (1)$$

The proposed work is closely related to [10], [15]. In [10], the authors discuss a computationally efficient dynamic programming solution for the stylization of pitch contour. The approach calculates the MSE (mean square error) of the stylized pitch by predetermining the number of segments  $K$  using [15]. The authors in [15], use Daubechies wavelet (Db10) to perform a multilevel decomposition of the pitch contour and use third-level decomposition to extract the number of extremes ( $K$ ) for the stylization. The choice for the third level is based upon the empirically tested results, which show the

best result for 60% of the cases. However, for the same data 29% of the cases show better results for higher wavelet decompositions or fewer segments, and 11% of the cases have better performance for second level decomposition. On contrary, in our approach, the number of segments is determined by the intonation of the speaker's voice and no pre-determination is required for the same. That is, the number of segments required for pitch stylization is neither pre-determined nor depends on any empirical result. The algorithm computes the optimal number of segments based on the change in the pitch trajectory of the speaker.

To understand the performance of the proposed algorithm, we analyze matrices such as mean squared error (MSE) and the number of line segments ( $K$ ) used for stylization. For our analysis, we use voice samples from the LibriSpeech ASR corpus [26] and the EUSTACE speech corpus [27] to compare the performance with [15]. The experimental results show that in comparison to [15], the proposed methodology uses less number of lines ( $K$ ) to represent the pitch contour of a speech signal. Also, the proposed approach has a lower MSE, in comparison to stylization via wavelet decomposition [15].

The rest of the paper is organized as follows. Section II presents the related work. Section III presents the methodology of the proposed piecewise linear stylization approach. In Section IV, we discuss the experimental setup and simulation

TABLE I. SUMMARY ON EXISTING WORK ON PITCH CONTOUR STYLIZATION

Works	Approach	Algorithm	Application
Xiang Yin et.al. [2016] [13]	Stat. Learning	Hierarchically structured deep neural networks	Statistical parametric speech synthesis
Nicolas Obin et.al. [2018] [14]	Stat. Learning	Deep Auto-Encoders	Learning pitch templates for synthesis and voice conversion.
J't Hart et.al. [1991] [11]	Stat. Analysis	Piecewise stylization	Parabolas's adequate for F0 approximations
Daniel Hirst et.al. [1993] [12]	Stat. Analysis	Stylization using quadratic spline function	Coding and synthesis of curve used for different languages.
D'Alessandro et. at. [1995] [20]	Stat. Analysis	Perceptual model of intonation	Prosodic analysis and speech synthesis
Nygaard et.al. [1998] [9]	Stat. Analysis	Piecewise polynomial approximation	Electrocardiogram (ECG)
Dagen Wang et. at. [2005] [15]	Stat. Analysis	Piecewise stylization via wavelet analysis	Pitch stylization for spoken languages
Prashant K. Gosh et.al.[2009] [10]	Stat. Analysis	Polynomial approximation via dynamic programming	Pitch stylization
Origlia A. et.al.[2011] [21]	Stat. Analysis	Divide and conquer approach	Pitch stylization
Yadav O. P. et.al.[2019] [22]	Stat. Analysis	Piecewise approximation via Chebyshev polynomial	Electrocardiogram (ECG)
Yadav O. P. et.al.[2019] [23]	Stat. Analysis	Chebyshev nodes used for Lagrange interpolation	Electrocardiogram (ECG)
This paper	Stat. Analysis	Piecewise approximation via Pitch Marks	Pitch stylization

results. Finally, Section V concludes the paper.

## II. RELATED WORKS

Pitch Stylization is the process of retrieving pitch contours of an audio signal using linear or polynomial functions, without affecting any perceptually relevant properties of the pitch contours. Broadly, the stylization of pitch contour either uses statistical learning or statistical analysis models. Table I, summarizes the stylization algorithms to show the current state-of-art. In the following, we discuss these approaches in detail.

### A. Stylization using Statistical Learning

Recently, researchers used statistical learning models for pitch contour stylization. In [13], the author uses deep neural networks (DNN) to consider the intrinsic F0 property for modeling the F0 trajectories for statistical parametric speech synthesis. The approach embodies the long-term F0 property by parametrization of the F0 trajectories using optimized discrete cosine transform (DCT) analysis. Two different structural arrangements of a DNN group, namely cascade, and parallel, are compared to study the contributions of context features at different prosodic levels of the F0 trajectory. The authors in [14] propose a sparse coding algorithm based on deep-auto encoders for the stylization and clustering of the pitch contour. The approach learns a set of pitch templates for the approximation of the pitch contour. However, both these approaches use a large data set for training and may not be applicable for stylizing unknown audio samples.

### B. Stylization using Statistical Analysis

In contrary to the previous approaches, statistical analysis models have low computational complexity and can be used for unknown audio samples. This is a well-studied technique for stylization and researchers are actively proposing newer

methods for optimally approximating signals. In [11], authors introduce the concept of piecewise approximation of F0 curve using fragments of a parabola and perform stylization of the contour via rectilinear approximation. Similarly, authors in [12], propose a model for the approximation of fundamental frequency curves that incorporates both coding and synthesis of pitch contours using quadratic spline function. The model is applied for the analysis of fundamental frequency curves in several languages including English, French, Spanish, Italian and Arabic. The author in [20] discuss a new quantitative model of tonal perception for continuous speech. In this, the authors discuss automatic stylization of pitch contour with applications to prosodic analysis and speech synthesis.

In [9] the authors discuss piecewise polynomial approximation for the ECG signals. The paper uses second-order polynomials for reconstructing the signal with minimum error. The authors show that the method outperforms the linear interpolation method in various cases. The concept of polynomial interpolation is applied for the pitch contour stylization in [10]. The paper proposes an efficient dynamic programming solution for the pitch contour stylization with the complexity of  $O(KN^2)$ . It calculates the MSE (mean square error) of the stylized pitch by predetermining the number of segments  $K$  using [15]. The authors in [15], use Daubechies wavelet (Db10) to perform a multilevel decomposition of the pitch contour and use third-level decomposition to extract the number of extremes ( $K$ ) for stylization. The choice for the third level is based upon the empirically testing, showing the best result for 60% of the cases. For remaining cases, 29% shows the better result on higher wavelet decompositions or fewer segments, and 11% of the cases have better performance for second level decomposition. The author in [21] proposes a divide and conquer approach for pitch stylization to balance the number of control points required for the approximation. Recently, in [22], authors used bottom-up time series for the segmentation of the signal, and the restoration is performed using the Chebyshev polynomials. An improvement to the approach

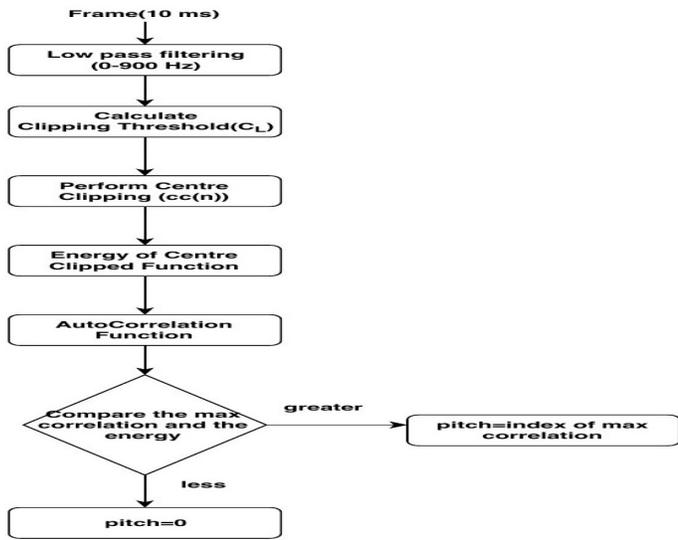


Fig. 2. Pitch Detection.

is proposed by the authors in [23], where the Chebyshev nodes are used for the segmentation of the signal and the approximation is performed using Lagrange interpolation.

### C. Summary

In the proposed algorithm, we use statistical analysis for stylization. Unlike previous works, the number of segments is determined by the intonation of the speaker’s voice and no pre-determination is required for the same. That is, the number of segments required for pitch stylization is neither pre-determined nor depends on any empirical result. The algorithm computes the number of segments based on the changes in the pitch trajectory of the speaker. The pitch marks are used for the linear stylization of the contour. The purpose of choosing pitch marks as the subset is to capture the intonation of the speaker in the pitch contour, which can further be used for various other applications like voice morphing, dubbing and can also act as an input to [9].

## III. PROPOSED METHODOLOGY

The process of pitch stylization is divided into three steps: (1) pitch ( $F_0$ ) determination, (2) pitch marking, and (3) linear stylization. In the following, we discuss these steps in detail.

### A. Pitch Determination

Pitch determination is a process of determining the fundamental frequency or the fundamental period duration [28]. Pitch period is directly related to speaker’s vocal cord and is used for speaker identification [4], emotion prediction [5], real-time speaker count problem [29]–[31]. This is one of the fundamental operations performed in any speech processing application. Researchers have proposed various algorithms for pitch determination, including YAAPT [32], Wu [33], SAcC [34]. However, in this paper, we are using the auto-correlation technique for the same.

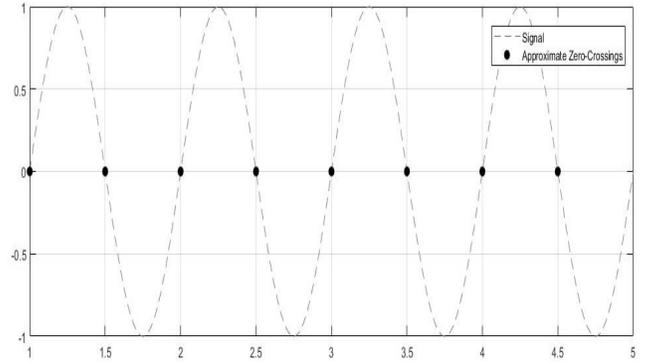


Fig. 3. Zero Crossing Points.

For pitch determination, we first perform low-pass filtering with a passband frequency of 900 Hz. As the fundamental frequency ranges between 80-500 Hz, the frequency components above 500 Hz can be discarded for pitch detection. In order to remove the formant frequencies in the speech signal and to retain the periodicity, center clipping is performed using a clipping threshold ( $C_L$ ) [35]. We choose 30% of the max amplitude as  $C_L$ . We use equation 2 for center clipping, where  $x(n)$  is speech signal and  $cc(n)$  is the center clipped signal.

$$cc(n) = \begin{cases} x(n) - C_L & \text{if } x(n) > C_L \\ x(n) + C_L & \text{if } x(n) < -C_L \end{cases} \quad (2)$$

Furthermore, the energy of the center-clipped signal can be evaluated using equation 3. This can be used for determining the voiced and unvoiced regions in the pitch contour.

$$E_s = \sum_{n=1}^N |x(n)|^2 \quad (3)$$

Finally, we use the autocorrelation method to detect the periodicity of a speech signal. The frame size used for pitch estimation is 10 ms. For a speech signal, autocorrelation measures the similarity of the signal with itself with a time lag. Given a discrete-time speech signal  $x(n), n \in [0, N - 1]$  of length  $N$  and  $\tau$  as the time lag, the autocorrelation can be defined as the following.

$$R(\tau) = \sum_{n=0}^{N-1-\tau} x(n)x(n+\tau) \quad \tau \in [0, 1, \dots, N - 1] \quad (4)$$

We compare the energy  $E_s$  to the maximum correlation value, to determine the pitch of the frame. Fig. 2 gives the flowchart of the steps followed. This step generates the pitch contour  $pcont$  corresponding to a speech signal.

### B. Pitch Marking

A pitch mark can be defined as an instance of the glottal closures in a speech waveform. Previously, researchers have used pitch marks for various applications, such as voice transformation and pitch contour mapping [36]. However, in this paper, we are using pitch marks for pitch contour stylization. The following steps are used for generating the pitch marks.

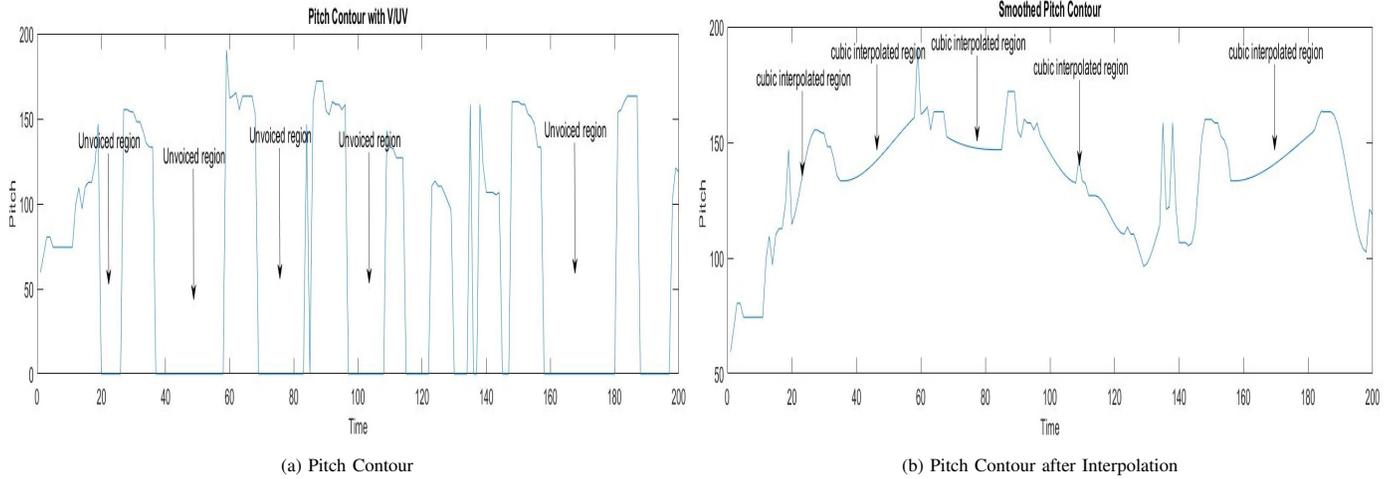


Fig. 4. Smoothed Pitch Contour.

---

**Algorithm 1** Extract Pitch Marks ( $p_{start}, p_{end}$ )

---

- 1: Low pass filtering with cutoff frequency 500Hz
  - 2: Reverse the signal again perform low pass filtering
  - 3: High pass filtering with cutoff frequency 150Hz
  - 4: Reverse the signal again perform high pass filtering
  - 5: The delta function is used to differentiate the filtered signal.
  - 6: The delta signal is again double low pass filtered to remove any noise or phase differences.
  - 7: find the zero crossing points.
- 

---

**Algorithm 2** Pitch Marking for Voiced Region

---

- 1: Extract voiced ( $P_v$ ) and unvoiced ( $P_{uv}$ ) segments from the pitch contour
    - ▷ For each  $i$ th segment  $2i$  is the starting point and  $2i + 1$  is the end point
  - 2: **for** each  $i$ -th voiced segment in ( $P_v$ ) **do**
  - 3:      $p_{start} = get\_start\_point(i)$
  - 4:      $p_{end} = get\_end\_point(i)$
  - 5:      $S_v =$  Extract pitch marks ( $p_{start}, p_{end}$ )
  - 6: **end for**
  - 7: **for** each  $i$ -th unvoiced segment in ( $P_{uv}$ ) **do**
  - 8:      $p_{start} = get\_start\_point(i)$
  - 9:      $p_{end} = get\_end\_point(i)$
  - 10:      $S_{uv} \leftarrow$  Append  $p_{start}, p_{end}$  to the list.
  - 11: **end for**
  - 12:  $pitchMarks \leftarrow$  MERGE ( $S_v, S_{uv}$ ) ▷ Merge two sorted lists in  $O(n)$
- 

Algorithm 1, is used for pitch marking. In the algorithm, we first perform low pass double filtering. It is a process where the first filtered waveform is reversed and fed again to the filter to diminish the phase difference between the input and output of the filter. Subsequently, double high pass filtering is performed to lessen the phase shifts, followed by the application of the delta function for differentiating the filtered signal. The delta signal is again passed through a double low pass filter

---

**Algorithm 3** Pitch Marking after Smoothing

---

- 1:  $smooth\_pcont \leftarrow ptch\_fix(pcont)$
  - 2:  $fsize \leftarrow$  size of the frame,  $f_s * t$
  - 3:  $nof \leftarrow$  number of frames of frame size  $fsize$
  - 4:  $temp \leftarrow 0$
  - 5: **for**  $i \leftarrow 1$  to  $nof$  **do**
  - 6:      $range \leftarrow temp + 1 : temp + fsize$
  - 7:      $pitchMarks \leftarrow$  find pitch marks in each frame from  $smooth\_pcont(range)$
  - 8:      $temp \leftarrow temp + fsize$
  - 9: **end for**
- 

to remove any noise or phase differences. The zero-crossing points are considered as the pitch marks. Zero crossings are points where the signal changes from positive to negative or vice-versa. Fig. 3 marks the zero-crossing points of a simple sine wave.

The pitch marks are a compact representation of the pitch contour. By knowing the position of pitch marks, a very accurate estimation of  $f_0$  contour can be obtained, which can be further utilized for various speech analysis and processing methods [37]. Next, we use Algorithm 1 for determining the pitch marks from the pitch contour ( $pcont$ ) for the following two cases.

1) *Pitch marking for voiced region:* In this approach, we extract the pitch marks from the voiced regions. The classification of the voiced and unvoiced regions can be determined by using the values of  $pcont$ , as the unvoiced regions are marked by zero pitch values. Fig. 4 shows the voiced and the unvoiced regions in the pitch contour. The unvoiced region is marked by black arrows and has zero value. On the other hand, the non-zero values represent the voiced regions, where the pitch marking is performed. For each unvoiced region, we store the first and the last data points in the  $pitchMarks$ . The steps followed for pitch marking are shown in Algorithm 2. In the algorithm, for each  $i^{th}$  voice segment, we extract the pitch marks using Algorithm 1. The extracted pitch marks of the voiced region are stored in  $S_v$  (step 5). Similarly, the starting

---

**Algorithm 4** Linear Stylization Algorithm
 

---

```

1:  $i \leftarrow 1$ 
2: while  $i \leq \text{length}(\text{pitchMarks})-1$  do
3:    $\text{slopes}(i) \leftarrow$  slope of the points  $i$  and  $i + 1$ 
4:    $i \leftarrow i + 1$ 
5: end while
6: for  $i \leftarrow 1$  to  $\text{length}(\text{slopes})$  do
7:    $p \leftarrow \text{pitchMarks}(i)$ 
8:    $q \leftarrow \text{pitchMarks}(i + 1)$ 
9:    $k \leftarrow 1$ 
10:  for  $p$  to  $q$  do
11:     $y = \text{slope}(i) * k + p$ 
12:     $k \leftarrow k + 1$ 
13:  end for
14:   $y$  is the stylized pitch contours
15: end for
    
```

---

and end time instance of the unvoiced regions are stored in  $S_{uv}$  (step 10). Finally, the two lists, i.e.,  $S_v$  and  $S_{uv}$  are merged. As the lists are sorted, the run-time complexity for merging is  $O(n)$ , where  $n$  is the maximum number of elements in both lists.

2) *Pitch marking after smoothing*: Above, the pitch marks are extracted only from voiced frames. As an extension, the unvoiced regions in the pitch contour are interpolated to generate a smoothed pitch contour. The shape-preserving piecewise cubic interpolation is performed in each segment and then median filtering is performed to get the new pitch contour. Fig. 5 shows the smoothed pitch contour. The generated pitch contours are segmented and pitch marks in each segment are stored. The steps followed for pitch marking are shown in the Algorithm 3. In the algorithm, we perform framing to extract the pitch mark from each frame, where  $t$  is the frame size. The main difference between the two approaches is that in the first approach the pitch marking is performed in each voiced region which is of variable length, on the other hand in the second approach the pitch marking is performed in fixed-size frames which gives a better approximation of the pitch contour as seen in the results.

The calculated *pitchMarks* is the input for linear stylization, discussed below.

### C. Linear Stylization

In this, we approximate the stylized pitch contour using linear functions. The linear stylization is done using *pitchMarks*. First, we calculate the slope between two consecutive pitch marks using equation 5, where  $m$  is the slope and  $(x_1, y_1)$  and  $(x_2, y_2)$  are coordinates of the two consecutive pitch marks. The number of slopes generated is equal to the number of straight lines ( $K$ ) needed to approximate the pitch contours of a speech signal.

$$m = \frac{y_2 - y_1}{x_2 - x_1} \quad (5)$$

Next, the intermediate pitches, called stylized pitches, between two consecutive pitch marks are calculated using the straight-line equation. Algorithm 4 shows the detailed steps of

TABLE II. MSE COMPARISON

Samples	Mean Squared Error (MSE)		
	Stylization via Wavelet [15]	Algorithm 2	Algorithm 3
1272-135031-0009.flac	3883.70	118.40	11.19
1272-135031-0010.flac	2999.80	89.30	2.60
1272-141231-0002.flac	1932.80	7192.80	1.17
1462-170138-0000.flac	2941.00	8451.40	19.64
2035-147961-0000.flac	1428.50	3124.50	32.12
422-122949-0025.flac	1669.20	6645.30	6.27
1673-143396-0004.flac	2911.50	17382.00	24.45
2035-152373-0013.flac	3055.50	3471.60	16.32
2803-161169-0009.flac	860.37	4766.20	0.67
7850-73752-0003.flac	1201.70	13129.00	6.64

Linear Stylization. In the algorithm, we use  $k$  to generate the intermediate points between two pitch marks.

## IV. EXPERIMENT AND RESULTS

For the experimental evaluation, we use voice samples from the LibriSpeech ASR corpus [26]. LibriSpeech is a corpus of English speech containing approximately 1000 hours of audio samples of 16kHz, prepared by Vassil Panayotov with the assistance of Daniel Povey. The data is derived from audiobooks (part of LibriVox project) and is carefully segmented and aligned. We test the voice samples for both Algorithm 2, 3 and compare our results with the previously proposed methodology [15]. We use Edinburgh Speech Tools Library for pitch marking [38]. We use the *ptch\_fix* function which is a part of YAAPT pitch tracking Algorithm [39], to perform the pitch smoothing.

### A. Comparison using MSE

Linear stylization approximates the original pitch contour using subset points, the parameter used to test the accuracy of the approximation is mean squared error (MSE). The lower values of MSE suggest a better approximation of the original pitch contours. The stylized pitch contour generated by the proposed algorithms is shown in Fig. 5. Fig. 5a, shows the pitch marks retrieved from the voiced region of the pitch contours. The pitch marks retrieved from smoothed pitch contour are shown in Fig. 5b.

Table II, shows a comparison between the three approaches. From the table, the MSE of Algorithm 2 is higher than the previously proposed speech stylization methodology using wavelet analysis [15]. This is because, in [15] the change points are extracted from each frame, whereas an Algorithm 2 the pitch marks are extracted from the complete signal, without framing of the pitch contour. However, for Algorithm 2, the MSE is considerably low compared to the [15], as the pitch marks are extracted for both voiced and unvoiced regions from each frame. The second approach of stylization yields better results than [15]. This gives a perception that the subset points extracted via pitch marks give better approximations. The average of the corpus is given in Fig. 6, in the figure we plot the values of MSE at log scale to give better representation.

### B. Comparison using Subset Size( $K$ )

The efficiency of the algorithm is tested using the number of segments ( $K$ ), as  $K$  is directly proportional to the number of intermediate points generated. It is evident from the Algorithm

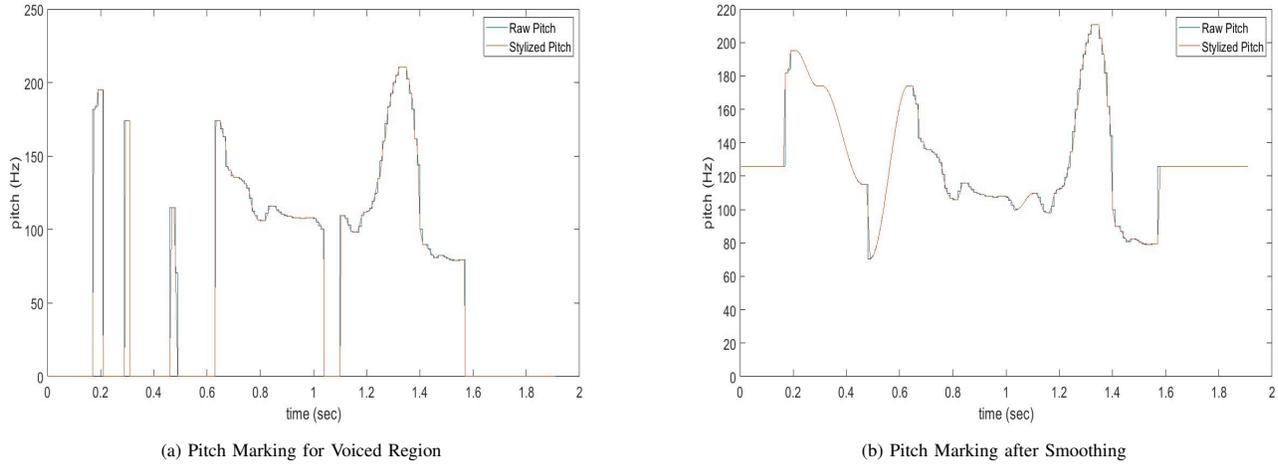


Fig. 5. Original Pitch Contour and Stylized Pitch Contour for Audio Sample “1272-135031-0009.flac [26]”.

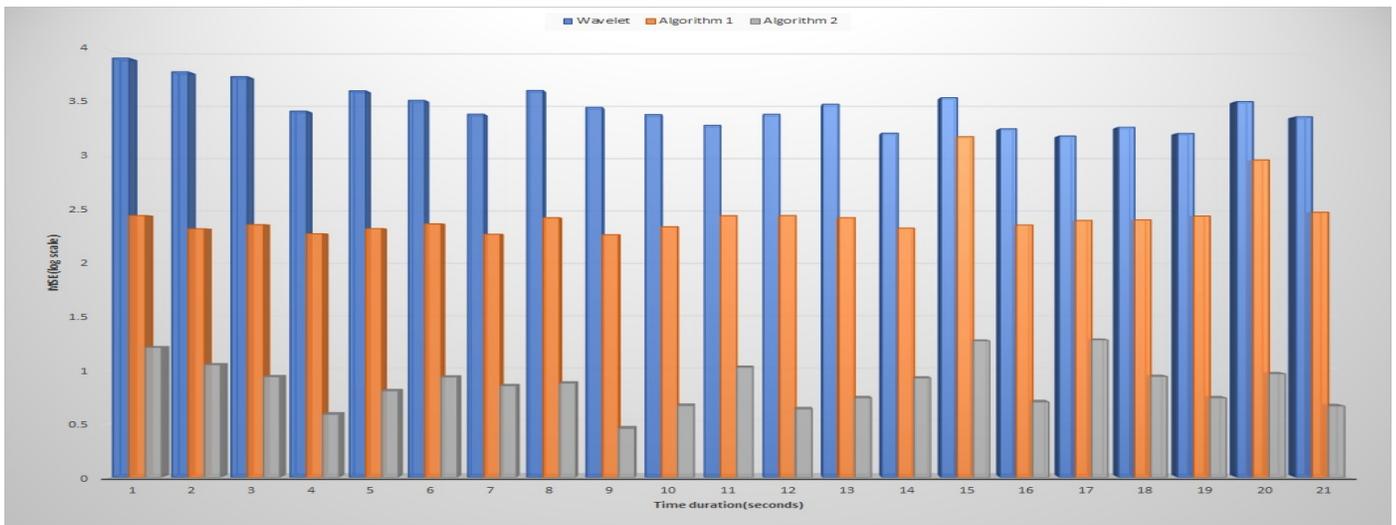


Fig. 6. The Average Mean Square Error by the Three Algorithms.

4 that the more the number of segments in the linear stylization process more is the time complexity. The number of segments  $K$  in the stylized pitch contours generated by the proposed algorithms is shown in Fig. 8. Fig. 8a and 8b, shows the segments obtained by using Algorithm 2 and 3, respectively.

Table III, shows the number of segments generated by the proposed algorithms and compares the same with [15]. The table shows that the proposed algorithms need less number of line segments for the stylized pitch contour in comparison to [15]. For all cases, we find that there is a significant difference in the number of line segments  $K$  generated by the proposed approach in comparison to [15]. The average result of the complete corpus is given in Fig. 7, the results show that on average 82.97% less is the subset size.

### C. Comparison of the Proposed Algorithms

Finally, we compare the number of line segments ( $K$ ) and the MSE of the proposed algorithms. The number of segments

TABLE III. COMPARISON OF  $K$

Samples	No. of lines		
	Stylization via Wavelet [15]	Algorithm 2	Algorithm 3
1272-135031-0009.flac	730	135	250
1272-135031-0010.flac	3656	725	1121
1272-141231-0002.flac	4454	920	1664
1462-170138-0000.flac	4574	1518	2714
2035-147961-0000.flac	4454	2300	3338
422-122949-0025.flac	5568	1159	2165
1673-143396-0004.flac	7225	2827	4316
2035-152373-0013.flac	5681	3144	4860
2803-161169-0009.flac	10189	1948	3007
7850-73752-0003.flac	10382	2873	4970

$K$ , is significantly large when the pitch marks are retrieved from voiced and unvoiced regions after pitch smoothing, Fig. 9. The reason for this is framing, the segments are extracted from each frame which results in a better approximation of the original pitch contour. We can also see from Fig. 10 that mean

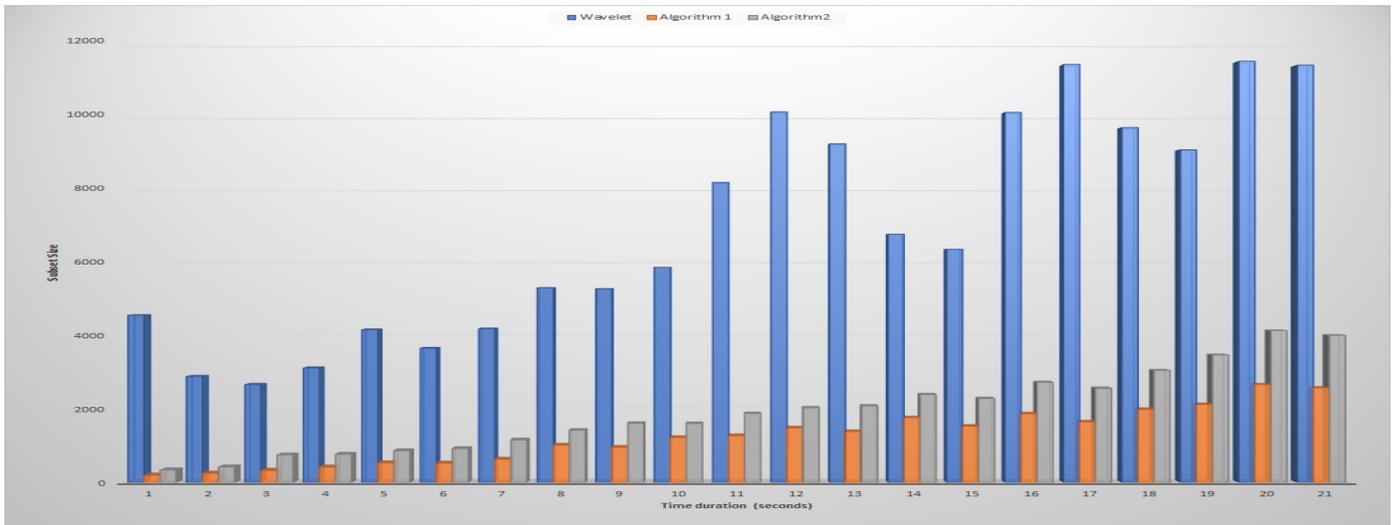
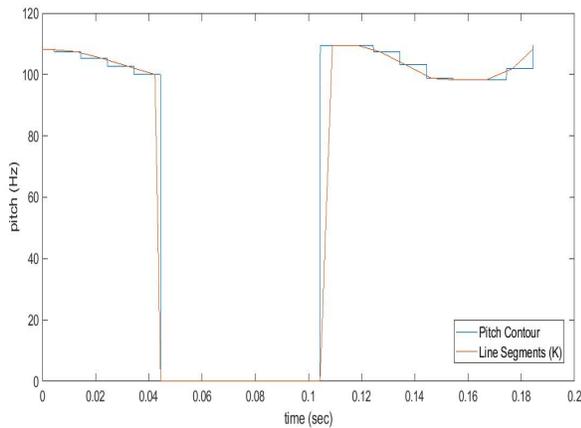
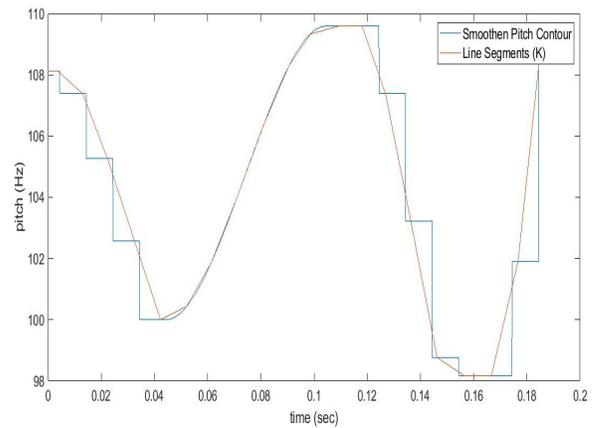


Fig. 7. The Average Subset Size by the Three Algorithms.



(a) Pitch Marking for Voiced Region



(b) Pitch Marking after Smoothing

Fig. 8. Number of Segments  $K$  for Audio Sample “1272-135031-0009.flac [26]”.

square error reduces with an increase in the subset points. The results show that the approach that extracts the pitch marks both from voiced and unvoiced regions using framing is better in terms of MSE, but the complexity of the same is more.

## V. CONCLUSION

The paper proposes two stylization approaches of pitch contour using linear functions. The subset of points used for stylization is the pitch marks on the pitch contour. The pitch marks capture the voice intonation of a speaker. The experimental results show that the proposed algorithms need fewer line segments ( $K$ ) to approximate the stylized pitch contour with a low mean squared error. The results show a better approximation of the pitch contour using the pitch marks in comparison to the change points selected in the wavelet decomposition. First, the pitch marks are extracted from the voiced region of the pitch contours. Further, as an extension, we consider both voiced and unvoiced regions in

the pitch contour to retrieve the pitch marks after performing pitch smoothing. The approximation result is better for the latter approach. In the future, we intend to test the proposed algorithm for more voice samples and apply it for real-time applications like voice morphing, templates to speaker recognition, etc.

## REFERENCES

- [1] B. Gillett and S. King, “Transforming f0 contours,” 2003.
- [2] N. Obin, “Analysis and modelling of speech prosody and speaking style,” Ph.D. dissertation, Ph. D. dissertation, IRCAM, Paris VI University, 2011.
- [3] R. W. Ng, T. Lee, C.-C. Leung, B. Ma, and H. Li, “Analysis and selection of prosodic features for language identification,” in *Asian Language Processing, 2009. IALP’09. International Conference on. IEEE*, 2009, pp. 123–128.
- [4] P. Labutin, S. Koval, and A. Raev, “Speaker identification based on the statistical analysis of f0,” *women*, vol. 16, no. 23.7, pp. 24–9, 2007.

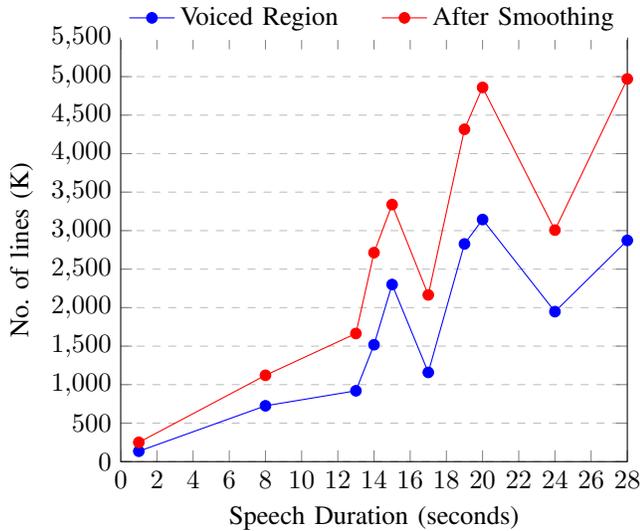


Fig. 9. Number of Segments(K) Vs Time.

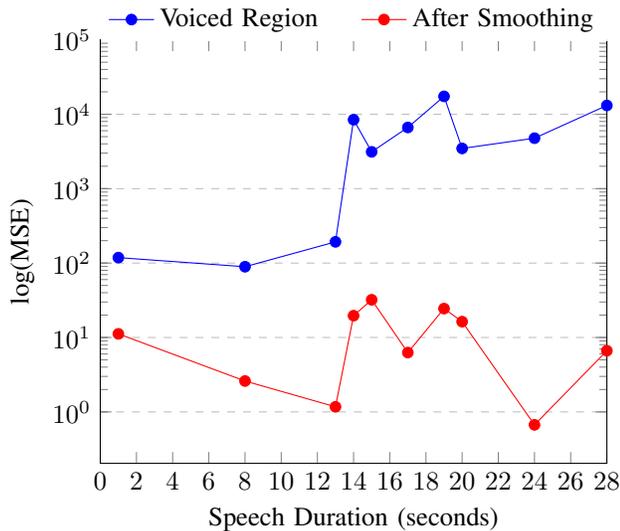


Fig. 10. MSE Vs Time.

- [5] D. Guo, H. Yu, A. Hu, and Y. Ding, "Statistical analysis of acoustic characteristics of tibetan lhasa dialect speech emotion," in *SHS Web of Conferences*, vol. 25. EDP Sciences, 2016.
- [6] N. Obin, J. Beliao, C. Veaux, and A. Lacheret, "Slam: Automatic stylization and labelling of speech melody," 2014.
- [7] R. Dall and X. Gonzalvo, "Jndslam: A slam extension for speech synthesis," in *Proc. Speech Prosody*, 2016, pp. 1024–1028.
- [8] J. Hart, R. Collier, and A. Cohen, *A perceptual study of intonation: an experimental-phonetic approach to speech melody*. Cambridge University Press, 2006.
- [9] R. Nygaard and D. Haugland, "Compressing ecg signals by piecewise polynomial approximation," in *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP'98 (Cat. No. 98CH36181)*, vol. 3. IEEE, 1998, pp. 1809–1812.
- [10] P. K. Ghosh and S. S. Narayanan, "Pitch contour stylization using an optimal piecewise polynomial approximation," *IEEE signal processing letters*, vol. 16, no. 9, pp. 810–813, 2009.
- [11] J. 't Hart, "F 0 stylization in speech: Straight lines versus parabolas," *The Journal of the Acoustical Society of America*, vol. 90, no. 6, pp. 3368–3370, 1991.
- [12] D. Hirst and R. Espesser, "Automatic modelling of fundamental frequency using a quadratic spline function," 1993.
- [13] X. Yin, M. Lei, Y. Qian, F. K. Soong, L. He, Z.-H. Ling, and L.-R. Dai, "Modeling f0 trajectories in hierarchically structured deep neural networks," *Speech Communication*, vol. 76, pp. 82–92, 2016.
- [14] N. Obin and J. Beliao, "Sparse coding of pitch contours with deep auto-encoders," 2018.
- [15] D. Wang and S. Narayanan, "Piecewise linear stylization of pitch via wavelet analysis," in *INTERSPEECH*, 2005.
- [16] E. Shriberg, A. Stolcke, D. Hakkani-Tur, and G. Tur, "Prosody-based automatic segmentation of speech into sentences and topics," *Speech Communication*, vol. 32, pp. 127–154, 09 2000.
- [17] E. Shriberg, R. A. Bates, and A. Stolcke, "A prosody only decision-tree model for disfluency detection," in *EUROSPEECH*, 1997.
- [18] A. Stolcke, N. Coccaro, R. Bates, P. Taylor, C. Van Ess-Dykema, K. Ries, E. Shriberg, D. Jurafsky, R. Martin, and M. Meter. "Dialogue act modeling for automatic tagging and recognition of conversational speech." *Comput. Linguist.*, vol. 26, no. 3, pp. 339–373, Sep. 2000. [Online]. Available: <https://doi.org/10.1162/089120100561737>
- [19] M. Sönmez, E. Shriberg, L. Heck, and M. Weintraub, "Modeling dynamic prosodic variation for speaker verification," in *ICSLP, Sydney, Australia*, August 1998.
- [20] C. d'Alessandro and P. Mertens, "Automatic pitch contour stylization using a model of tonal perception," *Computer Speech and Language*, vol. 9, no. 3, pp. 257–288, 1995.
- [21] A. Origlia, G. Abete, F. Cutugno, I. Alfano, R. Savy, and B. Ludusan, "A divide et impera algorithm for optimal pitch stylization," in *Twelfth Annual Conference of the International Speech Communication Association*, 2011.
- [22] O. P. Yadav and S. Ray, "Piecewise modeling of ecg signals using chebyshev polynomials," in *Computational Intelligence in Data Mining*. Springer, 2019, pp. 287–296.
- [23] —, "Ecg signal characterization using lagrange-chebyshev polynomials," *Radioelectronics and Communications Systems*, vol. 62, no. 2, pp. 72–85, 2019.
- [24] R. Bakis, "Systems and methods for pitch smoothing for text-to-speech synthesis," Nov. 16 2006, uS Patent App. 11/128,003.
- [25] X. Zhao, D. O'Shaughnessy, and N. Minh-Quang, "A processing method for pitch smoothing based on autocorrelation and cepstral f0 detection approaches," in *2007 International Symposium on Signals, Systems and Electronics*. IEEE, 2007, pp. 59–62.
- [26] V. Panayotov, G. Chen, D. Povey, and S. Khudanpur, "Librispeech: an asr corpus based on public domain audio books," in *2015 IEEE international conference on acoustics, speech and signal processing (ICASSP)*. IEEE, 2015, pp. 5206–5210.
- [27] L. White and S. King, "The eustace speech corpus," 2003.
- [28] W. J. Hess, "Algorithms and devices for pitch determination of speech signals," in *Automatic Speech Analysis and Recognition*. Springer, 1982, pp. 49–67.
- [29] A. Banerjee, S. Pandey, and M. A. Hussainy, "Separability of human voices by clustering statistical pitch parameters," in *2018 3rd International Conference for Convergence in Technology (I2CT)*. IEEE, 2018, pp. 1–5.
- [30] C. Xu, S. Li, G. Liu, Y. Zhang, E. Miluzzo, Y.-F. Chen, J. Li, and B. Firner, "Crowd++: Unsupervised speaker count with smartphones," in *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. ACM, 2013, pp. 43–52.
- [31] A. Agneessens, I. Bisio, F. Lavagetto, M. Marchese, and A. Sciarone, "Speaker count application for smartphone platforms," in *Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium on*. IEEE, 2010, pp. 361–366.
- [32] K. Kasi, "Yet another algorithm for pitch tracking:(yaapt)," Ph.D. dissertation, Old Dominion University, 2002.
- [33] M. Wu, D. Wang, and G. J. Brown, "A multipitch tracking algorithm for noisy speech," *IEEE Transactions on Speech and Audio Processing*, vol. 11, no. 3, pp. 229–241, 2003.
- [34] B. S. Lee, "Noise robust pitch tracking by subband autocorrelation classification," Ph.D. dissertation, Columbia University, 2012.

- [35] M. Sondhi, "New methods of pitch extraction," *IEEE Transactions on audio and electroacoustics*, vol. 16, no. 2, pp. 262–266, 1968.
- [36] A. Banerjee, S. Pandey, and K. Khushboo, "Voice intonation transformation using segmental linear mapping of pitch contours," in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*. IEEE, 2018, pp. 1278–1282.
- [37] M. Legát, J. Matoušek, and D. Tihelka, "A robust multi-phase pitch-mark detection algorithm," in *Eighth Annual Conference of the International Speech Communication Association*, 2007.
- [38] P. Taylor, R. Caley, A. W. Black, and S. King, "Edinburgh speech tools library," *System Documentation Edition*, vol. 1, pp. 1994–1999, 1999. [Online]. Available: [http://www.cstr.ed.ac.uk/projects/speech\\_tools](http://www.cstr.ed.ac.uk/projects/speech_tools)
- [39] H. H. Stephen A. Zahorian. Yaapt pitch tracking matlab function. [Online]. Available: <http://www.ws.binghamton.edu/zahorian>

# A Multi-purpose Data Pre-processing Framework using Machine Learning for Enterprise Data Models

Venkata Ramana B<sup>1</sup>, Dr.Narsimha G<sup>2</sup>

Research Scholar, Department of Computer Science and Engineering, JNTU, Hyderabad<sup>1</sup>

Professor, Department of Computer Science and Engineering, JNTU, Hyderabad<sup>2</sup>

**Abstract**—Growth in the data processing industry has automated decision making for various domains such as engineering, education and also many fields of research. The increased growth has also accelerated higher dependencies on the data driven business decisions on enterprise scale data models. The accuracy of such decisions solely depends on correctness of the data. In the recent past, a good number of data cleaning methods are projected by various research attempts. Nonetheless, most of these outcomes are criticized for higher generalness or higher specificity. Thus, the demand for multi-purpose, however domain specific, framework for enterprise scale data pre-processing is in demand in the recent time. Hence, this work proposes a novel framework for data cleaning method as missing value identification using the standard domain length with significantly reduced time complexity, domain specific outlier identification using customizable rule engine, detailed generic outlier reduction using double differential clustering and finally dimensionality reduction using the change percentage dependency mapping. The outcome from this framework is significantly impressive as the outliers and missing treatment showcases nearly 99% accuracy over benchmarked dataset.

**Keywords**—Standard domain length; domain specific rule engine; double differential clustering; change percentage; dependency map

## I. INTRODUCTION

Many enterprises use (probably) use a business data architecture that's an aggregation model, covering all of their details. Most business data models can be conceptual as well as physical. In certain instances, it is self-evident when to create a blueprint. Formal models (often, enterprise data models) seem to be different, And where what was requested has not been completed, or put to use, business use, enterprise data models have been abandoned or remain unfinished. The root cause of these errors is typically is found in a fundamental mathematical error. Initially, it was not obvious what issues the data model wanted to address, and it was not yet clear what was behind these responses. Setting the questions to be asked and the business data model's intent allows things obvious when finished data modeling. There is the option to build business data models unnecessarily, and this causes both cost and time to increase. When problems emerge that need more explanation, go back to the business data model. the use of an enterprise data model is particularly appropriate in the following two cases. The enterprise procedures are being changed due to an extensive reengineering program. Developing an organizational data model in tandem with an enterprise method delivers

tremendous benefit to the process reengineering process. The second implementation in business design is derived from a bottom-up method Integration necessitates the use of a logical data model to display the overlaps between different structures.

Pre-processing of the dataset is one of the primary tasks in any data analytics or data dependent researches or projects. The primary component of the pre-processing ensures removal and replacement of the outliers, removal and replacement of the missing values and sometimes the attribute reductions. Also, in some non-trivial situation removal of the critical and sensitive information is also part of the pre-processing method. The work by H. F. Ladd et al. [1] has clearly suggested many case studies where information hiding is highly important without missing any other crucial information. Nonetheless, the generic datasets, unless related to the personalized recommendation systems, come without the personal identification information sets. Thus, the primary task for any data analyst or a strongly data dependent machine learning engineer are to identify and remove or replace the outliers or missing values [14].

The reduction of the outliers and missing values improves the accuracy as proven by many research attempts such as the work by T. Calders et al. [2]. Nonetheless, many of the parallel research works also have suggested that, removing or replacing the outliers or the missing values directly from the dataset without much customization can directly lead to loss of data and result into incorrect classification or clustering. Thus, it is highly important to generate the data pre-processing method suitable to domain from which the data is originally generated. This belief was initially projected by D. Pedreschi et al. [3] in the year 2008. Through many researchers such as S. Hajian et al. [4] have always emphasised on the data security.

Realizing the need for the domain specific data pre-processing and the need for enterprise scale data pre-processing for domain specific outliers and missing value imputation methods, this work formulates a novel multi-purpose framework for data pre-processing [15].

The rest of the paper is formulated such as, in the Section II, the parallel research outcomes are critically analysed; in Section III the used dataset for this research is described; in Section IV the proposed solutions are formulated using the mathematical models; in Section V, the proposed algorithms based on the mathematical models are discussed; in the Section VI the complete framework is elaborated; in the

Section VII the obtained results are discussed; in Section VIII the comparative analysis is furnished; and finally in Section IX, the research conclusion is formulated.

## II. PARALLEL RESEARCH OUTCOMES

The final outcome of any analytical project is to generate the final results in terms of predictions or projections or classifications or clustering. Nonetheless, all these outcomes solely depend on the cleanness of the data. The cleanness of the data primarily refers to the reduction of the missing values, outliers and sometimes the noises present in the spatial datasets. Hence, a good number of research attempts can be seen in order to propose a framework, which is specific in nature to reduce the anomalies from the datasets.

The work by B. Fish et al. [5] has proposed a method to reduce the anomalies from the datasets using the confidence factors and the confidence metric. This method identifies the outliers and missing values from each domain of the dataset and in case any attribute domain has more than half of the values as anomalies, then the confidence matrix decide, whether that specific attribute contributes to the final classification of the data. In case, that attribute showcases less dependencies, then that specific attribute can be completely discarded from the dataset. Regardless to mention, this method is criticized for lesser accuracy due to the information loss, in spite of the better time complexity.

Yet another research attempt by M. B. Zafar et al. [6] have tried showcasing the effect of anomalies in the final prediction from the dataset and up to certain extend, the effects can be ignored, and the pre-processing stages can be completely ignored. Nonetheless, this work is also highly criticised as this method does not suggest any specific boundaries for domain specific dataset treatments.

In the other direction, the work by T. Kamishima et al. [7] have showcased that the missing value imputation can be completely automated using various machine learning

methods and the accuracy of this method is also remarkable. Nevertheless, this work does not recommend any specific method to handle the domain specific anomalies as explained in Section IV of this literature. In the same direction, the work by M. Hardt et al. [8] has justified the process of weighted parameters for reduction of anomalies using equality principle. However, during a domain specific pre-processing task, it is nearly impossible to identify the weights as equal in the dataset. Thus, this work also cannot justify the need addressed in this literature.

Yet another approach by M. Feldman et al. [9] recommends that, during a pre-processing task, the knowledge from the previous attempts can be utilized to reduce the time complexity. Using the recommendations from anomaly reduction process from the similar datasets can be utilized on the newer datasets and time complexity can be significantly reduced. Regardless to mention, generating the similarity characteristics from two different datasets are a challenge in itself and the added time complexity shall also be considered. This thought is confirmed by the work of C. Dwork et al. [10].

The two recent research outcomes by Z. Zhang et al. [11] and by J. Kleinberg et al. [12] have recommended using the backtracking methods, which is also adopted in this literature and extended in the Section V.

Further, with the detailed understanding of the parallel research attempts, in the next section of this work, the considered dataset for this research is analysed.

## III. DATASET DESCRIPTION

Master and reference data is necessary to ensure continuity across implementations, but it must also be considered scoped to prevent data processing consistency. Since most of the transaction data is almost invariably moved to data centers and monitoring structures, this is predicted to include most organizations' data.

TABLE I. DATASET DESCRIPTION

Attribute Serial #	Dataset Attribute Name	Attribute Alias	Attribute Description	Value Range
1	Employee ID	ID	Unique identification of the employee	Randomized due to identify hiding
2	Job Class	JC	Job category	Retired, Developer, Tester, Student, Etc.
3	Age	AGE	Age of the employee	18 to 70 Years
4	Experience	EXP	Number of years of experiences	0 to 40 years
5	Present Skill Sets	SKILLS_NOW	List of current skill sets	-
6	Upgradation Skill Sets	SKILLS_UP	List of skill sets, which the employee wants to learn	-
7	Job Satisfaction	JS	The level of job satisfaction	0 (Lowest) to 5 (Highest)
8	Job Change Willing ness	JCHA	The desire to change the current job	0 (Lowest) to 5 (Highest)
9	Project ID	PID	Project ID	Randomized due to identify hiding
10	Project Duration	DUR	Duration of the project	In Months
11	Customer Impression	CI	Feedback from the customer	0 (Lowest) to 5 (Highest)
12	Manager Impression	MI	Feedback from the project manager	0 (Lowest) to 5 (Highest)
13	Team Impression	TI	Feedback from the team members (Mean Value)	0 (Lowest) to 5 (Highest)
14	Project Completion Status	CS	Project completion percentage	0 to 100%

In order to carry forward, the research proposed in this work, the ‘The Public 2020 Stack Overflow Developer Survey Results’ [13] is utilized. The description of this dataset is furnished here [Table I].

Further, based on this domain specific dataset, the formulation of the problems is carried out in the next section of this work.

#### IV. PROPOSED SOLUTIONS: MATHEMATICAL MODELS

After the critical analysis of the parallel research works and identification of the research problems in the previous section of this work, in this section of the work, the proposed solutions are presented using mathematical models.

This section primarily focuses on four different pre-processing methods as identification of the missing values, conditional outliers, generic outliers and finally reduction of the attributes.

Lemma 1: The detection of the missing values, using the proposed domain count iterative method, reduces the time complexity.

Proof: The domain count of any dataset shall be realized as the maximum number of elements without the missing or null values. Hence, the maximum count will ensure that the maximum number of elements are considered without the missing values and in case of all missing values, the complete tuple is ignored.

Assuming that, the total dataset,  $DS[]$ , is a collection of multiple domains,  $D[]$ , and each domain is again collection of multiple data points,  $D_i$ . Thus, for a  $n$  number of domains or attributes, the initial relation can be formulated as,

$$DS[] = \sum_{i=1}^n D[](i) \quad (1)$$

Also, assuming that each domain is consisting of  $m$  number of data points, thus, this relation can be formulated as,

$$D[](i) = \sum_{j=1}^m D_j \quad (2)$$

Further, assuming that, the method  $\Phi$ , is responsible for identification of the number of data points without the missing or null values. Then,  $\lambda$  being the count of data points, this proposed function can be formulated as,

$$\lambda = \Phi(D[](i)) \quad (3)$$

Subsequently, the count of data points from each domain can be presented as  $\lambda[]$  and can be formulated as,

$$\lambda[] = \forall [D[](X)] \quad (4)$$

Further, assuming the maximum value from the  $\lambda[]$  collection is  $\delta$ , then this can be formulated as,

$$\delta =_{MAX} [\lambda[]] \quad (5)$$

Further for domain the count of the number of data points,  $Y$ , must be compared with the maximum data point count,  $X$ , using the divide and conquer method as following.

$$\begin{aligned} & \text{Iff } \delta > \lambda[i], \\ & \text{Then, Compare } \delta/2 > \prod_{j=1}^{i/2} (\lambda[i]) \\ & \text{Else, Compare } \delta/2 > \prod_{j=i/2+1}^i (\lambda[i]) \end{aligned} \quad (6)$$

Henceforth, if the count of data points is less than the expected count of the data points in first or second half of the domain, then the process must be repeated to identify the missing values only in that half of the domain and the process shall be repeated iteratively to identify all missing values.

Further, the time complexity of this proposed method is analysed against the generic method.

Assuming that, a total of  $k$  number of iterations has to be performed for  $n$  number of domains, thus the time complexity,  $T_1$ , can be formulated as,

$$T_1 = 1 + n/2 + n/4 + \dots + n/k \quad (7)$$

This can be re-written as,

$$T_1 = O(k \log_2 n) \quad (8)$$

In the other hand, for the similar identification, using the generic methods, thus the time complexity,  $T_2$ , can be formulated as,

$$T_2 = k * n \quad (9)$$

It is natural to realize that

$$T_1 \ll T_2 \quad (10)$$

Hence, the proposed method for outlier detection significantly reduces the time complexity with higher accuracy.

Further, the conditional outliers are addressed and resolved.

Lemma 2: The outliers within the valid range of the data, can be removed using the domain specific rule sets.

Proof: The dataset contains multiple outliers and can be residing in the valid range of data. Thus, the domain specific outliers must be addressed with the valid set domain specific rule engine.

Assuming that, the domain specific rulesets or rule engine,  $R[]$ , is a collection of individual rules,  $R_i$ . Thus, a total number of  $n$  rules, this relation can be formulated as,

$$R[] = \sum_{i=1}^n R_i \quad (11)$$

Further, from Eq. 1, the dataset is fetched and validated against the ruleset for removal of the outliers as,

$$R[]|DS[] \rightarrow \begin{cases} \text{Valid, } DS[] \\ \text{Invalid, } DS'[] \end{cases} \quad (12)$$

The reduced dataset,  $DS'[]$  shall be identified as domain specific outlier reduced dataset.

The following table defines the initial rulesets, specific to this project [Table II]:

TABLE II. DOMAIN SPECIFIC OUTLIER DETECTION RULESETS

Rule #	Ruleset Description		
	Target Rule	Validation Rule	Rule Outcome
1	Job_Satisfaction >=4	Job_Change>=3	Outlier
2	Job_Satisfaction >=5	Job_Change<=2	Not Outlier
3	Job_Satisfaction >= 3	Job_Satisfaction = Job_Change	Outlier
4	Experience>0	SKILLS_NOW is NULL	Outlier
5	Experience>0	SKILLS_NOW is NOT NULL	Not Outlier
6	Experience<=0	SKILLS_UP is NULL	Outlier
7	Experience=0	SKILLS_UP is NOT NULL	Not Outlier
8	Completion_Status is High	Customer_Rating is low	Outlier
9	Completion_Status is High	Customer_Rating is High	Not Outlier

Further, the generic outliers are addressed and resolved.

Lemma 3: The Double Clustering method, must be utilized to identify the outliers in the dataset.

Proof: Assuming that the complete dataset is denoted as  $D[]$  and each attribute in the dataset is assumed to be presented as,  $A_x$  for total of  $n$  number of attributes. Hence, the following relation can be formed.

$$D[] \rightarrow \langle A_1, A_2, A_3, \dots, A_n \rangle \quad (13)$$

Here, each and every attribute is considered to have their own domain with  $m$  number of records each and the data elements are denoted as  $D_i$ , which can be represented as,

$$A_x[] = \sum_{i=1}^m D_i \quad (14)$$

Further, the Euclidian distance between the data points can be considered as the similarity measure and the total distance set is represented as  $\lambda[]$ , then,

$$\lambda[] = \int_{i=1}^n |D_i - D_{i+1}| \quad (15)$$

Further, the Euclidian distance between the elements of  $\lambda[]$  are calculated,

$$\bar{\lambda}[] = \int_{i=1}^{n-1} |\lambda_i - \lambda_{i+1}| \quad (16)$$

The new  $\bar{\lambda}[]$  set defines the relation between the elements based on their similarities.

Furthermore, the repetitive iteration of the Eq. 16 can measure the similarities with deeper and contextual aspect, which can be represented as,

$$\bar{\lambda}_k[] = \int_{i=1}^{n-k} |\bar{\lambda}_i - \bar{\lambda}_{i+1}| \quad (17)$$

Thus, based on the similarity measures of Euclidian distance of the similarity measures of the elements and the Euclidian distance of the similarity measures of the Euclidian distances, the final cluster centroids can be calculated as,

$$C[] = \bar{\bar{\lambda}}_k[] = \frac{\bar{\lambda}_k[]}{\left| \lambda_i - \lambda_{i+1} \right|_{i=0}^n} \quad (18)$$

Further, the attribute reduction process is formulated.

Lemma 4: The domain specific dependency map can build the dimensionality reduced dataset.

Proof: Any two attributes or parameters in the existing dataset shall be compared to identify the change percentage in the complete domain. The parameters with highest amount of change percentages corresponding to the class variable shall define the reduced dataset and the parameters with less change percentage shall not be part of the final dataset.

Assuming that, the domain of the class variable,  $DC[]$ , is compared with two attributes,  $D1[]$  and  $D2[]$ , from the actual dataset for identification of the change percentages. Assuming,  $\Phi$  is the function responsible for change detection, thus this can be formulated as,

$$\Phi(DC[] \triangleright D1[]) \rightarrow n_1 \quad (19)$$

And,

$$\Phi(DC[] \triangleright D2[]) \rightarrow n_2 \quad (20)$$

Here,  $n_1$  and  $n_2$  are the change percentages.

Considering,  $n_1 < n_2$  and  $DR[]$  is the reduced dataset, then as per the proposed lemma, the  $DC2[]$  shall be part of the reduced dataset.

$$DR[] \leftarrow DC2[] \quad (21)$$

Similarly, the dependency map can be created such as Table III.

Here, the dependency map clearly suggests the priority of the attributes to be included in the final reduced dataset, as,

$$DR[] \leftarrow D2 > D3 > D4 > D1 > D5 > D6 : DC \quad (22)$$

TABLE III. DOMAIN DEPENDENCY MAP

	D1	D2	D3	D4	D5	D6	DC
D1	0	8	39	71	75	65	100
D2	72	0	58	71	74	81	100
D3	69	27	0	72	73	82	100
D4	72	55	18	0	74	84	100
D5	71	3	43	70	0	80	100
D6	73	24	65	71	73	0	100
DC	73	24	65	71	73	84	0

Further, accuracy must be verified with time complexity to realize the best possible reduced set.

In the results section of this work, the time complexity and accuracy are analysed for building the final reduced dataset.

Henceforth, in the next section of this work, the proposed algorithms are furnished based on the proposed mathematical models of the solutions.

### V. PROPOSED SOLUTIONS: ALGORITHMS

After the detailed analysis of the problems and formulation of the proposed solutions using the mathematical models, in this section of the work, the proposed algorithms are furnished here in this section of the work.

Firstly, the iterative missing value replacement algorithms are furnished here.

<b>Algorithm - I:</b> Detection and Replacements of Missing Values using Standard Domain Length (DMV-SDL) Algorithm
<b>Inputs:</b> Dataset, DS[]
<b>Output:</b> Final Missing Value Replaced Dataset, DSF[]
<b>Algorithm:</b> Step - 1. Import the dataset, DS[] Step - 2. For each attribute in DS[] as DS[i] a. Count the non-missing value fields as N[i] Step - 3. Find Max(N[i]) as CN Step - 4. For each N[i] a. If $N[i]/2 < CN/2$ b. Then, Check for missing values in DS[i][0] to DS[i][(N[i]/2)] and Add DS[i] to DST[] c. Else If $N[i]/2 > CN/2$ d. Then, Check for missing values in DS[i][(N[i]/2)] to DS[i][(N[i])] and Add DS[i] to DST[] e. Else, f. Mark DS[i] as No Missing Value Fields and Add DS[i] to DSF[] g. Repeat Step - 4 for CN/n with n from 4 to CN Step - 5. For each attribute fields in DST[] as DST[j] a. Calculate the domain moving average Avg_DST[j] and replace with missing values b. Add DST[j] to DSF[] Step - 6. Return DSF[] as missing value cleared dataset

The proposed algorithm is primarily based on the divide and conquer method and thus, demonstrates a huge improvement in terms of time complexity.

Also, the proposed algorithm is capable of reducing the total rows if all the fields are missing. In measurements, ascription is the way toward supplanting missing information with subbed values. There are three fundamental issues that missing information causes: missing information can present a generous measure of predisposition, make the taking care of and investigation of the information more challenging, and make decreases in efficiency. In other words, when at least one quality is absent for a case, most factual bundles default to disposing of any case that has a missing worth, which may present inclination or influence the representativeness of the outcomes. Ascription saves all cases by supplanting missing information with an expected worth dependent on other accessible data.

Secondly, the domain specific outlier removal algorithm is furnished here.

<b>Algorithm - II:</b> Outlier Removal using Domain Specific Rule Engine (OR-DSRE) Algorithm
<b>Inputs:</b> Dataset, FDS[] Rule Engine, RE[]
<b>Output:</b> Outlier Reduced Dataset, FFDS[]
<b>Algorithm:</b> Step - 1. Building the rule engine, RS a. Rule 1: Job_Satisfaction $\geq 4$ and Job_Change $\geq 4$ b. Rule 2: Job_Satisfaction $\leq 2$ and Job_Change $\leq 2$ c. Rule 3: Job_Satisfaction = 5 and Job_Change = 5 d. Rule 4: Job_Change $\geq 3$ and Job_Change $\geq$ Job_Satisfaction e. Rule 5: Experience $> 0$ and SKILLS_NOW is NULL f. Rule 6: Experience $\leq 0$ and SKILLS_UP is NULL g. Rule 7: Completion_Status $> 50\%$ and Customer_Rating $< 3$ h. Rule 8: Completion_Status $> 70\%$ and Customer_Rating $< 4$ i. Rule 9: Completion_Status $> 95\%$ and Customer_Rating $< 5$ j. Rule10 to Rule27: Not included in this paper due to page limit constraints Step - 2. Import the dataset, FDS[] Step - 3. For each attribute in FDS[] as FDS[i] a. If FDS[i][0..n] match (RS) b. Then, Mark as outlier and remove c. Else, Mark FDS[i] in FFDS[] Step - 4. Return FFDS[]

Abnormalities, or anomalies, can be a difficult issue when preparing AI calculations or applying factual methods. They are regularly the aftereffect of mistakes in estimations or extraordinary framework conditions and in this way don't depict the normal working of the basic framework. To be sure, the best practice is to actualize an anomaly expulsion stage prior to continuing with additional examination.

Sometimes, exceptions can give us data about confined peculiarities in the entire framework; so, the location of anomalies is a significant cycle due to the extra data they can give about your dataset.

Thirdly, the generic outlier removal algorithm is furnished here.

<b>Algorithm - III:</b> Double Differential Outlier Detection & Replacement (DDOD-R) Algorithm
<b>Input:</b> Dataset, FDS[]
<b>Output:</b> Outlier Replaced Dataset, FFDS[]
<b>Algorithm:</b> Step - 1. Import the dataset, FDS[] Step - 2. For each attribute in FDS[] as FDS[i] a. Calculate the element difference as $DIFF[j] = Abs[FDS[i][j] - FDS[i][j+1]]$ Step - 3. For each element in DIFF[] as DIFF[i] a. Calculate the element difference as $DIFF\_Second[j] = Abs[DIFF[i][k] - DIFF[i][k+1]]$ Step - 4. Apply k-Mean Clustering for DIFF[] Step - 5. Apply k-Mean Clustering for DIFF_Second[] Step - 6. Identify the outliers for DIFF_Second[] Step - 7. If DIFF_Second[m] is outlier Step - 8. Then check, a. If $DIFF[i][k]$ is outlier b. Then mark $FDS[i][j]$ as outlier c. Else if, $DIFF[i][k+1]$ is outlier d. Then mark $FDS[i][j+1]$ as outlier Step - 9. For each outlier in $FDS[i][j]$ a. Calculate the moving average and replace the outliers Step - 10. Repeat from Step - 2 until all outliers are detected Step - 11. Return the final dataset as FFDS[]

Clustering or grouping is the errand of collection a bunch of items so that objects in a similar gathering are more

comparative to one another than to those in different clusters. It is a fundamental undertaking of exploratory information mining, and a typical strategy for factual information investigation.

Fourthly, the attribute reduction algorithm is furnished here.

<b>Algorithm - IV:</b> Change Percentage Oriented Dependency Map based Attribute Reduction (CPODM-AR) Algorithm
<b>Input:</b> Dataset, FFDS[]
<b>Output:</b> Reduced Dataset, FFFDS[]
<b>Algorithm:</b> Step - 1. Import the dataset, FFDS[] Step - 2. For each attribute in FFDS[] as FFDS[i] a. Calculate the change percentage, $CDP[i] = FFDS[i]$ with $FFDS[0..(i-1)]$ Step - 3. For each element in CDP[] a. If $CDP[i] < CDP[i+1]$ b. Then, remove $FFDS[i]$ and calculate the Classification accuracy as $CA[i]$ c. If $CA[i] > CA[i+1]$ d. Then, Assign $FFDS[i]$ to $FFFDS[j]$ e. Else, Assign $FFDS[i+1]$ to $FFFDS[j]$ Step - 4. Return the final dataset as FFFDS[]

### VI. PROPOSED FRAMEWORK

After the detailed analysis of the proposed algorithms in this section of the work, the proposed framework is furnished and discussed [Fig. 1].

The dataset for this research is adopted from the stack overflow developer survey and identified as one of the prominent datasets for enterprise scale research for pre-processing.

The dataset is distributed in two parts as employee dataset, as described already and project dataset, as described in the previous section of the work.

The proposed framework functions in four phases as in the initial phase the missing values from the employee collection are reduced and generates the missing value reduced dataset for employee collection using the DMV-SDL algorithm.

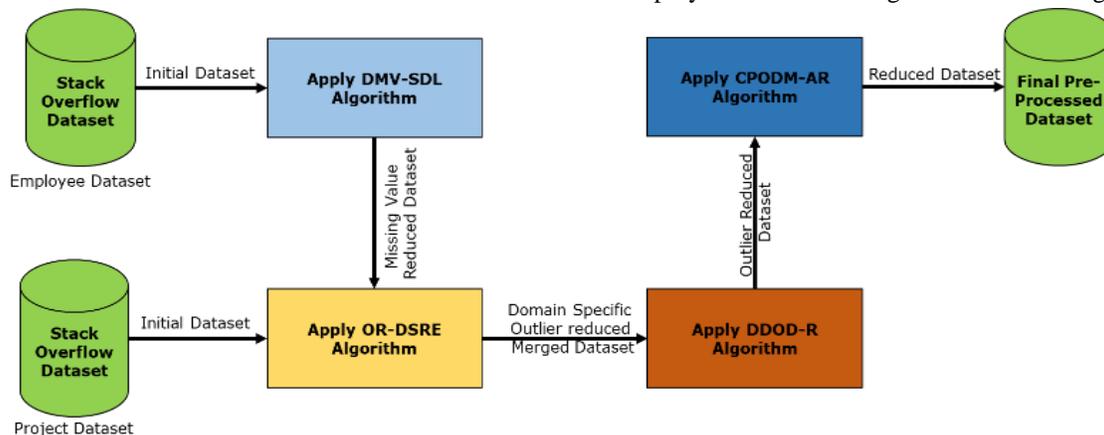


Fig. 1. Multi-Purpose Data Pre-Processing Framework.

The second phase of the proposed framework actually performs two different tasks as reduction of the domain specific outliers from the employee and the project dataset, and further merges the dataset based on the employees' assigned project using the OR-DSRE algorithm.

In the third phase of the proposed framework, the generic outliers are removed using the DDOD-R algorithm from merged dataset with employee and project specific outlines.

In the final phase of the proposed framework, the reduction of the attributes is taken care using the CPODM-AR algorithm where the validation of the reduction process is done using the classification method with the measuring parameters as accuracy and time complexity.

Further, the obtained results from this proposed framework are discussed in the next section of this work.

The dataset for this research is adopted from the stack overflow developer survey and identified as one of the prominent datasets for enterprise scale research for pre-processing.

The dataset is distributed in two parts as employee dataset, as described already and project dataset, as described in the previous section of the work.

The proposed framework functions in four phases as in the initial phase the missing values from the employee collection are reduced and generates the missing value reduced dataset for employee collection using the DMV-SDL algorithm.

The second phase of the proposed framework actually performs two different tasks as reduction of the domain specific outliers from the employee and the project dataset, and further merges the dataset based on the employees' assigned project using the OR-DSRE algorithm.

In the third phase of the proposed framework, the generic outliers are removed using the DDOD-R algorithm from merged dataset with employee and project specific outlines.

In the final phase of the proposed framework, the reduction of the attributes is taken care using the CPODM-AR algorithm where the validation of the reduction process is

done using the classification method with the measuring parameters as accuracy and time complexity.

Further, the obtained results from this proposed framework are discussed in the next section of this work.

## VII. RESULTS AND DISCUSSIONS

The obtained results from the proposed framework and the algorithms are highly satisfactory. In this section of the work, the obtained results are furnished and discussed in five segments.

Firstly, the missing value detection and replacement results are observed from the employee dataset [Table IV].

The results are visualized graphically here [Fig. 2].

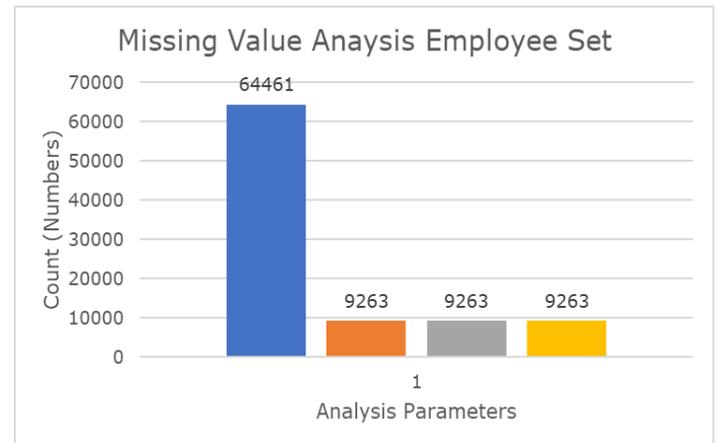


Fig. 2. Employee Dataset Missing Value Analysis

The missing value analysis from the initial employee dataset by the proposed DMV-SDL is highly accurate and demonstrates 100% accuracy.

Secondly, the merged dataset domain specific outlier and missing value analysis, after the merging analysis is here in Table V.

TABLE IV. EMPLOYEE DATASET MISSING VALUE DETECTION AND REPLACEMENT

Total Number of Observation	Initial Number of Missing Values	Missing Values Detected	Missing Values Replaced	Missing Value Detection Accuracy (%)
64461	9263	9263	9263	100

TABLE V. MERGED DATASET MISSING VALUE AND DOMAIN SPECIFIC OUTLIER ANALYSIS

Total Number of Missing Values Identified	Total Number of Missing Values Replaced	Missing Value Detection Accuracy (%)	Total Number of Outliers Identified	Total Number of Outliers Replaced	Outlier Detection Accuracy (%)
156060	156060	100%	17255	15492	89%

The results are visualized graphically here [Fig. 3].

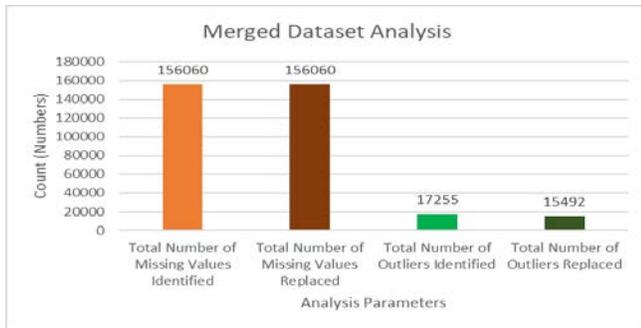


Fig. 3. Merged Dataset Missing Value and Outlier Analysis.

The proposed OR-DSRE algorithm has demonstrated 100% accuracy during the missing value analysis and nearly 90% accuracy during the domain specific outlier detection process.

Thirdly, the generic outlier removal outcomes are furnished here [Table VI].

The results are visualized graphically here [Fig. 4].

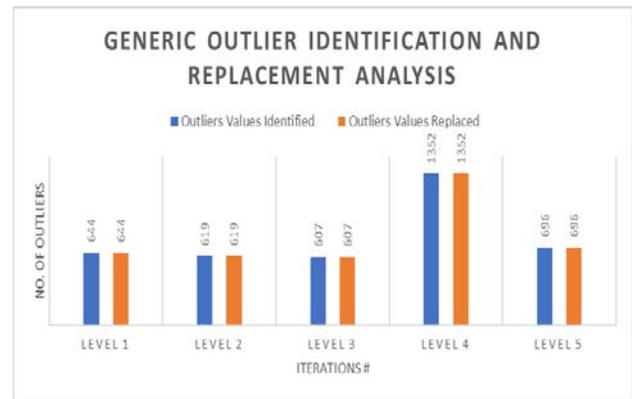


Fig. 4. Generic Outlier Identification and Replacement Analysis.

The iterative outlier identification and removal algorithm have also demonstrated nearly 100% accuracy and the algorithm identifies all the outliers within 5 iterations using the DDOD-R algorithm.

Finally, the attribute reduction results are furnished here [Table VII].

TABLE VI. GENERIC OUTLIER IDENTIFICATION AND REPLACEMENT ANALYSIS

Iteration #	Outliers Values Identified	Outliers Values Replaced
Level 1	644	644
Level 2	619	619
Level 3	607	607
Level 4	1352	1352
Level 5	696	696

TABLE VII. CHANGE PERCENTAGE METRIC

	ID	JC	AGE	EXP	SKILLS_NOW	SKILLS_UP	JS	JCHA	PID	DUR	CI	MI	TI	CS
ID	0	81	81	83	80	84	79	73	8	39	71	75	65	100
JC	21	0	81	83	80	85	76	72	11	58	71	74	81	100
AGE	59	81	0	84	79	84	75	69	27	61	72	73	82	100
EXP	2	81	81	0	79	84	76	72	55	18	73	74	84	100
SKILLS_NOW	6	81	81	82	0	85	79	71	3	43	70	73	80	100
SKILLS_UP	36	80	81	82	79	0	77	73	24	65	71	73	85	100
JS	27	80	81	82	80	84	0	70	61	1	70	73	79	100
JCHA	18	80	80	84	79	84	75	0	24	17	73	73	73	100
PID	8	80	80	83	79	84	76	72	0	40	70	75	67	100
DUR	61	81	81	83	80	85	78	72	61	0	69	73	69	100
CI	52	80	81	84	79	85	77	73	10	8	0	74	73	100
MI	40	80	81	82	80	85	79	70	28	55	70	0	75	100
TI	65	81	82	84	80	85	79	73	67	69	73	75	0	100
CS	100	100	100	100	100	100	100	100	100	100	100	100	100	0

Henceforth, based on the change percentage, the order of the attributes from the highest importance to the lowest is furnished here [Table VIII].

Further, based on the given rank, the attribute reduction process is carried out. The validation of the removal process is based on accuracy of classification and time complexity of processing [Table IX].

It is natural to realize that after the 5<sup>th</sup> iteration, the time complexity is reduced to a greater scale, but the accuracy has

also declined. Thus, the attributes identified till the 5<sup>th</sup> iteration shall be marked as optimal.

The result is visualized graphically here [Fig. 5].

Thus, based on the final analysis the reduced set attributes are furnished here [Table X].

Further, in the next section of this work, the comparative analysis is carried out.

TABLE VIII. ATTRIBUTE RANKING ANALYSIS

Rank	Attribute Number	Attribute Name
Class Variable	0	CS
1	13	TI
2	6	SKILLS_UP
3	4	EXP
4	3	AGE
5	2	JC
6	5	SKILLS_NOW
7	7	JS
8	12	MI
9	8	JCHA
10	11	CI
11	10	DUR
12	9	PID
13	1	ID

TABLE IX. FINAL ATTRIBUTE REDUCTION ANALYSIS

Iteration #	List of Attributes	Classification Accuracy	Time Complexity (msec)
1	13,6,4,3,2,5,7,12,8,11,10,9,1	66	188
2	13,6,4,3,2,5,7,12,8,11,10,9	92	152
3	13,6,4,3,2,5,7,12,8,11,10	97	143
4	13,6,4,3,2,5,7,12,8,11	98	101
5	13,6,4,3,2,5,7,12,8	97	99
6	13,6,4,3,2,5,7,12	96	97
7	13,6,4,3,2,5,7	94	96
8	13,6,4,3,2,5	93	95
9	13,6,4,3,2	92	91
10	13,6,4,3	92	87
11	13,6,4	71	76
12	13,6	69	71
13	13	66	70

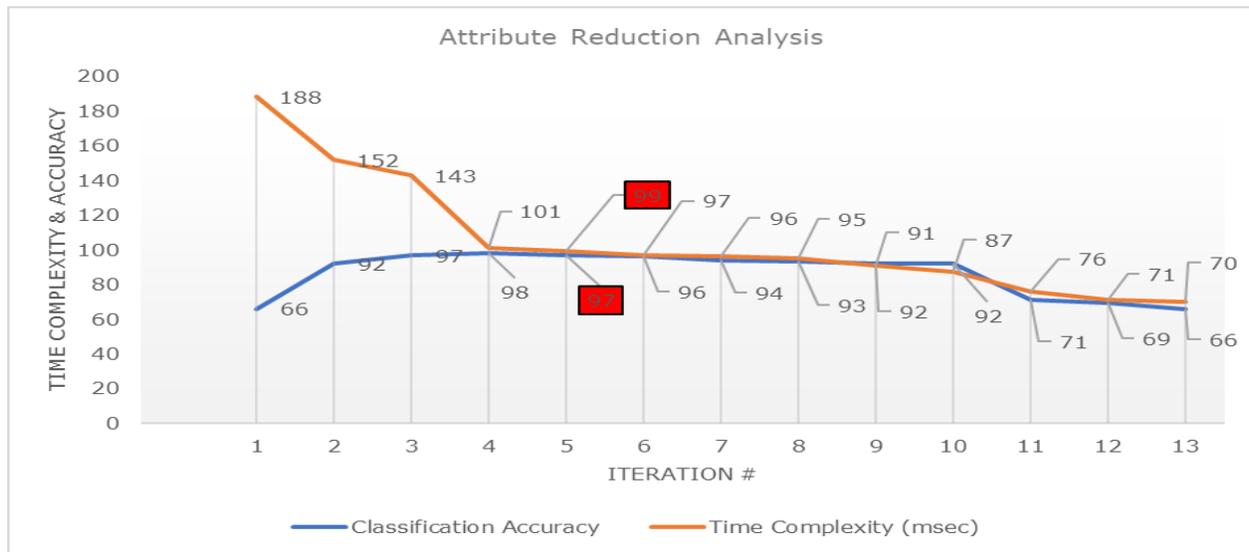


Fig. 5. Attributes Identified Till the 5th Iteration.

TABLE X. FINAL REDUCED DATASET

Rank	Attribute Number	Attribute Name
Class Variable	0	CS
1	13	TI
2	6	SKILLS_UP
3	4	EXP
4	3	AGE
5	2	JC
6	5	SKILLS_NOW
7	7	JS
8	12	MI
9	8	JCHA

### VIII. COMPARATIVE ANALYSIS

After the detailed analysis of the results obtained from the proposed algorithms, in this section of the work, the proposed methods are compared with the parallel research outcomes [Table XI].

It is natural to realize that, the proposed framework deploys more extraction and analysis method for final detection, thus the accuracy in detection of the outliers and missing values are significantly high compared with the existing parallel research attempts. Finally, in the next section of this work, the research conclusion is presented.

TABLE XI. COMPARATIVE ANALYSIS

Research work, Year	Proposed Method	Missing Value Reduction	Outlier Reduction	Domain Information Preservation	Missing Value Detection Accuracy	Outlier Detection Accuracy
M. Hardt et al. [8], 2016	Equality Matrix with Supervised Learning	Yes	No	No	91	-
Z. Zhang et al. [9], 2016	Bias-based Identification	No	Yes	No	-	92
M. B. Zafar et al. [6], 2017	No Reduction	No	No	No	-	-
J. Kleinberg et al. [12], 2017	Risk Score	Yes	Yes	No	95	96
Proposed Framework, 2021	Standard Domain Length, Domain Specific Rule Engine, Double Differential Clustering, Change Percentage Oriented Dependency Map	Yes	Yes	Yes	99	99

## IX. CONCLUSION

This research purposes on the benchmarked dataset by Stack overflow and a synthetic dataset. The proposed DMV-SDL algorithm first processes the employee-related dataset, and due to the nature of the divide and conquer method, the reduction in the time complexity is significant. Further, the stack overflow dataset and the synthetic project-specific dataset are analyzed under the OR-DSRE algorithm for domain-specific outlier imputation and provide a strategic merging of the datasets. Further, DDOD-R algorithm is applied on the merged dataset for generic outlier imputations. The proposed framework demonstrates a nearly 99% accuracy and some cases, up to 100% accuracy. The pre-processed dataset is analyzed under the CPODM-AR algorithm for dimensionality reduction and demonstrates nearly 99% accuracy with reduced time complexity for generic benchmarked classification algorithms. The work finally outcomes into a multi-purpose domain-specific data pre-processing framework for enterprise-scale data to make the data-driven business decisions more reliable.

**Future Enhancements:** Each pre-processed dataset attribute may be linked to as many timelines as required. In both the dependency properties and dependency forms, this is right (start- and end-attributes). In terms of accuracy, mostly related dataset related libraries are strongly recommended matched with the Original datasets.

### REFERENCES

- [1] H. F. Ladd, "Evidence on discrimination in mortgage lending", *J. Econ. Perspectives*, vol. 12, no. 2, pp. 41-62, 1998.
- [2] T. Calders and I. Žliobaitė, "Why unbiased computational processes can lead to discriminative decision procedures" in *Discrimination and Privacy in the Information Society*, New York, NY, USA:Springer, pp. 43-57, 2013.
- [3] D. Pedreschi, S. Ruggieri and F. Turini, "Discrimination-aware data mining", *Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, pp. 560-568, 2008.
- [4] S. Hajian, "Simultaneous discrimination prevention and privacy protection in data publishing and mining", 2013, [online] Available: <https://arxiv.org/abs/1306.6805>.
- [5] B. Fish, J. Kun and Á. D. Lelkes, "A confidence-based approach for balancing fairness and accuracy", *Proc. SIAM Int. Conf. Data Mining*, pp. 144-152, 2016.
- [6] M. B. Zafar, I. Valera, M. G. Rodriguez and K. P. Gummadi, "Fairness beyond disparate treatment & disparate impact: Learning classification without disparate mistreatment", *Proc. 26th Int. World Wide Web Conf.*, pp. 1171-1180, 2017.
- [7] T. Kamishima, S. Akaho and J. Sakuma, "Fairness-aware learning through regularization approach", *Proc. IEEE 11th Int. Conf. Data Mining Workshops*, pp. 643-650, 2011.
- [8] M. Hardt, E. Price and N. Srebro, "Equality of opportunity in supervised learning", *Proc. Adv. Neural Inf. Process. Syst.*, pp. 3315-3323, 2016.
- [9] M. Feldman, S. A. Friedler, J. Moeller, C. Scheidegger and S. Venkatasubramanian, "Certifying and removing disparate impact", *Proc. ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, pp. 259-268, 2015.
- [10] C. Dwork, M. Hardt, T. Pitassi, O. Reingold and R. Zemel, "Fairness through awareness", *Proc. 3rd Innov. Theor. Comput. Sci. Conf.*, pp. 214-226, 2012.
- [11] Z. Zhang and D. B. Neill, "Identifying significant predictive bias in classifiers", *Proc. NIPS Workshop Interpretable Mach. Learn. Complex Syst.*, 2016, [online] Available: <https://arxiv.org/abs/1611.08292>.
- [12] J. Kleinberg, S. Mullainathan and M. Raghavan, "Inherent trade-offs in the fair determination of risk scores", *Proc. Innov. Theor. Comput. Sci. Conf.*, 2017.
- [13] The Public 2020 Stack Overflow Developer Survey Results, <https://insights.stackoverflow.com/survey/2020>.
- [14] Li, Shaoying, et al. "Inferring the trip purposes and uncovering spatio-temporal activity patterns from dockless shared bike dataset in Shenzhen, China." *Journal of Transport Geography* 91 (2021): 102974.
- [15] Wagner, Joachim. "Exports, R&D and Productivity: A test of the Bustos-model with enterprise data from France, Italy and Spain." *MICROECONOMETRIC STUDIES OF FIRMS' IMPORTS AND EXPORTS: Advanced Methods of Analysis and Evidence from German Enterprises*. 2021. 217-222.

# Deep Attention on Measurable and Behavioral-driven Complete Service Composition Design Process

Ilyass El Kassmi<sup>1</sup>, Radia Belkeziz<sup>2</sup>, Zahi Jarir<sup>3</sup>

LISI Laboratory, Computer Science Department  
Faculty of Sciences, Cadi Ayyad University, Marrakech, Morocco

**Abstract**—The web service technology has still proved its effectiveness in the digital revolution we are facing. This success unfortunately raises more and more complex obstacles, particularly related to the service composition. The integration of Non-Functional Requirements (NFRs) in each step of service composition process, starting with abstract service composition specification to the generation of the verified and concrete composed services, represents one of them. Furthermore, this complexity remains more difficult when NFRs are addressed in both quantifiable (i.e. Quality of Service) and behavioral aspects. Despite the relevant contributions present in the literature, this challenge still remains an open issue when considering NFRs modeling, publishing, integrating with each other, and handling conflicts and dependencies in the whole composition's lifecycle. As a consequence, we suggest this contribution that aims to propose an approach showing how to weave efficiently required NFRs with functional requirements in a complete lifecycle composition supporting specification, formalization, model checking verification and integration steps of desired concrete composite service. Patient Health Records in Regional and University Health Centers in Morocco is used as a case study to experiment our approach.

**Keywords**—Non-Functional requirements composition; behavioral non-functional requirements; quantifiable non-functional requirements; model checking; web service composition formalization

## I. INTRODUCTION

In the digital revolution we are facing, Web Service (WS) technology still proved its effectiveness. This technology is widely used to build highly advanced applications that support digital transformation, including artificial intelligence, big data, the Internet of Things, cloud computing, and other emerging technologies. Web Services are defined as loosely-coupled, distributed processes that communicate over a network to perform a specific task and to facilitate interoperability among heterogeneous systems. They can be autonomously developed, decentralized and independently deployable, built and integrated by composition processes to fulfill complex requirements. These requirements, known in software engineering by properties or concerns, are classified mainly into two main classes: Functional requirements (FRs) and Non-Functional Requirements (NFRs). Functional Requirements specify what business-related goals the service composition should achieve. Whereas Non-Functional Requirements define how these services are supposed to fulfill their goals in term of performance and other quality constraints, mainly known as quantifiable QoS properties (e.g. availability, reliability, etc.).

In the software engineering literature, specifically in the service-oriented architectures (SOA), different definitions and classifications of NFRs can be found [1]. We can notice that most of contributions addressing NFRs are focusing on QoS attributes. These attributes describe mainly quality aspects of published services such as availability, cost, response time, reliability, performance, etc. An interesting work classified and analyzed each of 530 studied attributes extracted from 11 industrial requirements specification [2]. The aim of this work is to determine if the NFRs can be really considered as non-functional requirements, or simply be approached as behavioral aspects that can be treated in the same way as the functional requirements. Until now, less efforts are deployed to address unquantifiable requirements in web service composition process. In fact, providing a complete service composition process that details NFR quality-oriented and behavioral integration from specification, modeling, and verification to the composition is always a fastidious task and still an open issue. This difficulty comes from the fact that the web service composition is closely linked to other challenges such as discovery and selection of the most appropriate services, implementing FRs or NFRs, the verification of feature interactions between the non-functional properties of a specific functional service, etc.

Before integrating NFRs with each concerned FR, there is a clear need to specify and formalize them correctly. Some interesting surveys outlined the most used formalization method including Automata, Process Algebra, Petri Nets, etc. [3]. Once NFRs are formalized, some algorithms and techniques are then required to combine them seamlessly with associated FRs to avoid any feature interaction.

To enable our approach to meet the majority of needs in terms of modeling and implementing a complete service composition design process, we are convinced that the use of automata is a better method due to the advantages and the simplicity they offer and also satisfactory results obtained during our previous contributions [4][5]. Therefore, in this contribution we propose an automata modelling approach for Functional and Non-Functional Requirements aimed at providing expert users with increased flexibility to design and integrate numerous complex behavioral NFRs, such as security attributes (e.g. authentication, access-control methods, encryption, etc.), to others custom business-related behavioral NFRs. A varied choice of QoS oriented properties is also integrated in our approach to help selecting the optimal service composition based on attributed weights for each property.

In this perspective, we suggest in this paper a contribution having the advantage of:

- Handling quantifiable and behavioral NFRs using automata-based modeling.
- Publishing, discovering and selecting services implementing behavioral NFR.
- Providing support for composing NFRs with FRs.
- Performing a QoS-driven selection for quantifiable NFRs to generate the best matching service composition.
- Proposing a model checking verification to validate the proposed composition.

The remainder of the paper is organized as follows. Section 2 exposes some interesting contributions tackling service composition integration with NFRs. In Section 3 we present an analysis of QoS-oriented NFR integration to the service composition. In Section 4 we project our contribution to integrate behavioral NFRs to the composition process. In Section 5 we present a novel approach handling integration of both quantifiable and behavioral NFRs to the service composition, whereas Section 6 presents a case study to demonstrate the behavior of this approach. Finally, we conclude by summarizing suggested approach and highlighting future works and upcoming perspectives on Section 7.

## II. RELATED WORKS AND MOTIVATION

The service composition is a widely explored topic. A considerable amount of literature has been published tackling different aspects, problems and perspectives from design time to execution including and not limited to modeling, formalization, discovery, NFR integration, selection, optimization, verification and code generation. In this section we present some interesting contributions addressing this challenge, their limits and similarities with our approach.

In order to conduct and classify the main contributions and provide their motivations in more details, we define a list of research guidelines (RG) as follows:

- RG1 – Are both FR and NFR modeling included in the service composition process?
- RG2 – Does the service composition integrate quantifiable NFRs?
- RG3 – Does the service composition integrate behavioral NFRs?
- RG4 – Is there any validation of the overall behavior of the composed service?
- RG5 – Does the service composition process allow the service publication and discovery based on behavioral NFRs?
- RG6 – Does the service composition provide the optimal service selection based on quantifiable NFRs?

- RG7 – Does the service composition support multiple behavioral NFRs integration applied to the same autonomous service?

Chen et al. proposed in [6] an approach allowing to compose services addressing QoS attributes and dependencies. This work consists of performing a goal softening to reduce the candidate using Pareto techniques combined with Vector Ordinal Optimization in order to find Pareto Optimal Solutions, by considering multiple QoS dependencies criteria to prune uninteresting candidates. Deng et al. proposed in [7] a Correlation-Aware Service Pruning method that improves the QoS of the generated sequential service composition by taking QoS correlations into account in the service selection process. This proposed method is based on a preprocessing algorithm for candidate services to remove irrelevant services. Then a service selection with correlation in adjacent or not adjacent tasks is performed step by step for each task in the service plan to compose the optimal composite services and prune services that are concluded not optimal. In [8], authors proposed a contribution performing exploration of cloud services and returning the optimal solution based on QoS parameters using Eagle Strategy with Whale Optimization Algorithm (ESWOA). According to presented experimentation, the proposed approach got better results compared to other optimization algorithms such as Genetic Algorithm (GA), Hybrid Genetic Algorithm (HGA), Whale Optimization Algorithm (WOA). Y. Liang et al. proposed in [9] a QoS-aware automatic service composition based on QoS correlations between services. They proposed a preprocessing algorithm to address the available services on the pool and generate a service dependency graph. The experimental results are compared to the approach in [10] proposed by Feng et al., which used a method that dynamically refines the composed workflow considering the QoS dependencies, user-provided constraints and QoS constraints. These two approaches offer significant improvements in performance dealing with QoS dependencies. The work in [11] presented by Jatoth et al. proposed a MapReduce-based Evolutionary Algorithm with Guided Mutation MR-EA/G in order to compose Big services with better performance, considering five QoS attributes: price, throughput, availability, reliability and response-time. Jin et al. proposed in [12] a service description modeling associated with a service correlation mapping allowing to get the QoS values of described services automatically. They highlighted the result of comparing results obtained by their proposed approach for candidate service search for the selected QoS parameters: time, cost, availability and reliability against the traditional Genetic Algorithms. Liang et al. proposed another approach in [13] which aims to handle QoS inter-service correlation using Double Information based Cooperative Coevolutionary Algorithm. They use Potter's cooperative coevolutionary framework and provide both local and global knowledge for the dynamic service selection optimization. Wang et al. proposed a Q-Graphplan approach in [14] to solve the QoS-aware automatic service composition problem with multiple QoS criteria constraints. The optimal solution is extracted from the path generation graph using a backward A\* algorithm with the heuristics of the planning graph. The experiment is conducted according to six QoS criteria (response time, price, latency, availability, successful rate, and reliability).

As presented above most cited contributions tackling the integration of NFRs into the service composition focus only on measurable QoS NFRs. Behavioral NFRs are not widely explored, and are commonly restricted to specific security attributes. Also, a verification phase to validate the conformance of constructed composition is often omitted.

Since our objective in this article is to focus on both measurable and behavioral NFRs in a complete service composition process, the rest of this section will be dedicated to present some interesting and similar contributions addressing the same objective.

Lu et al. proposed a model-checking based approach in [15] to verify the satisfaction of behavior-aware privacy requirements in services composition. They used extended interface automata for modeling BPEL process, including a support for privacy semantics. The proposed approach consists on extracting Linear Temporal Logic (LTL) specification from behavioral constraints, but limited to privacy requirements. These specifications are transformed to Promela description in order to allow a model-checking based verification using SPIN. Dou et al. presented in [16] an enhanced version of their proposed method implementing k-means algorithm to ensure privacy-aware cross-cloud service composition based on QoS history records. Sourì et al. proposed in [17] a formal verification approach to tackle cloud service composition problem in the multi-cloud environment in order to decrease the number of cloud providers and obtain optimal results according to QoS parameters. The presented approach proposed a behavioral modeling using a Multi-Labeled Transition Systems (MLTS)-based model checking and Pi-Calculus-based process algebra methods for monitoring functional and non-functional requirements.

Most of proposed approaches are focusing their contribution on adding a specific security layer to the composite service, and consequently ensuring the satisfaction of some security attributes additionally to commonly explored QoS properties. In other hand, Brucker et al. proposed in [18] a framework for modeling, validating and composing secure services. The approach uses a BPMN based modeling to design the user’s functional need and implement the desired security properties based on ConSpec formalization. The overall

framework allows different actors to collaborate starting from requirements definition, modeling, security planning, security validation then generating the secure service composition. The framework supports three non-functional properties which are encryption, cost and availability in order to rank discovered services based on attributed weights.

Table I presents a summary of the above cited contributions according to raised research guidelines. We notice that the focus is mainly conducted to the integration of quantifiable quality-oriented NFRs. Behavioral NFRs (e.g. security attributes) are either neglected, or conducted separately for each security property (e.g. privacy, integrity, encryption, etc.).

This survey incorporated our previous contribution to the proposed classification which consisted of a verification module to validate the correctness of the composition of the designed service. This prompted us to improve the validation of the service composition obtained and to enrich it with appropriate formalization and algorithms, taking into account the specifications of quality and behavioral NFR integrations. This survey incorporated our previous contribution to the proposed classification which consisted of a verification module to validate the correctness of the composition of the designed service. This prompted us to improve the validation of the service composition obtained and to enrich it with appropriate formalization and algorithms, taking into account the specifications of quality and behavioral NFR integrations. Thus, the integration of both behavioral NFRs and quantifiable quality-oriented NFRs in more fine-grained analysis is still an open challenging issue. This motivated us to suggest an approach to tackle the issue of integrating both behavioral and quality-oriented NFRs in the service composition context. Another motivation comes from the work of Rai and Gangadharan that presented a survey consisting on classifying approaches tackling the model checking based verification of web service composition [19]. This survey incorporated our previous contribution to the proposed classification which consisted of a verification module to validate the correctness of the composition of the designed service. This prompted us to improve the validation of the service composition obtained and to enrich it with appropriate formalization and algorithms, taking into account the specifications of quality and behavioral NFR integrations.

TABLE I. CATEGORIZATION OF CITED CONTRIBUTIONS ACCORDING TO RESEARCH GUIDELINES

	[6] Chen et al.	[7] Deng et al.	[8] Gavvala et al.	[9] Liang et al.	[10] Feng et al.	[11] Jatoth et al.	[12] Jin et al.	[13] Liang and Du	[14] Wang et al.	[15] Lu et al.	[16] Dou et al.	[18] Brucker et al.
RG1	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RG2	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓
RG3	-	-	-	-	-	-	-	-	-	✓	✓	✓
RG4	-	-	✓	-	-	-	-	✓	-	✓	-	✓
RG5	-	-	-	-	-	-	-	-	-	-	-	✓
RG6	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓
RG7	-	-	-	-	-	-	-	-	-	-	-	-

### III. DEEP ANALYSIS ON SERVICE-ORIENTED BEHAVIORAL NON-FUNCTIONAL REQUIREMENTS

The literature reveals an increasing attention to quality properties when dealing with NFRs in web service context. However, there are some quality properties that cannot be quantifiable using QoS metrics, e.g. security-oriented properties. Additionally, these properties are not fulfilled with a common behavior, but instead, it may differ from a use case to another. These properties are denoted as “Behavioral NFRs”. Behavioral NFRs are defined as rules, policies or restrictions applied to an abstract service. They aim to integrate specific behaviors before or after the execution of the services they are associated to. Behavioral NFRs integration change depending on the use case. For instance, authentication and access control attributes can be implemented using different methods and schemes, depending on the user’s perspectives and goals. Consequently, unlike quantifiable quality attributes behavioral NFRs integration need a complete understanding of the context, and require a detailed modeling to express in an accurate way the behavioral interactions with collaborative services.

In the literature, studies have suggested different methods to tackle modeling and formalization of NFRs in the context of web service composition such as Process Algebra, Finite State Automata and Petri Nets [20]. Other contributions opted for BPMN as a modeling method for aspect-oriented service composition [21] due to its exhaustivity and expressiveness. In our approach and in order to help ensuring a rigorous composition fulfilling the designer’s requirements, we aim to use a Finite State Automata (FSA) based modeling. Using FSA allows us to extend its formalization to meet our requirements and to proceed to a model checking phase to verify the correctness of designed models according to user’s properties. In the service composition context, FSA allows a rich description of services and their interactions. The modeling phase consists on describing three different sets of requirements: (1) Functional requirements, which are the main business-oriented goals required by the end user. They are translated into an abstract functional automaton (AFA) defining the main functional process describing the interactions between contributing abstract services, (2) Behavioral NFRs representing the desired constraints, policies or restrictions applied to contributing services, and (3) Measurable quality-oriented NFRs dealing with QoS preferences to fit, in order to build the optimal composition. Designing all these NFRs together produces an Abstract Service Composition Automaton (ASCA), which groups all behavioral and quality-oriented scopes applied to the primary AFA.

Definition 1: An Abstract Service (AS) is a service mold, allowing to group a set of desired functionalities (goals) as functional queries. These functional goals need to be fulfilled by some potentially adapted concrete services.

Definition 2: Abstract Functional Automaton (AFA) is a septuple  $AFA = (S, s_0, S_f, T, R_F, R_B, R_Q)$ , where:

- $S$  is a set of states,  $s_0 \in S$  is the initial state,  $S_f \subseteq S$  is a set of final states.

- $T$  is a set of transitions where  $S \times T \times S$  is the transition relation, graphically denoted as  $s^{src} \xrightarrow{t} s^{tar}$ , which means that the transition  $t$  changes the state from the source AS state  $s^{src}$  to the target AS state  $s^{tar}$ .
- $R_F$ ,  $R_B$  and  $R_Q$  express respectively the sets of Functional Requirements  $fr_j$ , Behavioral Requirements and Quality Requirements associated to abstract services. To get the set of functional, behavioral NFRs and quality NFRs for a defined abstract service we use respectively the functions  $functionalReq(as)$ ,  $behavioralReq(as)$  and  $qualityReq(as)$  as follow:

$$functionalReq(s_i) = \{fr_{i1}, \dots, fr_{in} \mid fr \in Q, s_i \in S \text{ and } n \geq 1\}.$$

$$behavioralReq(as_i) = \{br_i \mid br \in R_B \text{ and } s_i \in S\}.$$

$$qualityReq(as_i) = \{qr_{i1}, \dots, qr_{im} \mid qr \in R_Q, s_i \in S \text{ and } m \geq 1\}.$$

In order to complete the modeling of the AFA, the designer proceeds to describe the NFR preferences. We use scope notations to associate NF attributes to a service or a subset of services. Behavioral NFRs are integrated to the AFA using behavioral scopes, illustrated using dotted lines surrounding the service subset.

Since behavioral NFRs constitute an additional restriction over the functional automaton, they are dealt with as a particular workflow having its own description and modeled separately as Behavioral Requirement Automata (BRA). This workflow illustrates the desired NFR behavior with respect to the same automata formalization. Each behavioral NFR is indexed using a behavioral signature [22]. A behavioral signature is a regular expression notation describing the translation of the associated BRA in summarized and verbally understandable way. BRAs are published in a Non-Functional Registry represented by a database indexed using the behavioral signatures. This registry groups all the BRAs with their associated URIs corresponding to associated published concrete services. In Fig. 1, “UHCAuthentication.UHCAccessControl” is an example of a behavioral signature outlining the behavioral scope associated to the abstract service AS2’. This regular expression is summarizing the desired behavior including both Authentication and Access Control. Each behavioral scope in the modeling phase corresponds to an atomic or composite service that needs to be integrated to the current functional composition.

Definition 3: Behavioral Requirement Automaton (BRA) is a quadruple  $BRA = (S, s_0, S_f, T, BS)$ , where:

- $S$  is a set of states,  $s_0 \in S$  is the initial state,  $S_f \subseteq S$  is a set of final states.
- $T$  is a set of transitions where  $S \times T \times S$  is the transition relation, graphically denoted as  $s^{src} \xrightarrow{t} s^{tar}$ , which means that the transition  $t$  changes the state from the source AS state  $s^{src}$  to the target AS state  $s^{tar}$ .

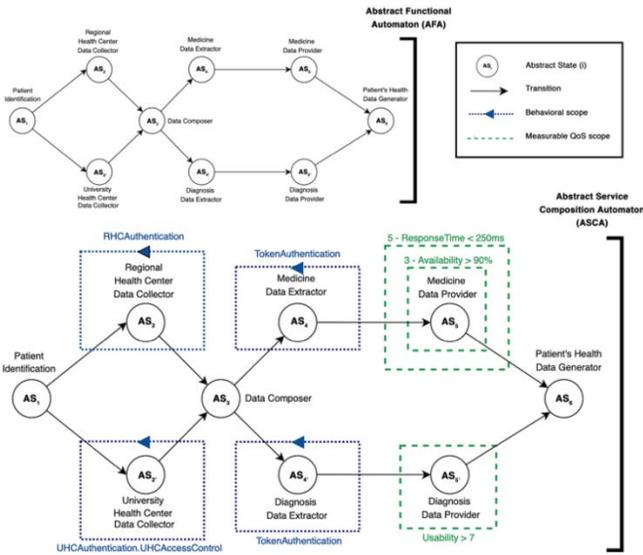


Fig. 1. An Abstract Service Composition Automaton based on the Illustrative Scenario.

In our approach, we distinguish between two types of behavioral NFRs: the pre-execution and the post-execution behavioral requirements. The pre-execution behavioral requirement is illustrated by an arrow in backward direction over the behavioral scope. It aims to be handled before the execution of the associated concrete service, whereas the post-execution behavioral requirement, illustrated by an arrow in forward direction over the behavioral scope, defines the required behavioral process to be performed after the execution of the associated concrete service. For both cases, we proceed to an automata composition allowing to merge the BRAs with the AFA. This composition process for each case is defined below.

**Definition 4:** Prior Execution Behavioral Automata Composition is the merging operation between the Abstract Functional Automaton  $AFA = (S, s_0, S_f, T, RF, RB, RQ)$  and a Behavioral Requirement Automaton  $BRA = (S, s_0, S_f, T)$  to fulfill the prior execution behavioral requirement associated to the state  $s_b$  (i.e. having a pre-execution behavioral scope). The product is a Composition Automaton  $CA = (S, s_0, S_f, T)CA$ , a quadruple described as following:

- $S_{CA}$  is a set of states, such that  $S_{CA} = S_{AFA} \cup S_{BRA}$  and  $S_f \subseteq S_{CA}$ .
- $s_0 \in S_{CA}$ , and  $s_{0(CA)} = s_{0(AFA)}$  when  $s_b \neq s_{0(AFA)}$
- $T_{CA}$  is a set of transitions where  $T_{CA} = T_{AFA} \cup T_{BRA} \cup T_{AFA \rightarrow BRA} \cup T_{BRA \rightarrow AFA}$  such that:
- $T_{AFA \rightarrow BRA}$  is a set of transitions where  $t_1 \in S_{AFA} \times T_{AFA \rightarrow BRA} \times S_{BRA}$  is the transition relation from the state  $s_{b-1}$  directly before  $s_b$  with the initial state  $s_{0(BRA)}$ , graphically denoted as  $s_{b-1} \xrightarrow{t_1} s_{0(BRA)}$ .
- $T_{BRA \rightarrow AFA}$  is a set of transitions where  $t_2 \in S_{BRA} \times T_{BRA \rightarrow AFA} \times S_{AFA}$  is the transition relation from the final states  $s_{fi(BRA)}$  with the scoped state  $s_b$ , graphically

denoted as  $s_{fi(BRA)} \xrightarrow{t_2} s_b$  such that  $s_{fi} \in S_{fi(BRA)}$  and  $i \geq 1$ .

**Definition 5:** Post Execution Behavioral Automata Composition is the merging operation between the Abstract Functional Automaton  $AFA = (S, s_0, S_f, T, RF, RB, RQ)$  and a Behavioral Requirement Automaton  $BRA = (S, s_0, S_f, T)$  to fulfill the post execution behavioral requirement associated to the state  $s_b$  (i.e. having a post-execution behavioral scope). The product is a Composition Automaton  $CA = (S, s_0, S_f, T)CA$ , a quadruple described as following:

- $S_{CA}$  is a set of states, such that  $S_{CA} = S_{AFA} \cup S_{BRA}$ ,
- $s_{0(CA)} = s_{0(AFA)}$ , and  $S_f \subseteq S_{CA}$ .
- $T_{CA}$  is a set of transitions where  $T_{CA} = T_{AFA} \cup T_{BRA} \cup T_{AFA \rightarrow BRA} \cup T_{BRA \rightarrow AFA}$  such that:
- $T_{AFA \rightarrow BRA}$  is a set of transitions where  $t_1 \in S_{AFA} \times T_{AFA \rightarrow BRA} \times S_{BRA}$  is the transition relation from the scoped state  $s_b$  with the initial state  $s_{0(BRA)}$ , graphically denoted as  $s_b \xrightarrow{t_1} s_{0(BRA)}$ .
- $T_{BRA \rightarrow AFA}$  is a set of transitions where  $t_2 \in S_{BRA} \times T_{BRA \rightarrow AFA} \times S_{AFA}$  is the transition relation from the final states  $s_{fi(BRA)}$  with the state  $s_{b+1}$  directly after the scoped state  $s_b$ , graphically denoted as  $s_{fi(BRA)} \xrightarrow{t_2} s_{b+1}$  such that  $s_{fi} \in S_{fi(BRA)}$  and  $i \geq 1$ .

#### IV. DEEP ANALYSIS ON QUALITY-OF-SERVICE NON-FUNCTIONAL REQUIREMENTS IN THE SERVICE COMPOSITION

In the literature, Non-Functional Requirements can be defined and classified in various ways depending on the context of use. Chung and do Prado Leite [23] presented different representations and classifications of NFRs. FURPS+ model is an example of classifications for software quality attributes, which illustrates a software quality tree and aims to address concerns for key types of NFRs and importantly possible correlations among them. Another model is proposed by the international standard for the evaluation of software quality ISO/IEC [24] which is a quality-oriented scheme. Its revised version in 2011 [25] proposed two main models: (1) software product quality model that groups attributes such as reliability, performance, operability, security, maintainability, etc., and (2) Quality in use model, defined using three main attributes: a) Usability in use describing the effectiveness, efficiency and satisfaction in use, b) Flexibility in use dealing with the context conformity, and c) Safety for operator, public and environment. In other hand, Galster and Bucherer [26] proposed a service-oriented taxonomy to classify NFRs. They introduced the quantifiability factor allowing to define how each attribute can be measured. This classification consists on dividing NFRs into three main classes: a) Process requirements, which are properties dealing with service design, discovery, composition and runtime, b) Service requirements, centered on the service and can be derived directly from user needs, and c) External requirements, defining the external economic or legal constraints on the development or deployment process. Authors in [27] proposed a literature review highlighting the most frequently used NFRs in service-oriented context, such as performance, reliability, usability, security, and maintainability. It aims to propose a classification

based on definitions, typologies, types of systems and application domains of NFRs. Another contribution [28] proposes a detailed review classifying the NFR approaches according to different criteria, then providing a qualitative analysis of their scopes and characteristics. This work focuses on the three main classes of NFR approaches which are the Goal-oriented approaches, the Aspect-oriented approaches and the Pattern-based approaches. The work on NFRs integration to service composition has been the subject of various contributions. However, most of proposed works surrounding this topic are limited to quantifiable quality-oriented NFRs, commonly known as Quality-of-Service (QoS) attributes.

In our approach, each quality attribute is defined by a set of metrics (cf. Table II). The designer selects the appropriate quality metrics to apply to a set of abstract service. The measurement correlation expresses whether the best results are associated to higher metric value (Positive: +), or lower metric value otherwise (Negative: -).

In order to select the best matching quality-aware concrete service for a specific abstract service, we apply a weight coefficient to each desired quality metric. This coefficient helps to select the most appropriate services according to user's preferences, when dealing with multiple quality conditions associated to a common set of abstract services. The Web Service Popularity Score [29] (WSPS) was previously introduced to compute the quality measures by introducing a more appropriate and decisive factor to distinguish functionally similar services using an algorithm based on multiple criteria for multiple candidates. In our approach, this allows us to reduce the pool of candidate services by guaranteeing the satisfaction of the multiple criteria quality requirements defined by the designer. In this paper we enhance the Popularity Score metric coverage by integrating some relevant QoS metrics. The covered QoS attributes with their associated metrics and their calculation formulas are depicted in Table II.

TABLE II. TABLE OF QUALITY OF SERVICE ATTRIBUTES AND THEIR APPROPRIATE METRICS

QoS Attribute	QoS Metric	Calculation Formulae
Availability	+ <b>The Availability</b> metric (Av) is the percentage of time, in a specific time interval, during which the service can be reachable and functional. The commonly used formula uses uptime and downtime values.	$Av(s) = Uptime(s)/(Uptime(s) + Downtime(s))$ $Av(s) = MTBF(s)/(MTBF(s) + MTTR(s))$ <i>MTBF is the Mean Time Between Failure, and MTTR is the Mean Time To Repair.</i>
	- <b>The Mean Time To Repair</b> (MTTR) refers to the amount of time required to repair the service and restore it to full functionality.	$MTTR(s) = \sum MT(s) / MN(s)$ <i>MT represents the maintenance time for a specific service, and MN defines the number of Maintenance actions for that service.</i>
Reliability	+ <b>The Mean Time Between Failure</b> (MTBF) refers to the amount of time a service is up before it fails. It is the average (expected) time between two successive failures to reach the service.	$MTBF(s) = \sum OpT(s) / FN(s)$ <i>OpT represents the operational time for the service, where FN defines the number of failures actions for that service.</i>
	- <b>The Failure Rate</b> metric (FR) is the frequency with which the service fails, expressed in failures per unit of time.	$FR(ws) = FN(ws) / T$ <i>FN defines the number of failures actions for the service, while T defines the amount of time.</i>
	- <b>The Defects per Million</b> factor (DPM) refers to the number of defects for each million attempts of user's requests. It is defined as the ratio of the number of defects in the service to the total number of defect opportunities multiplied by 1 million.	$DPM(ws) = FReq(ws) * 1000000 / TReq(ws)$ <i>FReq defines the number of unsuccessful (Failed) Requests, while TReq defines Total Requests performed.</i>
	+ <b>Reliability</b> (Re) refers to the service ability to function according to the agreed upon performance requirements in SLA.	$Re(ws) = [(1000000 - DPM(ws)) / 1000000] * 100\%$ <i>DPM is the Defects Per Million metric.</i>
Response Time	- <b>The Processing Time</b> (Proc) is the amount of time consumed for fulfilling the request by executing the corresponding functions.	$Proc(ws) = \sum ExT(ws) / N(ws)$ <i>ExT defines the elapsed time during the execution of the service, while N is the total number of calls.</i>
	- <b>The Transmission Time</b> (Trans) is the total time for communication between the client and the provider's hosting server.	$Trans(ws) = \sum (SendT(ws) + ReplyT(ws)) / N(ws)$ <i>SendT defines the transmission time during the request sending to the server, while ReplyT is the consumed time during the transmission of the reply from the server. N is the total number of calls.</i>
	- <b>The Response Time</b> (RT) is the amount of time elapsed between sending a request and receiving a response. It is including both transmission and execution time.	$RT(ws) = Trans(ws) + Proc(ws)$ <i>Trans is the Transmission Time and Proc is the Processing Time.</i>
Reputation	+ <b>Usability</b> (Us) is describing the service characteristic of being easy to use. To measure the usability, we consider the users' feedback to rate the services based on their ease of use.	$Us(ws) = \sum UserRating(ws) / NbUse(ws)$
	- <b>The Age</b> (Age) is measured by using the number of days between the last dates of invoke or discover interaction and the current date. We estimate that the best WS is the one that is also recently used.	$Age(ws) = now() - LastCallDate(ws)$ <i>LastCallDate refers to the last date concerning the WS invocation or WS discovering operation.</i>
	+ <b>The Frequency</b> (Frq) metric represents the number of uses of the service by duration (day, week, month or year), and it's presented by the number of use and its duration.	$Frq(ws) = \sum NbUse(ws) / NbMonth(ws)$ <i>NbUse is the total of WS called by each duration and the NbMonth is the number of months where the WS was consumed.</i>
Cost	- <b>Cost</b> (Co) metric represents the incurred fees by service invocation.	

All aforementioned metrics constitute a more fine-grained service metrics taxonomy. The combination of these metrics will help surely to get eligibility (Popularity) of services. In this score, each quality metric is associated to a coefficient represented by an integer from 0 to 5. This coefficient reflects its importance among other proposed metrics when searching user appropriate services. The one which is more important has higher value.

$$WSPS(ws) = \frac{[\sum (Metric(ws) * Coef(Metric))]}{\sum (Coef(Metric))}$$

Metric in {"Av", "MTTR", "MTBF", "FR", "DPM", "Re", "Trans", "Proc", "RT", "Us", "Age", "Frq", "Co"}.

To evaluate the performance of popularity score, Elfirdoussi et al. developed a framework [30] called DIVISE (Discovery and Visual Search Engine). DIVISE is a web service search engine that has the advantage to discover simple, composite or semantic services based on the user's functional needs and quality metrics in order to select the most appropriate service from a generated list of potentially candidate services. We enhance the DIVISE framework for our QoS based selection module in order to automatically select the best matching service using the popularity score computation.

### V. PROPOSED APPROACH

In this paper, our contribution aims to propose a comprehensive approach where the designer has a multitude of options for modeling a reliable service composition including both functional goals and NFRs. The workflow designer gains a total control of which services are meant to be implemented, according to the primary goals (FRs). Then he/she adjusts non-functional customizations by refining how these services are meant to be implemented (NFRs). In fact, we distinguish between two disjoint types of NFRs. Each of these types is fulfilled and treated differently: a) The quantifiable NFRs, commonly qualified as measurable NFRs or Quality-of-Service (QoS) requirements, such as availability, reliability, response-time, cost, etc., and b) the Behavioral requirements, as considered as non-quantifiable requirements, such as security requirements [31]. These NFRs cannot be measured using

common quality metrics. The proposed approach is based on four main phases. For each phase, a dedicated module is implemented. An overview of the composition process with associated modules is illustrated in the Fig. 2.

#### A. Modeling Phase

The modeling module is the first interaction point between the designer and the system. It consists on a modeling tool allowing to draw adapted and easy to understand composition automata. It allows to describe desired functional and non-functional requirements by designing an Abstract Functional Automaton. Below we present the four key components used in the automata modeling module:

1) *States*: Each state is composed of a label which is a non-unique string attribute, and a type to describe whether it is a start, intermediate or final state.

2) *Transitions*: Each transition is identified by two key elements: the source state and the target state. The source state is the state launching the transition, while the target state is the reached state using that transition. Three more attributes can describe transitions which are: The inputs, the guard conditions and the outputs.

3) *Behavioral scopes*: The behavioral scopes are used to specify the states concerned by the behavioral requirement to integrate. They are identified using a string attribute in the form of a regular expression to describe the behavioral signature, in addition to a time indicator to specify whether the associated service will be performed before or after the scoped state's concrete service.

4) *Quality scopes*: The quality scopes are used to define quality restrictions over discovered concrete services. They are identified using three key elements: a) the quality metrics which are the supported quality properties depicted in Table II, b) the metric weight which constitutes the coefficient attributed to the chosen quality metric, c) the quality condition which is an expression describing the desired restrictions over the chosen quality metric.

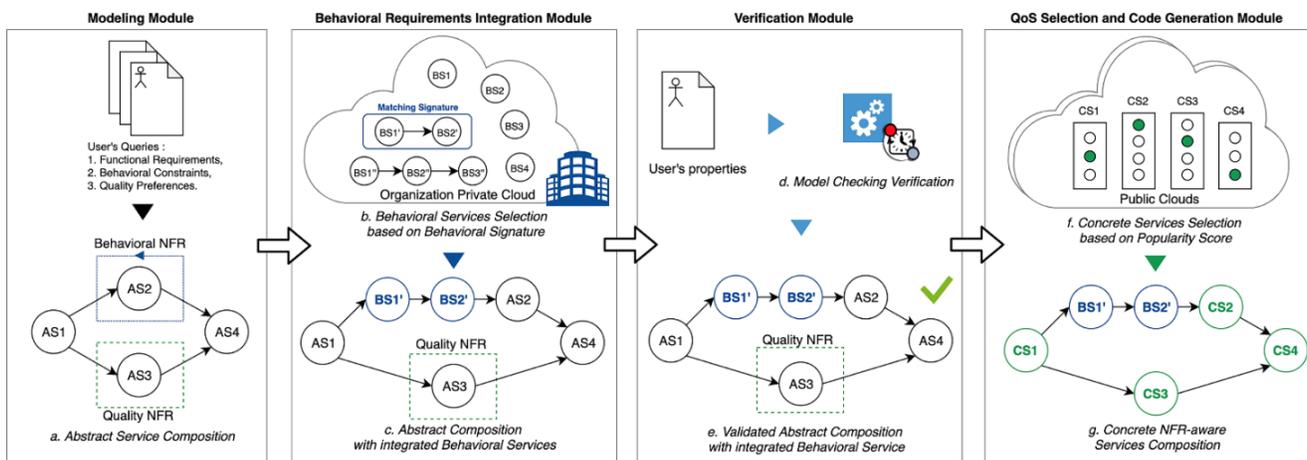


Fig. 2. The Service Composition Process Workflow.

The proposed modeling module is a web-based graphical interface allowing to draw an automata models using four aforementioned key components. It automatically generates a ready-to-use JSON representation of the composition. Additionally, the composition is saved in dedicated database to allow reuse and future improvement. The class diagram we proposed to build the modeling tool is illustrated in Fig. 3(a). The Fig. 3(b) shows an example of an AFA designed using the modeling tool module.

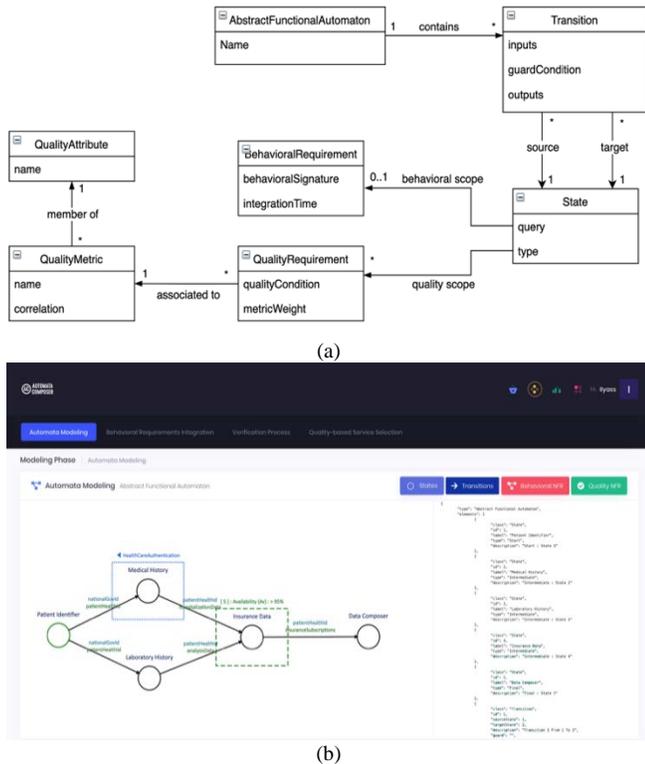


Fig. 3. (a). The Class Diagram Related to the Modeling Module. (b). An Example of Designing an AFA using the Modeling Tool.

### B. Behavioral Requirements Integration Phase

The aim of this phase consists on the integration of behavioral NFRs defined in the scopes at the modeling phase. The integration of behavioral NFRs is based on lookup operation into the behavioral NF-registry to find adequate concrete services able to fulfill the behavioral NFRs. A response is returned to the designer depending on the lookup results. If the process finds an atomic or composite service indexed by the required behavioral signature, it is automatically integrated to the AFA. Otherwise, the designer is redirected to the modeling tool in order to design an automata-based representation of the needed behavioral requirement. Then he/she develops and publishes the associated concrete services in the behavioral NF-registry. The behavioral requirements' records published are indexed using their behavioral signatures in order to facilitate their discovery and integration for further uses. The Algorithm 1 illustrates the process of integrating the behavioral NFRs into the Abstract Service Composition Automaton.

### Algorithm 1: Behavioral NFRs Integration

```

Input:
Set(State) states // A set of abstract states.
Registry nfrRegistry // A non-functional registry.

Output:
Map(State, BehavioralSignature) validStateMap
//A map of abstract states with valid signatures.
Map(State, BehavioralSignature) incompleteStateMap
//A map of incomplete states: unfound behavioral signatures.

for each state in states do
signature ← state.getBehavioralRequirement()
.getBehavioralSignature()
foundSignature ← nfrRegistry.lookup(signature)
if foundSignature is NOT NULL
validStateMap.addElement(state, foundSignature)
else
incompleteStateMap.addElement(state, signature)
end if
end for

return {incompleteStateMap, validStateMap}
    
```

### C. Verification Phase

This phase consists of verifying the composition between the AFA and all behavioral NF automata models obtained from the Behavioral Requirements Integration Module. The resulted Non-Functional Composition Automaton represents a workflow process gathering the user's functional and non-functional requirements combined. In order to validate its conformity, we use Uppsala-Aalborg verification tool (UPPAAL). UPPAAL is a toolbox for verification of real-time systems. In order to automate the model checking verification using UPPAAL, we implement an intermediate adapter allowing to translate automatically our automata models to understandable UPPAAL templates. The composition automaton is reproduced in UPPAAL's formalization using a composition of multiple templates. A template is an automata-based modeling describing a specific system and illustrating interactions between its states.

The automata adapter presented in our approach performs a translation between two different schemes: (1) the first is a JSON-based representation scheme of the proposed modeling, supporting integration of quantifiable and behavioral NFRs with the initial AFA, (2) the second scheme is adapted to UPPAAL's XML description. In verification phase, quantifiable quality attributes associated to the AFA are omitted, as they intervene mainly in the service selection phase and do not affect the composition workflow.

The UPPAAL model checking tool allows also to verify the conformance of native properties such as deadlock freeness, reachability, or custom logical properties defined by the designer. It supports various properties verification [32] such as:

- Reachability properties denoted as  $E \langle \diamond \rangle \varphi$ , which allows to check whether it exists a path starting from the initial state such that  $\varphi$  is eventually satisfied along that path.
- Safety properties, commonly known in the form “Something bad will possibly never happen”, are denoted either with the formulae  $A[] \varphi$  to describe that  $\varphi$  should be true in all reachable states, or using the formulae  $E[] \varphi$  to state that there should exist a maximal path such that  $\varphi$  is always true.
- Liveness properties, commonly known in the form “Something will eventually happen”, and denoted either using the formulae  $A \langle \diamond \rangle \varphi$  meaning that  $\varphi$  is eventually satisfied, or using the formulae  $\varphi \dashv \rightarrow \psi$  to state that whenever  $\varphi$  is satisfied, then eventually  $\psi$  will be satisfied.

The verification module consists on translating the automata scheme of the Service Composition Automaton into an automata scheme understandable by UPPAAL model checking tool. This verification can be a fully automated verification or a semi-automatic verification to validate the overall modeling. The fully automated verification consists on performing a direct verification of the translated UPPAAL automata model with the designer’s desired properties. Whereas the semi-automatic verification consists on adding some adjustments into the generated UPPAAL’s automata modeling then running the verification of designer’s properties. The main automaton and associated behavioral automata are translated into UPPAAL templates. In our approach, the formalization of SCA is comparable to UPPAAL’s formalization. The modeling of SCA using the modeling tool module omits defining synchronization in the transitions, as this information can be automatically concluded from the automata modeling. In other words, parallel and synchronous executions are defined directly from the modeling. A parallel execution is performed when a source state has more than one outgoing transitions with no guard condition. In UPPAAL, we are modeling the main automaton as a main template connected to all concurrent automata using synchronization channels.

The automata adapter is introduced to transform the JSON format corresponding to the modeled AFA with integrated behavioral services into an XML-based representation adapted to UPPAAL templating format. Table III shows the main transformation rules ensuring this transition. The coordinates  $x$  and  $y$  of all elements composing the modeled automaton are forwarded to fill the attributes of associated elements in UPPAAL’s XML file.

TABLE III. TRANSFORMATION RULES FROM JSON SCHEME TO UPPAAL XML SCHEME

Elements	JSON Modeling Tool Scheme	UPPAAL XML Description Sheme
Composition Automaton	{ "name": "Funct. Automaton", "elements": [ ... ] }	<template> <name>Funct. Automaton</name> ... </template>
States	{ "class": "State", "id": 1, "label": "Service 1", "type": "Intermediate" }	<location id="1" x="" y=""> <name>Service 1 </name> </location>
Start state	{ "class": "State", "id": 1, "type": "Start" }	<location id="1" x="" y=""> <name>Service 1</name> </location> <init ref="1"/>
Final state	{ "class": "State", "id": 8, "label": "Service 8", "type": "Final" }	<init ref="1"/> <location id="8" x="" y=""> <name>Service 8</name> </location> <transition> <source ref="8"/> <target ref="1"/> </transition>
Transitions	{ "class": "Transition", "id": 4, "sourceState": 1, "targetState": 3, "description": "Transition 4 From 1 To 3", "guard": "age < 18", "input": "age" }	<transition> <source ref="1"/> <target ref="3"/> <label kind="select"> age </label> <label kind="guard"> age &lt; 18 </label> </transition>

#### D. The QoS-oriented Service Selection Phase

The last phase consists on building a QoS-aware concrete service composition. It is called when all designer’s properties are verified. The associated module stores in a pool for each abstract service in the AFA all functionally-equivalent concrete services. Then, for each pool a QoS-based computation is performed to select the best matching service according to its popularity score. The quality requirements are initially defined in the quality scopes associated to the abstract services in the ASCA. The best matching service is the concrete service with the highest score. We describe in the algorithm below the Quality NFRs integration process.

---

Algorithm 2: Quality-oriented NFRs Integration

---

```
Input:
Set(State) states //A set of abstract states.

Output:
Map(State, Service) validServicesMap. /*A map of
abstract services with appropriate validated concrete
services.*/

for each state in states do
stateQualityNFRs ← state.getQualityRequirements()
for each qualityNFR in stateQualityNFRs do
// Fetching the state's quality NFRs
condition ← qualityNFR.getQualityCondition()
weight ← qualityNFR.getMetricWeight()
criteriaMap.addElement(condition, weight)
endfor

servicePool ← state
.selectServicesByQualityNFRs(criteriaMap)
/* Selecting the services fulfilling the state's main functional
requirements in addition to the Quality conditions */

for each candidateService in servicePool do
popularityScore =
computePopularityScore(candidateService, criteriaMap)
scoreMap.addElement(candidateService, popularityScore)
endfor

bestService = scoreMap.getBestMatchingService()
/* Selection of the best matching candidate service according
to its score */

validServicesMap.addElement(state, bestService)
endfor

return validServicesMap
```

---

## VI. ILLUSTRATIVE SCENARIO

To illustrate the proposed approach, a collaborative scenario related to the Healthcare domain is studied, due to the diverse NF needs in this field. The aim is to create a service composition allowing to get all patient's history: health records, medical diagnosis, taken medicines, etc., then to generate a folder grouping these data. This collaborative system engages multiple Healthcare centers. We focus mainly on Regional Health Centers (RHC) and University Health Centers (UHC) in Morocco, due to the advanced information system implemented allowing a web service-based interoperability.

To initiate the modeling phase, we elaborate the Abstract Functional Automaton (AFA). In our example, the main goal consists on generating a patient health folder grouping the patient's medical history including diagnosis, medical prescriptions and analysis results. Fig. 1 illustrates the proposed AFA for the demonstrative scenario. In this AFA the states constitute the desired abstract services, and the

transitions describe the intended interactions between states' corresponding concrete services.

The designed process described in this example requires as input the identification of the patient. The role of the first abstract service "Patient Identification" is to return the patient's Unique Healthcare Identifier (UHI) recognized by all Healthcare systems. The following step consists on providing, according to the patient's UHI, all patient data grouped from both RHCs and UHCs. To return all patient's health history we propose a parallel invocation of corresponding services for both types: "RHC Data Collector" and "UHC Data Collector" for regional and university healthcare centers respectively. Then, the abstract services defined as "Medicine Data Extractor" and "Diagnosis Data Extractor" aim to extract respectively the diagnosis information and the medicine information from the collected medical data history. The final step consists on searching for exhaustive information about returned medicines and diagnosis from third-party services using respectively "Medicine Data Provider" and "Diagnosis Data Provider". Finally, the abstract service "Patient Health Data Generator" will construct the patient folder with all collected information to allow returning a deep analysis based on the patient's medical history.

The proposed collaboration system involves manipulating sensitive and confidential information (medical history, diagnosis, prescription, medicine, etc.). Since this information is qualified to be very critical, we find necessary to protect the collaboration system by implementing some security policies. These security requirements are considered as Behavioral NFRs, as they define the behavioral aspect of the current process. Thus, the integration of these security-oriented behavioral NFRs should guarantee a result similar to the initial functional process but also acts on improving how this process should behave by adding security restrictions. In order to implement these behavioral NFRs to the current modeling, we integrate behavioral scopes to the Abstract Functional Automaton.

In our example, we integrate four security constraints to the functional process. They are all pre-execution behavioral requirements illustrated by the backward direction arrows on the behavioral scopes. It means that the security requirements should be implemented and executed before invoking the associated services. The behavioral signatures are defined using regular expressions labeling the behavioral scopes. The system will further lookup in the NF-Registry for associated atomic or composite services indexed by the provided behavioral signatures. In case the signature is not found in the NF-Registry, the designer proceeds to model the desired behavior as an automaton, to conceive and to publish the associated service in the NF-Registry indexed with its related behavioral signature. This process allows implementing and reusing specific services with customized behavioral needs.

The automata modeling proposed in our approach supports two possible execution paths. The success path corresponds to all possible executions leading to the valid final state. The second case concerns the executions that doesn't reach the final state, and instead, are reaching the trap state. A trap state, illustrated using the "π" symbol, is an error output. This error

output can be enhanced by adding an output message describing the violated constraint in order to keep the user informed about the failure cause. The automata modeling of desired NFRs is illustrated and described below:

- The first applied behavioral NFR using the behavioral signature “RHCAuthentication” associated to the AS “RHC Data Collector” aims to integrate an Authentication system to secure and limit access to the service for registered users only.
- The second behavioral NFR labeled using the behavioral signature “UHCAuthentication.UHCAccessControl” associated to the AS labeled “UHC Data Collector” aims to integrate a Role-based Access-Control (RBAC) to the service allowing to verify the authenticated users’ role before performing the related service.
- The third and fourth applied constraints labeled using the behavioral signatures “TokenAuthentication” are associated respectively to the abstract services labeled “Medicine Data Extractor” and “Diagnosis Data Extractor”. They aim to restrict access to the service by integrating a Token-based Authentication system.

Finally, we can generate the Service Composition Automaton (SCA) by composing all the behavioral automata with their appropriate abstract services. This automaton allows to illustrate in an exhaustive way the interactions of all components. Once the SCA is generated, the following step consists on performing the model checking verification using UPPAAL.

Transitions in UPPAAL are defined as follow: The selection information, the guard conditions labelled in green color, the synchronization labelled in light blue color, and the update information labeled in dark blue color.

Fig. 4 shows the modeling of the SCA automaton using UPPAAL. The automaton illustrated in Fig. 4(b) shows the main process, gathering atomic and composite components together, using sequential and synchronous communication channels. The parallel executions are launched using broadcast channels, allowing to push a synchronization from the composition process using the exclamation mark “!” near the synch expression, and receive it on the other components using question mark “?”. The first example of synchronous execution is the invocation of DataCollector services. We use “DataCollectorSynch!” in the composition process (Fig. 4(b)), which is a broadcast channel allowing to start a parallel execution of both UHCDataCollector and RHCDDataCollector using “DataCollectorSynch?” in both concurrent target processes (Fig. 4(c)). In the same way the synchronous execution of “Diagnosis Data Extractor” and “Medicine Data Extractor” illustrated in the Fig. 4(d) are launched using the broadcast channel “DataExtractorSynch!” from the main process, and towards “DataExtractorSynch?” in both concurrent processes. Finally, the “Diagnosis Data Provider” and “Medicine Data Provider” are launched using “DataProviderSynch!” broadcast channel from the main

process towards “DataProviderSynch?” in both concurrent processes. UPPAAL’s model checking allows us to validate the correctness of designed models by verifying safety and liveness properties, in addition to user’s custom logical properties related to the deployed service-oriented process. As shown in Fig. 4(e) illustrating the verified properties, the first checked property verifies whether the generated system is deadlock-free as follow “A[] not deadlock”. A deadlock is an unmarked state where no events are possible. The automaton jams in a state that we have not specified as a possible final state. In our approach, we use trap states to define undesired events, happening when some predefined conditions are not met. We keep track of successful and error executions using incremental variables. It also allows to control the concurrent components executed. Table IV shows the verified properties with corresponding descriptions.

According to provided modeling we notice that all desired properties are satisfied, which means that the associated automata modeling is valid considering final state reachability, deadlock-freeness and user’s custom logical preferences. The next step consists on selecting the best matching service to meet the abstract services having quality scopes. In Fig. 1 we notice that the “Medicine Data Provider” and “Diagnosis Data Provider” abstract services have quality scopes with different criteria: Response-Time and Availability for the Medicine Data Provider service and Usability for the Diagnosis Data Provider. The popularity score computation will be performed on the pool of concrete services associated to the AS “Medicine Data Provider”, as they require more than one quality criterion to be fulfilled by the scoped subset. While the AS “Diagnosis Data Provider” needs only one criterion to be met, and then, no weight is required to compute the popularity score.

In Table V, we provide the computed popularity score for concurrent concrete services fulfilling the Medicine Data Provider and Diagnosis Data Provider abstract services. The service Medicine Data Provider requires two quality conditions: Response-Time < 250ms with a weight of 5, and Availability > 90% with a weight of 3. We proceed to the metric normalization in order to compute uniformly the popularity score. For rate-based metrics i.e. metrics calculated in a percentage basis, the score constitutes the value of the measured quality metric when the measurement correlation is positive. Otherwise, when the correlation is negative, the score is the subtraction of the measured value from a basis of 100. In other hand, for non-rate-based quality metrics, we use the proportional computation of the service metric value according to the maximal value for the target metric. The maximal value for a non-rate-based quality metric is concluded by using the desired value as a median. For instance, for the desired value of Response-Time less than 250ms we use this value as a median to conclude that the maximal value for the Response-Time is 500ms. The second method consists on providing the maximal values for each quality metric by the expert rather than concluding it using the reversed median calculation. A deeper explanation of the proposed popularity score computation methods is provided in a previous work [5].

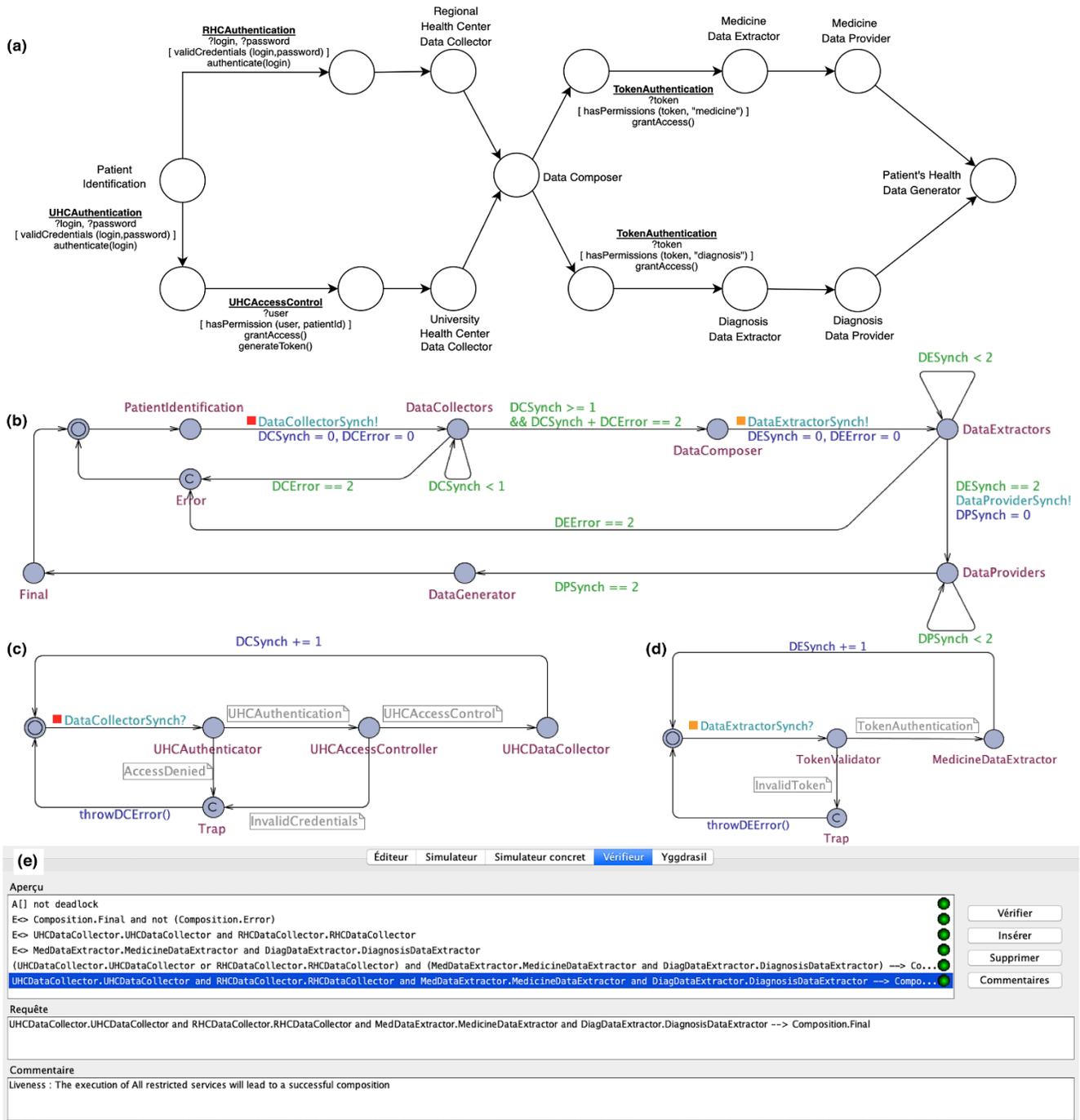


Fig. 4. The Service Composition Automaton and its Appropriate UPPAAL Modelling and Verification.

TABLE IV. UPPAAL'S VERIFIED PROPERTIES WITH CORRESPONDING DESCRIPTIONS

Verified properties	Descriptions
E<> Composition.Final AND NOT (Composition.Error)	There exists eventually a path leading to the final state without reaching any error state.
E<> UHCDDataCollector.UHCDDataCollector AND RHCDDataCollector.RHCDDataCollector	There is eventually a parallel execution of the Data Collectors in both UHC and RHC. It assumes that the associated security services are preliminarily performed, i.e. UHCAuthenticator and UHCAccessController before UHCDDataCollector, and RHCAuthenticator before RHCDDataCollector.
E<> MedDataExtractor.MedicineDataExtractor AND DiagDataExtractor.DiagnosisDataExtractor	There is eventually a parallel execution of Medicine Data Extractors and Diagnosis Data Extractor.
(UHCDDataCollector.UHCDDataCollector OR RHCDDataCollector.RHCDDataCollector) AND (MedDataExtractor.MedicineDataExtractor AND DiagDataExtractor.DiagnosisDataExtractor) → Composition.Final	A successful composition is conditioned by an execution of at least one Data Collector of either UHC or RHC (OR), additionally to an execution of both Medicine Data Extractor and Diagnosis Data Extractor (AND)
UHCDDataCollector.UHCDDataCollector AND RHCDDataCollector.RHCDDataCollector AND MedDataExtractor.MedicineDataExtractor AND DiagDataExtractor.DiagnosisDataExtractor → Composition.Final	An execution of all restricted services which are UHCs' and RHCs' Data Collectors in addition to Diagnosis and Medicine Data Extractors will lead to a successful execution of the composition

TABLE V. CONCRETE SERVICE COMPARISON BASED ON POPULARITY SCORE

Abstract Service	Associated Concrete Services	Popularity Score
Medicine Data Provider	<b>WS<sub>11</sub> (Response-Time: 150ms, Availability: 94%)</b>	<b>90.28</b>
	WS <sub>12</sub> (Response-Time: 200ms, Availability: 98%)	84.85
Diagnosis Data Provider	WS <sub>21</sub> (Usability:8.2)	82
	WS <sub>23</sub> (Usability:6.9)	69
	<b>WS<sub>24</sub> (Usability:8.8)</b>	<b>88</b>

The final step consists on generating a ready-to-execute BPEL code using the engine provided by the previously developed framework, i.e., Discovery and Visual Interactive Web Service Engine (DIVISE) [30]. The produced code of the composite service assembles all selected concrete services with their appropriate interactions according the validated process. In this contribution we aim to enhance the engine by providing design and verification-oriented modules allowing an exhaustive modeling taking into account functional requirements in addition to both behavioral and measurable non-functional requirements.

## VII. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Our current contribution consists on defining a more fine-grained composition process workflow and its implementation and handling the main phases from the design time to code generation. This workflow integrates both behavioral and measurable quality-oriented NFRs into service composition process. An Automata-based modeling of the functional requirements (FRs) and non-functional requirements (NFRs) is suggested with an explicit distinction between measurable quality-oriented NFRs and the newly introduced behavioral NFRs. These NFRs are integrated into the abstract functional automaton using scopes. The needed behavioral NFRs are modeled separately then merged to the functional abstract automaton in order to perform a model checking verification using UPPAAL. In addition, the desired measurable quality-oriented NFRs have no impact on the behavioral workflow of

the composition automaton, and are explored in the selection phase using Popularity score enabling to return the best matching concrete services for each associated abstract service. A use case process using Patient Health Records in Regional and University Health Centers in Morocco is used to experiment our approach.

Although this approach handles the overall process of service composition from design to execution phases, it can be considered as limited to the current state of evaluated QoS properties of services, as we did not integrate the tracking module in the current contribution. Thus, the service selection based on Popularity Score is using provided values for each quality metric. These values are provided mainly by the provider. However, for an accurate classification, we are orienting our research to perform a new computation based on service tracking of service quality over time using Machine Learning techniques and technologies. It will allow us to have a clear idea regarding variation of service quality in a wide timeline, and compute the Popularity Score either using average function for the whole time or partially for a recent limited period of time.

## REFERENCES

- [1] L. Chung, B. A. Nixon, E. Yu, J. Mylopoulos, "Non-Functional Requirements in Software Engineering", 2000, DOI: 10.1007/978-1-4615-5269-7.
- [2] J. Eckhardt, A. Vogelsang, D. Méndez Fernandez, "Are Non-functional Requirements really Non-functional? An Investigation of Non-functional Requirements in Practice", in 38th IEEE International Conference on Software Engineering (ICSE '16), pp. 832-842, 2016. DOI: <https://doi.org/10.1145/2884781.2884788>.
- [3] M. H. Beek, A. Bucchiarome, S. Gnesi, "Formal Methods for Service Composition", in Annals of Mathematics, Computing & Teleinformatics, vol. 1, pp 1-10, 2007.
- [4] I. El Kassmi, Z. Jarir, "Security Requirements in Web Service Composition: Formalization, Integration, and Verification", in 25th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Paris, France, 2016. DOI: 10.1109/WETICE.2016.47.
- [5] I. El Kassmi, Z. Jarir, "Toward a Smart Cloud Service Composition: Popularity-Driven Approach", in The 14th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), pp. 522-528, 2018. DOI: 10.1109/SITIS.2018.00085.

- [6] Y. Chen, J. Huang, C. Lin, X. Shen, "Multi-Objective Service Composition with QoS Dependencies", in *IEEE Transactions on Cloud Computing*, vol. 7, pp. 537-552, 2019. DOI: 10.1109/TCC.2016.2607750.
- [7] S. Deng, H. Wu, H. Hu, J. Leon Zhao, "Service Selection for Composition with QoS Correlations", in *IEEE Transactions on Services Computing*, vol. 9, pp. 291-303, 2016. DOI: 10.1109/TSC.2014.2361138.
- [8] S. K. Gavvala, C. Jatoth, G. R. Gangadharan, and R. Buyya, "QoS-aware cloud service composition using eagle strategy," in *Future Generation Computer Systems*, vol. 90, pp. 273-290, Jan. 2019.
- [9] Y. Liang, H. Hu, W. Song, J. Ge, "QoS-aware Automatic Web Service Composition Considering QoS Correlations", in *Proc. of the 7th Asia-Pacific Symposium on Internetware*, pp. 39-42, 2015. DOI: <https://doi.org/10.1145/2875913.2875940>.
- [10] Y. Feng, L. Ngan, R. Kanagasabai, "Dynamic Service Composition with Service-Dependent QoS Attributes", in *IEEE 20th International Conference on Web Services*, pp. 10-17, 2013. DOI: 10.1109/ICWS.2013.12.
- [11] C. Jatoth, G.R. Gangadharan, U. Fiore, R. Buyya, "QoS-aware Big service composition using MapReduce based evolutionary algorithm with guided mutation", in *Future Generation Computer Systems*, vol. 86, pp. 1008-1018, 2018. DOI:<http://dx.doi.org/10.1016/j.future.2017.07.042>.
- [12] H. Jin, X. Yao, Y. Chen, "Correlation-aware QoS modeling and manufacturing cloud service composition", in *Journal of Intelligent Manufacturing*, vol. 28, pp. 1947-1960, 2017. DOI:<https://doi.org/10.1007/s10845-015-1080-2>.
- [13] H. Liang, Y. Du, "Dynamic service selection with QoS constraints and inter-service correlations using cooperative coevolution", in *Future Generation Computer Systems*, vol. 76, pp. 119-135, 2017. DOI:<https://doi.org/10.1016/j.future.2017.05.019>.
- [14] H. Wang, D. Yang, Q. Yu, Y. Tao, "Integrating Modified Cuckoo Algorithm and Creditability Evaluation for QoS-Aware Service Composition", in *Knowledge-Based Systems*, vol. 140, pp. 64-81, 2017. DOI: 10.1016/j.knosys.2017.10.027.
- [15] J. Lu, Z. Huang, C. Ke, "Verification of Behavioral-aware Privacy Requirements in Web Service Composition", in *Journal of Software*, vol. 9, pp. 944-951, 2014. DOI:10.4304/jsw.9.4.944-951.
- [16] W. Dou, X. Zhang, J. Liu, J. Chen, "HireSome-II: Towards Privacy-Aware Cross-Cloud Service Composition for Big Data Applications", in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 455-466, 2015. DOI: 10.1109/TPDS.2013.246.
- [17] Xx5 A. Souri, A.M. Rahmani, N.J. Navimipour, "A hybrid formal verification approach for QoS-aware multi-cloud service composition". *Cluster Computing* vol. 23, pp. 2453-2470, 2020. DOI: <https://doi.org/10.1007/s10586-019-03018-9>.
- [18] A.D. Brucker, B. Zhou, F. Malmignati, Q. Shi, M. Merabti, "Modelling, validating, and ranking of secure service compositions", in *Journal of Software: Practice and Experience*, vol. 47, pp. 1923-1943, 2017. DOI: <https://doi.org/10.1002/spe.2513>.
- [19] G.N. Rai, G.R. Gangadharan, "Model Checking Based Web Service Verification: A Systematic Literature Review", in *IEEE Transactions on Services Computing*. DOI: 10.1109/TSC.2018.2845401.
- [20] M. H. Beek, A. Bucchiarome, S. Gnesi, "A Survey on Service Composition Approaches: From Industrial Standards to Formal Methods", in *Technical Report*, 2006.
- [21] A. Charfi, M. Mezini, "Aspect-Oriented Web Service Composition with AO4BPEL", in *Web Services, ECOWS 2004*, vol. 3250, pp. 168-182. DOI: [https://doi.org/10.1007/978-3-540-30209-4\\_13](https://doi.org/10.1007/978-3-540-30209-4_13).
- [22] Z. Shen, J. Su, "Web service discovery based on behavior signatures", in *2005 IEEE International Conference on Services Computing*, vol. 1, pp. 279-286, 2005. DOI: 10.1109/SCC.2005.107.
- [23] L. Chung, J.C.S. do Prado Leite, "On Non-Functional Requirements in Software Engineering" in *Conceptual Modeling: Foundations and Applications*, pp. 363-379, 2009.
- [24] ISO/IEC9126-1:2001, "Software Engineering – Product Quality-Part1: Quality Model", 2001.
- [25] ISO/IEC25010:2011, "System and Software – System and Software Quality Requirements and Evaluation Engineering: System and Software Quality Model", 2011.
- [26] M. Galster, E. Bucherer, "A Taxonomy for Identifying and Specifying Non-functional Requirements in Service-oriented Development", in *IEEE Congress on services*, pp. 345-352, 2008. DOI: 10.1109/SERVICES-1.2008.51.
- [27] D. Mairiza, D. Zowghi, N. Nurmiliani, "An investigation into the notion of non-functional requirements", in *ACM Symposium on Applied Computing*, pp. 311-318, 2010. DOI:<https://doi.org/10.1145/1774088.1774153>.
- [28] M.M. Hasan, P. Loucopoulos, M. Nikolaidou, "Classification and Qualitative Analysis of Non-Functional Requirements Approaches", in *Enterprise, Business-Process and Information Systems Modeling*, vol. 175, pp. 348-362, 2014.
- [29] S. Elfirdoussi, Z. Jarir, M. Quafafou, "Ranking Web Services using Web Service Popularity Score" in *International Journal of Information Technology and Web Engineering*, vol. 9, pp. 78-89, 2014. DOI: 10.4018/ijitwe.2014040105.
- [30] S. Elfirdoussi, Z. Jarir, M. Quafafou, "Discovery and Visual Interactive WS Engine based on popularity: Architecture and Implementation", in *International Journal of Software Engineering and Its Applications*, vol. 8, pp. 213-228, 2014. DOI: 10.14257/ijseia.2014.8.2.21.
- [31] D.G. Firesmith. "Engineering Security Requirements" in *Journal of Object Technology*, vol. 2, 2003. DOI: 10.5381/jot.2003.2.1.c6.
- [32] G. Behrmann, A. David, K.G. Larsen, "A Tutorial on UPPAAL", in *Formal Methods for the Design of Real-Time Systems*, pp. 200-236, 2004. DOI: 10.1007/978-3-540-30080-9\_7.

# Concatenative Speech Recognition using Morphemes

Afshan Jafri

College of Computer and Information Sciences  
King Saud University  
Riyadh, SA

**Abstract**—This paper adopts a novel sub-lexical approach to construct viable continuous speech recognition systems with scalable vocabulary that use the components of words to form the elements of pronunciation dictionaries and recognition lattices. The proposed Concatenative ASR family utilizes combination rules between morphemes (prefixes, stems, and suffixes), along with their theoretical grammatical categories. The constrained structure reduces invalid words by using grammar rules governing agglutination of affixes with stems, while having a large vocabulary space and hence fewer out-of-vocabulary words. In pursuing this approach, the project develops automatic speech recognition (ASR) parameterized models, designs parameter values, constructs and implements ASR systems, and analyzes the characteristics of these systems. The project designs parameter values in the context of Arabic to yield a subset hierarchy of vocabularies of the ASR systems facilitating meaningful analysis. It investigates the characteristics of the ASR systems with respect to vocabulary, recognition lattice, dictionary, and word error rate (WER). In the experiments, the standard Word ASR model has the best characteristics for vocabulary of up to five thousand words and the Concatenative ASR family is most appropriate for vocabulary of up to half a million words. The paper shows that the approach used encompasses fundamentally different processes of word formation and thus is applicable to languages that exhibit concatenative word-formation processes.

**Keywords**—Morphemes; sub-lexemes; speech recognition; Arabic; concatenative morphology

## I. INTRODUCTION

The standard automatic speech recognition (ASR) system uses Hidden Markov Models (HMMs) trained on phonetic units, along with a word pronunciation dictionary and a single level recognition lattice composed of words [1]. Application of the standard Word ASR model to vocabulary beyond a hundred thousand words poses complexities, including the construction of the pronunciation dictionary, estimation of the language model, efficient computation of the recognized utterance, and poor recognition performance due to out-of-vocabulary words (OOVs) [2]. For these reasons, the standard Word ASR model is not well suited to languages that are particularly rich in inflectional morphology and that consequently have large vocabularies.

Concatenative word formation of inflectional morphology, by far the most prevalent type in the world's languages, involves the linear affixation of discrete morphemes, including prefixes, stems, and suffixes.

The concatenative morphology in Arabic is illustrated through two examples provided below. Henceforth the

approach drops short vowels as they are not represented in modern Arabic orthography. Table I lists the Arabic characters and their roman transliterations.

The word "فكتابت", transliterated as "fkqbt" means 'so she corresponded', and demonstrates that a sentence is represented by a single highly inflected word. This word is composed of the stem "kqtb", the prefix 'f', and the suffix 't':

prefix+ stem+suffix (1)

f + kqtb + t → fkqbt 'so she corresponded'

Another example is the noun "مدرسة", which is transliterated as "mdrsO" and means "school". This word is composed of the stem "mdrs", and the suffix "O". Its derivation is shown below, where  $\phi$  is null:

prefix + stem + suffix (2)

$\phi$  + mdrs + O → mdrsO 'school'

By integrating speech recognition constructs with the morphological structure of a given language, the paper aims to develop models that have scalable vocabulary, valid words, moderate computational requirements, and good recognition performance. The objective is to explore the feasibility of sub-lexical models in speech recognition, rather than to optimize the performance of the proposed model families. Consequently, the paper does not deviate into stochastic models, focusing instead on deterministic models.

Vocabulary scalability is attained by constructing a variety of multilevel recognition lattices that utilize the components (sub-lexemes) of words, along with the component categories at different levels of abstraction. The vocabulary is the space of words spanned by the lattice, and the nodes correspond to word components and their categories.

The vocabulary is constrained to valid words in two ways. First, models are defined that constrain the vocabulary of the ASR system and implicitly the word lengths without actually listing words. Second, combination rules are imposed on word components or their categories to eliminate invalid words.

The computational requirements of the ASR system depend on the number of nodes and edges, as well as the structure of the recognition lattice; the size of the pronunciation dictionary; and the search method. Consequently, models with fewer nodes, edges, and items in the dictionary are desirable. Use of word components rather than words to represent nodes and dictionary items reduces the size of both the lattice and dictionary components of the models, thus reducing the computational requirements of the system.

TABLE I. ARABIC CHARACTERS

Ar	Rm	Ar	Rm	Ar	Rm	Ar	Rm
أ	A	آ	F	ذ	c	غ	x
ب	U	ب	b	ر	r	ف	f
ت	I	ة	O	ز	z	ق	K
ع	Q	ت	t	س	s	ك	k
أ	E	ث	B	ش	Z	م	m
ؤ	M	ج	j	ص	S	ن	n
ل	L	ح	H	ض	D	ه	h
ئ	N	خ	X	ط	T	و	w
ا	aa	ل	l	ظ	C	ي	y
ى	P	د	d	ع	R	ـ	G

No standard transliterations between Arabic (Ar) and Roman (Rm)

Recognition performance as measured by word error rate (WER) is determined by the HMMs and vocabulary of the test set, as well as by recognition lattice vocabulary, lattice structure, and search method. This multitude of factors makes prediction of recognition performance difficult, and hence required careful design of the experiments to produce empirical results that would enable us to measure and compare the recognition performance of different versions of the ASR systems, and to compare these results to those of standard Word ASR system counterparts.

The project's methodology for attaining the above is to: (1) construct parameterized models to build sub-lexical ASR models of increasing complexity and abstraction to attain larger vocabularies; (2) design parameter values in a way that parsimoniously yields a subset hierarchy of a wide spectrum of vocabularies; (3) construct implementable ASR systems using the derived parameter values (4) set up experiments through selection of speech training and test sets, and conduct ASR system training and recognition; (5) investigate the characteristics of the ASR systems with respect to vocabulary, recognition lattice, and word error rate (WER), and observe their robustness with respect to out-of-vocabulary words (OOVs).

The primary objective of this paper is to develop ASR models that are scalable and produce only valid words. Arabic has been chosen as the context for developing this new ASR paradigm. More specifically, Modern Standard Arabic (MSA) is utilized because it is widely used and has well established and standardized grammar and phonetics.

The paper is organized as follows: Section II contains literature review; Section III introduces the parameterized ASR models; Section IV constructs ASR systems for concatenative model; Section V explains how the system is constructed; Section VI discusses the experimental setup; Section VII evaluates the system; Section VIII discusses the results; and Section IX has the conclusion.

## II. LITERATURE REVIEW

To overcome the limitations of the Word ASR model, a number of approaches have been suggested that have in

common their use of morphemes (prefixes, stems, and suffixes) rather than words as the basic unit of analysis. Indeed, several studies have investigated the use of sub-lexical language constructs in speech recognition [3,4] and models incorporating this idea have been used in many languages, including German and Finnish [5,6], Korean [7,8,9], Dutch [10], Arabic [11,12, 13,14,15,16], Turkish [5,17], Slovenian [18] and English [5]. Other works utilizing such an approach for multiple languages have been published [19,20].

Existing approaches use empirical morphemes and direct relationships between prefixes, stems, and suffixes. They suffer from generation of invalid words because the recognition lattice does not adequately constrain formation of words from morphemes. The invalid words lead to lower recognition performance. The problem is alleviated to some extent by replacing the morphemes of most frequently occurring words by surface forms (complete words) themselves.

Recent work has been conducted for MSA automatic speech recognition utilizing weighted finite state transducer structure in the Kaldi ASR system [21]. Finite state transducer has also been utilized for MSA morphological analysis and diacritization [22].

## III. PARAMETERIZED ASR MODELS

The concatenative grammar-based parameterized models' objective is to have increasing levels of complexity and abstraction to attain larger vocabularies. This is achieved by the models by utilizing categories of word components rather than word components alone. The categories reflect two basic sub-lexical classes (stems and affixes) and the objects they can combine with.

The four models are termed: Direct Morpheme, Affix Category, Stem Category, and Full Category in addition to the baseline model called Independent Morpheme (described in the Appendix), which corresponds to currently proposed models in the literature.

With the exception of Independent Morpheme, all of the system's ASR models have a vocabulary of only valid words because they use three-dimensional combination matrices that constrain the relations between morphemes or their categories. The baseline Independent Morpheme model does admit invalid words in the vocabulary because it lacks these constraints.

Each of these grammar-based ASR models has a distinct set of parameters, with the common parameters being Prefix, Stem, and Suffix –more specifically, the indexed listings of prefixes, stems, and suffixes. For the same set of parameter values of Prefix, Stem, and Suffix, the various ASR models have the same terminal nodes comprising prefixes, stems, and suffixes, and the same dictionary, whose items are the union of prefixes, stems and suffixes.

However, the models have distinct recognition grammars. The reason for the distinct recognition grammars is that the models use component categories and different two-dimensional binary association matrices defining associations between components and their categories, as well as three-dimensional binary combinations defining licit combinations between morphemes or between their categories. The

morphemes, categories, associations, and combinations are based on theoretical morphological grammar.

#### A. Direct Morpheme ASR Model

The Direct Morpheme ASR parameterized model involves the most constrained structure, incorporating direct combination constraints among prefixes, stems, and suffixes. The parameters are Prefix, Stem, and Suffix, and the binary three-dimensional combination matrix PrefixXStemXSuffix. The recognition grammar is given below:

```
# {Word '&' }+ #  
Word → WordStem1 | WordStem2 | ...;  
WordStem1 → stemPrefix11 stem1 stemSuffix11 |  
stemPrefix12 stem1 stemSuffix12 | ...;  
WordStem2 → stemPrefix21 stem2 stemSuffix21 |  
stemPrefix22 stem2 stemSuffix22 | ...;
```

The second line expands a word into stem-grouped words, which share a common stem. The words are not explicitly listed. Each stem-grouped word is a choice of prefix-stem-suffix combinations for the particular stem, as allowed by the combination matrix PrefixXStemXSuffix. An implementable example is shown below:

```
(# {Word '&' }+ #)  
Word → WordStem_ktb | WordStem_drs | ... ;  
WordStem_ktb → ' ' 'ktb' ' ' | 'f' 'ktb' 't' | ... ;  
WordStem_drs → 'w' 'drs' 'h' | 'l' 'drs' 'hmq' | ... ;
```

#### B. Affix Category ASR Model

The Affix Category ASR parameterized model is both an abstraction of the Direct Morpheme model and potentially more efficient than that model because it classifies affixes (prefixes and suffixes) according to their grammatical categories. The parameters of this model are: Prefix, Stem, Suffix; PrefixCateg, SuffixCateg; the binary association matrices Prefix\_PrefixCateg and Suffix\_SuffixCateg; and the binary combination matrix PrefixCategXStemXSuffixCateg. The recognition grammar for the Affix Category parameterized model is:

```
# {Word '&' }+ #  
Word → WordStem1 | WordStem2 | ...;  
WordStem1 → PrefixCateg11 stem1 SuffixCateg11 | ...  
PrefixCateg12 stem1 SuffixCateg12 | ...;  
WordStem2 → PrefixCateg21 stem2 SuffixCateg21 |  
PrefixCateg22 stem2 SuffixCateg22 | ...;  
PrefixCateg11 → prefix11 | prefix12 | ...;  
PrefixCateg21 → prefix21 | prefix22 | ...;  
SuffixCateg11 → suffix11 | suffix12 | ...;  
SuffixCateg21 → suffix21 | suffix22 | ...;
```

The second line expands a word into alternatives among words grouped according to stems. Each stem grouped word is a choice between PrefixCateg-stem-SuffixCateg combinations for the stem, as allowed by PrefixCategXStemXSuffixCateg. Each PrefixCateg and SuffixCateg is expanded into prefixes and suffixes according to the association matrices.

#### C. Stem Category ASR Model

The Stem Category ASR parameterized model is also an abstraction of the Direct Morpheme model by its classification of stems into their grammatical categories. In classifying stems rather than affixes, this model is more effective than the Affix Category model because the number of stems is much larger than the number of affixes. The parameters are Prefix, Stem, Suffix; StemCateg representing the indexed listing of stem categories; binary association matrix Stem\_StemCateg; binary combination matrix PrefixXStemCategXSuffix. The recognition grammar for the Stem Category model is:

```
# {Word '&' }+ #  
Word → WordStem1 | WordStem2 | ...;  
WordStem1 → prefix11 StemCateg1 suffix11 |  
prefix12 StemCateg1 suffix12 | ...;  
WordStem2 → prefix21 StemCateg2 suffix21 |  
prefix22 StemCateg2 suffix22 | ...;  
StemCateg1 → stem11 | stem12 | ...;  
StemCateg2 → stem21 | stem22 | ...;
```

The group for each WordStem is a choice of prefix-StemCateg-suffix combinations for the specific item in StemCateg, as allowed by PrefixXStemCategXSuffix. A specific member in StemCateg is expanded into stems according to the association matrix.

#### D. Full Category ASR Model

The Full Category ASR parameterized model abstracts all morphemes--prefixes, stems and suffixes--into their grammatical categories, thereby producing the most abstract Concatenative ASR model. The parameters are Prefix, Stem, Suffix; PrefixCateg, StemCateg, SuffixCateg; binary association matrices Prefix\_PrefixCateg, Stem\_StemCateg, Suffix\_SuffixCateg; and binary combination matrix PrefixCategXStemCategXSuffixCateg. The recognition grammar is given below:

```
# {Word '&' }+ #  
Word → WordStemCateg1 | WordStemCateg2 | ...;  
WordStemCateg1 →  
PrefixCateg11 StemCateg1 SuffixCateg11 |  
PrefixCateg12 StemCateg1 SuffixCateg12 | ...;  
WordStemCateg2 →  
PrefixCateg21 StemCateg2 SuffixCateg21 |  
PrefixCateg22 StemCateg2 SuffixCateg22 | ...;
```

PrefixCateg<sub>11</sub> → prefix<sub>111</sub> | prefix<sub>112</sub> | ...;  
 PrefixCateg<sub>12</sub> → prefix<sub>121</sub> | prefix<sub>122</sub> | ...;  
 StemCateg<sub>1</sub> → stem<sub>11</sub> | stem<sub>12</sub> | ...;  
 StemCateg<sub>2</sub> → stem<sub>21</sub> | stem<sub>22</sub> | ...;  
 SuffixCateg<sub>11</sub> → suffix<sub>111</sub> | suffix<sub>112</sub> | ...;  
 SuffixCateg<sub>12</sub> → suffix<sub>121</sub> | suffix<sub>122</sub> | ...;

Each collection of words centered on a specific StemCateg is a choice between PrefixCateg-StemCateg-SuffixCateg combinations for the given StemCateg as allowed by PrefixCategXStemCategXSuffixCateg.

The categories PrefixCateg, StemCateg, and SuffixCateg are expanded into prefixes, stems, and suffixes according to the association matrices Prefix\_PrefixCateg, Stem\_StemCateg, Suffix\_SuffixCateg respectively. An illustrative example is as follows, with FW1Wa denoting a stem category, Pref1Wa a prefix category, and Suff10 a suffix category.

Word\_FW1Wa →  
 Prefix\_Pref1Wa Stem\_FW1Wa Suffix\_Suff10 |  
 Prefix\_Pref10 Stem\_FW1Wa Suffix\_Suff10 ;  
 Stem\_FW1Wa → 'EbnqQ' | 'Ef' | 'Em' | 'En' | 'Ew' |  
 'Ey' | 'Eyn' | 'Lz' | 'Lbnqn' | 'Lcq' | 'Ls' | ...;  
 Prefix\_Pref1Wa → 'f' | 'w';  
 Suffix\_Suff10 → ' ' ;

This section presented four Concatenative grammar-based ASR parameterized models to develop a hierarchy of vocabularies from the same set of parameter values and to provide models suitable for a variety of circumstances.

The Direct Morpheme model is suitable for cases where |Prefix|/|PrefixCateg| ~ 1, |Suffix|/|SuffixCateg| ~ 1, and |Stem|/|StemCateg| ~ 1; the Affix Category model is appropriate for situations where |Prefix|/|PrefixCateg| >> 1, |Suffix|/|SuffixCateg| >> 1, and |Stem|/|StemCateg| ~ 1; the Stem Category model is suitable for cases where |Prefix|/|PrefixCateg| ~ 1, |Suffix|/|SuffixCateg| ~ 1, and |Stem|/|StemCateg| >> 1; and the Full Category model is appropriate for situations where |Prefix|/|PrefixCateg| >> 1, |Suffix|/|SuffixCateg| >> 1, |Stem|/|StemCateg| >> 1.

#### IV. PARAMETER DESIGN

This section illustrates how the parameter values and combination matrices are derived and ASR systems constructed for concatenative models. Parameter values are designed to parsimoniously cover a wide spectrum of vocabulary for construction of the implementable ASR systems from the models developed in Section III.

The system vocabulary is derived indirectly by the specification of morphemes, and their combinations and association matrices. This is in contrast to Word ASR, in which systems may be constructed for arbitrary vocabulary sizes.

The careful parameter design yields a subset hierarchy of vocabularies for the ASR systems, thereby facilitating comparative analysis of the various models. Both a language dataset and a speech corpus are used to derive the parameter values for the ASR systems, as the approach combines the speech and language aspects into the development of an ASR system.

The Buckwalter language dataset was chosen because it is the most complete morphological dataset and the Saavb corpus as both a speech and text corpus because it has accurate transcriptions in Modern Standard Arabic validated by IBM [23]. The recognition grammar is generated from the text corpora, while the training and test sets are generated from the speech corpus with the difference between the recognition lattice span and the recognition set determining the out-of-vocabulary (OOV) words.

The Buckwalter dataset contains three lexicon files and three compatibility tables with a vocabulary of more than five million consisting of only valid words. The three lexicon files tabulate the prefixes, stems, and suffixes with their grammatical categories. Categories of stems and affixes reflect both language classification and the objects that they can combine with. The three compatibility files have two-column tables that provide the relations between the following: prefix categories & suffix categories, prefix categories & stem categories, and suffix categories & stem categories.

The parameter values for the ASR models are computed in three stages, which are briefly described below, with details omitted due to space considerations. In Stage I, we compute the various listings, association and combination matrices from the Buckwalter lexicon files, and compatibility tables. To accomplish this, we first compute the indexed listings of unique prefixes, stems, and suffixes from the tokens in the three lexicons, and compute the categories of the prefixes, stems, and suffixes from both the lexicon files and the compatibility tables. Table II lists the sizes of the Buckwalter parameter values, such as BuckwalterStem, BuckwalterStemCateg. Then, the computed indexed listings are used, along with the lexicon files and compatibility tables to produce the two-dimensional binary association matrices (such as Suffix\_SuffixCateg) and two-dimensional binary compatibility matrices (such as PrefixXSuffix). These two-dimensional compatibility matrices are used to derive the three-dimensional binary combination matrices (such as PrefixXStemXSuffix).

TABLE II. BUCKWALTER MORPHEME PARAMETER SIZES\*

Parameter	Size
BuckwalterPrefix	131
BuckwalterSuffix	209
BuckwalterStem	43870
BuckwalterPrefixCateg	88
BuckwalterSuffixCateg	173
BuckwalterStemCateg	218
* From original Buckwalter dataset	

In Stage II, the system morphologizes the Saavb corpus words according to the generated Buckwalter listings and matrices to produce the SaavbMorphologicalTable consisting of the following columns: word, prefix, stem, suffix, prefixCateg, stemCateg, and suffixCateg. Because a word may have multiple decompositions, each word in the table may have more than one row corresponding to it. Saavb words that are outside the vocabulary of Buckwalter (mainly mispronunciations) are decomposed as prefix =  $\phi$ , stem = word, suffix =  $\phi$ , and stemCateg = 'NonSubword'. This results in updated values of |BuckwalterStem| = 44212 and |BuckwalterStemCateg| = 219. Henceforth, these extended parameter values are referred to as Buckwalter parameter values.

In Stage III, the subsets of the appended listings are extracted and matrices to define the parameter values. The system computes two groups of subsets of the Buckwalter listings and matrices: Saavb Group and Buck Group. The Saavb Group is created by traversing through the SaavbMorphologicalTable to compute the indexed listing SaavbPrefix, SaavbStem, SaavbSuffix, SaavbPrefixCateg, SaavbStemCateg, SaavbSuffixCateg, as well as the two-dimensional binary association matrices and three-dimensional binary combination matrices. These parameter sizes are summarized in Table III. For the Buck Group, a subset of the Buckwalter listings and matrices is created that is larger than the Saavb Group by extracting subsets of BuckwalterPrefix, BuckwalterStem, and BuckwalterSuffix whose categories are the same as SaavbPrefixCateg, SaavbStemCateg, and SaavbSuffixCateg respectively. The resulting listings are BuckPrefix, BuckStem, BuckSuffix, BuckPrefixCateg, BuckStemCateg, and BuckSuffixCateg, with sizes summarized in Table IV.

TABLE III. SAAVB MORPHEME PARAMETER SIZES\*

Parameter	Size
SaavbPrefix	37
SaavbSuffix	34
SaavbStem	1586
SaavbPrefixCateg	36
SaavbSuffixCateg	102
SaavbStemCateg	110
SaavbNonSubword	342
*From Saavb corpus. A member of SaavbPrefix may be associated with more than one member of SaavbPrefixCateg. Same applies for Suffix and Stem	

TABLE IV. BUCK MORPHEME PARAMETER SIZES\*

Parameter	Size
BuckPrefix = BuckwalterPrefix	131
BuckSuffix = BuckwalterSuffix	209
BuckStem = BuckwalterStem + NonSubword	44212
BuckPrefixCateg = SaavbPrefixCateg	36
BuckSuffixCateg = SaavbSuffixCateg	102
BuckStemCateg = SaavbStemCateg	110
* From Saavb morpheme categories and modified Buckwalter morphemes	

## V. CONSTRUCTION OF ASR SYSTEM

The parameters generated in the previous section are used with the ASR parameterized grammar-based models of Section III to construct seven ASR systems with a wide range of vocabularies. The Saavb Group parameter values of Table III are used with the ASR models of Section III to construct the following ASR systems: (1) Saavb Independent Morpheme (IM), (2) Saavb Direct Morpheme (DM), (3) Saavb Affix Category (AC), (4) Saavb Stem Category (SC), (5) Saavb Full Category (FC), (6) LargeBuck Full Category (LBFC), and (7) SmallBuck Full Category (SBFC).

The LargeBuck Full Category ASR system is created by using the Buck Group parameters summarized in Table IV with the Full Category model. The SmallBuck Full Category ASR system is built from Saavb Group stems and Buck Group affixes, with the parameters consisting of indexed listings BuckPrefix, SaavbStem, BuckSuffix, SaavbPrefixCateg, SaavbSuffixCateg, SaavbStemCateg summarized in Tables III and IV; the association matrices:

- BuckPrefix\_SaavbPrefixCateg,
- SaavbStem\_SaavbStemCateg,
- BuckSuffix\_SaavbSuffixCateg; and the combination matrix
- SaavbPrefixCategXSaavbStemCategXSaavbSuffixCateg.

The vocabulary sizes of the concatenative ASR systems are listed in Table V. All vocabularies have only valid words except for the Independent Morpheme system. The following represents the subset relations between vocabularies:  $DM \subset AC$ ,  $DM \subset SC$ ,  $AC \subset FC$ ,  $SC \subset FC$  and  $FC \subset SBFC \subset LBFC$ . The vocabulary of DM is equal to the SAAVB vocabulary by construction.

TABLE V. ASR SYSTEM CHARACTERISTICS

System	Vocabulary	Dictionary	Nodes (Edges)	WER %
<b>Saavb Concatenative ASR Systems and Word counterparts</b>				
IM	1,995.188	1,623	1,666 (3,320)	67
W_IM	1,995.188	1,995.188	1,995.192 (3,990,379)	*
DM	1,719	1,623	5,920 (7,890)	55.7
W_DM	1,719	1,719	1,723 (3,441)	55.8
AC	5,069	1,623	36,778 (55,586)	57.5
W_AC	5,069	5,069	5,073 (10,141)	57.8
SC	30,603	1,623	42,011 (82,208)	63.3
W_SC	30,603	30,603	30,607 (61,209)	64.6
FC	74,543	1,623	68,547 (133,491)	63.6
W_FC	74,543	74,543	74,547 (149,089)	64.6
<b>Buck Concatenative ASR Systems and Word counterparts</b>				
SBFC	226,861	1,875	73,477 (143,292)	63.8
W_SBFC	226,861	226,861	226,865 (453,725)	*
LBFC	5,323,415	44,429	1,135,723 (2,267,729)	*
W_LBFC	5,323,415	5,323,415	5,323,419 (10,646,833)	*
- DM=Direct Morpheme, AC=Affix Category, SC=Stem Category, FC=Saavb Full Category, SBFC=Small Buck Full Category, LBFC=Large Buck Full Category. - W_ indicates corresponding word ASR * indicates that recognition experiments were not conducted because of the large lattice size				

The dictionary of all the ASR systems consists of pronunciations of the union of Prefix, Stem, and Suffix. Hence, the dictionaries of all Saavb concatenative ASR systems are the same, as indicated in Table V, which also shows the dictionary sizes for the SBFC and LBFC ASR systems. The recognition lattice sizes of the ASR systems are likewise summarized in Table V. The LBFC system, with a lattice size encompassing more than one million nodes and two million edges, is not implementable.

The concatenative ASR model is much more scalable than the standard Word ASR model for languages with inflectional morphology.

## VI. EXPERIMENTAL SETUP

This section presents implementation issues of ASR systems. Subsection A presents the conventional word ASR with which comparisons of the proposed ASR systems are made. Subsection B presents training and test sets used in the experiments. Subsection C summarizes the speech training and recognition steps taken.

### A. Conventional ASR Model

The standard word ASR model structure is used as a reference to evaluate the ASR models in terms of vocabulary size, computational requirements such as the number of nodes, edges, dictionary size, and recognition performance as measured by the word error rate (WER). The word ASR is the most structured model as the grammar specifies exactly the vocabulary of the recognition system, and hence provides complete control of the character sequences that are allowed.

The EBNF syntax for the word ASR recognition grammar with words being the terminal nodes is as follows: '#' {Word '&' }+ '#'; Word -> 'word1' | 'word2' | 'word3' |.

Although an end of word marker is not needed, '&' is used to be consistent with the grammar of the ASR model structures. An example of the second line is Word = 'fy' | 'mn' | 'RIP' | 'En' | 'LIP' | 'qlty' | 'mNO' |.

The standard Word ASR systems that are build are counterparts to the Concatenative ASR systems by computing the vocabulary of the developed ASR through the span of its

recognition lattice, determining the dictionary based on the vocabulary, and constructing a word-loop recognition lattice with the nodes representing the words in the vocabulary. As the counterpart Word ASR systems are generated from the vocabulary of the Concatenative ASR systems, a similar subset hierarchical relationship holds true. Table V lists the vocabulary, dictionary, and lattice size for W\_IM, W\_DM, W\_AC, W\_SC, W\_FC, W\_SBFC, and W\_LBFC, where 'W' denotes the word counterpart ASR system.

### B. Training and Recognition Sets

The SAAVB speech corpus consists of prompted utterances spoken over cellular telephones in a quiet environment and received by land telephones sampled at 8 kHz. This corpus is appropriate for comparison between the different ASR systems. The data available for the paper consist of a total of approximately 25,000 utterances comprising 50 utterances with an average duration of 5.7 seconds per utterance spoken by each of the 484 subjects, with a vocabulary of 1719 (unique) words.

The utterances are divided into three mutually exclusive and collectively exhaustive sets, A, B, and C. Each balanced set consists of utterances for different speakers. Three partitions are utilized: Training set consisting of A and B with recognition set being C; training set composed of A and C with recognition set being B; training sets B and C and recognition set A.

### C. ASR Training and Recognition

The HTK toolkit is used in accordance with standard practices [24]. The HTK command HParse converts the generated EBNF of Sections 2 and 3 into recognition lattices. For each of the utterances, feature vectors are based on MFCC of length thirty-nine. Orthographic transcription is mapped into phonetic sequences using a pronunciation algorithm.

Training of HMMs is conducted on the three partitions. HMMs are left to right non-skip with twelve mixtures and they model the phonetic units associated with the Modern Standard Arabic transcriptions. The K-fold method is used with three folds to implement statistically valid training and recognition tasks [25]. Recognition is conducted using the Viterbi algorithm and the empirical results are obtained by averaging the recognition performance values and time durations for the three folds.

As this research's objective is proposal and analysis of sub-lexical speech recognition, rather than optimization of the proposed models, no optimization is conducted by using context dependent phones, large number mixtures, optimized size and structure of HMM, adaptive techniques, or use of stochastic lattices. Optimized choices may reduce word error rate by approximately 30%.

The ASR systems for Concatenative model have the same phonetic units and HMMs as the Word ASR systems and differ only in the lattice structure. Hence improvements in models of phonetic units would translate towards improvement in performance in the same manner for both Word ASR systems and systems proposed in this paper.

## VII. PERFORMANCE AND ANALYSIS

This section analyzes the characteristics of the ASR systems and the results are presented in Table V. It also compares the various sub-lexical ASR systems with their Word ASR counterparts, and derives conclusions on the suitability of the ASR models for the different cases examined in this paper.

Table V lists the vocabulary size, dictionary size, recognition lattice size, and word error rate (WER) for each of the concatenative and word ASR systems. Values for WER for LBFC, W\_SBFC and W\_LBFC are not available, as empirical experiments could not be conducted due to the large lattice size.

Fig. 1 and 2 plot lattice size and WER versus vocabulary on the log scale for the Concatenative ASR systems, in which the abscissa represents vocabulary of only valid words. The squares represent the DM, AC, SC, FC, and SBFC systems and the circles represent their Word counterparts.

### A. Vocabulary

Table V shows that using the same prefixes, stems, suffixes, and dictionary of the Saavb Group, the Concatenative ASR family has vocabularies that range from 1,719 to 74,543, with vocabulary size increasing in relation to the level of abstraction. This finding demonstrates the power of utilizing various levels of abstraction.

Examination of W\_SBFC, SBFC and LBFC reveals the empirical limitations of the Word ASR system and the Concatenative ASR system imposed by the lattice size.

All of the Concatenative ASR systems, with the exception of IM, have only valid words. The vocabulary of FC is the maximal vocabulary for an ASR system containing the prefixes, stems, and suffixes of Saavb, and is a subset of IM vocabulary. Thus, the vocabulary size of 74,543 of FC is the number of valid words in IM, suggesting that only 3.7% of the two million words in IM are valid.

### B. Lattice Size

Table V reveals the 1:1 ratio of the number of nodes to vocabulary size for Word ASR systems. The Concatenative ASR systems become increasingly more efficient for larger vocabularies, having a smaller lattice than the Word ASR systems for vocabularies of more than 50,000 words. In particular, the Full Category systems (FC, SBFC, LBFC) yield very compact lattices because of combination relations between categories of morphemes rather than morphemes themselves.

### C. Dictionary

As illustrated in Table V, the dictionary size of a Word ASR system equals the vocabulary size, and thus poses problems for large vocabulary. In contrast, the dictionary size for Concatenative ASR systems is relatively insensitive to vocabulary size. The dictionary size of Concatenative ASR systems relatively insensitive to vocabulary size in contrast to linear dependency of Word ASR systems.

#### D. Computation Time

Computation time increases with size of the lattice and dictionary. The Word ASR system exhibits an increasing relationship between the number of nodes and the dictionary size with respect to vocabulary size. Consequently, computation time in a Word ASR system is expected to increase with vocabulary size at a higher rate than in a Concatenative ASR system. In contrast, as the Concatenative ASR systems keep dictionary size constant, their computation time is expected to increase at a slower rate than in the Word ASR system. Empirical computation time versus vocabulary for the Concatenative and Word ASR systems confirms the observations above. While the Word ASR system is more efficient for small vocabulary size, the Concatenative ASR systems are superior for vocabulary sizes greater than 10,000 words.

#### E. Word Error Rate

In order to avoid miscalculation of the word error rate (WER) due to inflation of the correct rate arising from '&', the WER for the Concatenative ASR systems is calculated by concatenating the prefix, stem / character sequence and suffix through the end-of-word '&' marker, into words.

In general, for any given model, WER is expected to increase as a function of vocabulary size. Because the test set is the same, there are no OOVs, and the vocabulary has a subset structure, this trend can be attributed to larger search space. Accordingly, the order of ASR systems with respect to WER is expected to be the following: FC<SBFC<LBFC for the Concatenative ASR systems, and W\_DM<W\_AC, W\_DM<W\_SC, W\_AC<W\_FC, W\_SC<W\_FC, W\_FC<W\_SBFCLBFC for the Word ASR systems.

Comparison of the Concatenative ASR systems to their Word counterparts indicates that a Word ASR system is inferior to a Concatenative ASR system for vocabulary of more than 5,000 words. Even though the Concatenative ASR systems have the same vocabularies as their Word counterparts, the WER can be different because the recognition performance depends not only on vocabulary size but also on the lattice. The lattice structure of the Concatenative ASR is very different from the lattice structure of the Word ASR, even though the recognition lattices have the same vocabulary. The other factors that determine performance, such as HMMs, test set, and lattice search method are the same in both cases.

Comparing WER of IM with FC, and DR with IR, which have deviations of around 4%, provides some indication of the importance of combination constraints to ASR systems, and the effect of inflating vocabulary with invalid words on recognition performance.

#### F. ASR Systems with OOV Words

This section studies the effect of out-of-vocabulary (OOV) words on the performance of Concatenative and their Word ASR counterparts. In the empirical experiments, the test set is constrained by the speech corpus, and hence the OOV issue is best handled by modifying the vocabulary of the ASR system to exclude some of the words in the test set. Furthermore, in order to provide uniform comparison across all ASR systems,

OOV words are fixed for all systems and are not varied according to the ASR system vocabulary.

The vocabulary of Concatenative cannot be specified directly, and hence a practical approach is to specify OOV words as those for which stemCateg have particular value. Words for which stemCateg = 'NonSubword' are a good choice for OOVs, as the stems in this category are not additionally classified under other categories.

The test set is of fixed vocabulary and the systems have a subset hierarchy of vocabularies. Consequently, the deterioration in performance is expected to increase with the increase in vocabulary size of the ASR system. However, this is not an issue in our case because the objective is to compare the deterioration in performance of sub-lexical ASR models proposed in the paper with respect to their Word counterparts.

Comparison of performance of ASR systems with OOV to ASR systems without OOV indicates that the deterioration in performance of the Concatenative ASR systems is comparable to that of Word ASR systems at 3% for Direct Morpheme, reaching an insignificant level for Full Category with higher vocabulary. The models developed and analyzed in this paper are observed to be as robust to OOV as their Word counterparts.

### VIII. RESULTS AND DISCUSSION

This paper has developed promising Concatenative grammar-based ASR models for languages with distinctly different word formation processes with the objective of vocabulary scalability and good recognition performance, in which words are formed through affixation of prefixes, stem, and suffixes.

Theoretical grammar constructs of a language are used to develop a rich hierarchical structure of ASR models affording scalability. The concept of combination matrices to limit vocabulary to only valid words has been rigorously developed and applied. Empirical experiments show the viability of using Concatenative grammar-based ASR models to attain good recognition performance. Future work can develop stochastic Concatenative ASR models by addressing the issues presented in the paper.

In the experiments, the standard Word ASR model has the best characteristics for vocabulary of less than 5000 words and the Concatenative ASR family is most appropriate for vocabulary up to half a million words. Theoretical grammar-based combination constraints are an important factor in ASRs, and although ASRs without combination constraints have smaller lattices, their vocabularies have a significant number of invalid words and a higher WER.

### IX. CONCLUSION AND FUTURE WORK

A future research plan is to develop a stochastic concatenative ASR models to improve performance by incorporating statistics of word sequences in the recognition lattice. In contrast to uniform Word ASR lattice which may be extended to stochastic Word ASR by simply supplementing the single level lattice with additional edges between word nodes to reflect bigram statistics, stochastic concatenative ASR

model is fundamentally different from the theoretical grammar-based ASR model presented in this paper.

The lattice structures of the stochastic concatenative models need to be developed distinctly for the variety of paradigms developed. Particular attention has to be paid to ensure that stochastic models have vocabularies of only valid words just as the proposed concatenative ASR models which use combination matrices. Morphological processing of valid word lists yields vocabulary with invalid words.

Another challenge in the development of stochastic models is that words have multiple morphological decompositions, and hence the unigram statistics of a component would be based not only on the word unigram, but also on the conditional statistics of the decompositions of a given word. This issue carries on with higher level statistics.

#### ACKNOWLEDGMENT

This project was funded by the National Plan for Science, Technology and Innovation (MAARIFAH), King Abdulaziz City for Science and Technology, Kingdom of Saudi Arabia, Award Number (10-INF1324-02).

#### REFERENCES

- [1] Huang, Xuedong, et al. Spoken language processing: A guide to theory, algorithm, and system development. Prentice hall PTR, 2001.
- [2] Hirsimäki, Teemu, et al. "Morphologically motivated language models in speech recognition." Proceedings of the International and Interdisciplinary Conference on Adaptive Knowledge Representation and Reasoning. 2005.
- [3] Seneff, Stephanie. "The use of subword linguistic modeling for multiple tasks in speech recognition." Speech communication 42.3-4 (2004): 373-390.
- [4] Sak, Haşim, Murat Saraşlar, and Tunga Güngör. "Integrating morphology into automatic speech recognition." 2009 IEEE Workshop on Automatic Speech Recognition & Understanding. IEEE, 2009.
- [5] Creutz, Mathias, et al. "Morph-based speech recognition and modeling of out-of-vocabulary words across languages." *ACM Transactions on Speech and Language Processing (TSLP)* 5.1 (2007): 1-29.
- [6] Kneissler, Jan, and Dietrich Klakow. "Speech recognition for huge vocabularies by using optimized sub-word units." Seventh European Conference on Speech Communication and Technology. 2001.
- [7] Kwon, Oh-Wook, and Jun Park. "Korean large vocabulary continuous speech recognition with morpheme-based recognition units." Speech Communication 39.3-4 (2003): 287-300.
- [8] Ircing, Pavel, Josef V. Psutka, and Josef Psutka. "Using morphological information for robust language modeling in Czech ASR system." *IEEE transactions on audio, speech, and language processing* 17.4 (2009): 840-847.
- [9] Ri, Hyok-Chol. "A usage of the syllable unit based on morphological statistics in Korean large vocabulary continuous speech recognition system." *International Journal of Speech Technology* 22.4 (2019): 971-977.
- [10] Ordelman R., Hessen A., and Jong F., "Compound Decomposition in Dutch Large Vocabulary Speech Recognition," Proceedings of EUROSPEECH, pp. 225 –228, 2003.
- [11] Kirchhoff K., Vergyri D., Bilmes J., Duh K., and Stolcke A., "Morphology-Based Language Modeling for Conversational Arabic Speech Recognition," *Computer Speech and Language*, vol. 20, no. 4, pp. 589-608, 2006.
- [12] Choueiter G., Povey D., Chen S.F., and Zweig G., "Morpheme-based language modeling for Arabic LVCSR," Proceedings of ICASSP, 2006.
- [13] Lamel L., Messaoudi A., and Gauvain J., "Automatic speech-to-text transcription in Arabic", *ACM Transactions on Computational Logic*, 2009.
- [14] Xiang B., Nguyen K., Nguyen L., Schwartz R., and Makhoul J., "Morphological decomposition for Arabic broadcast news transcription", ICASSP, 2006.
- [15] Diehl F., Gales M., Tomalin M., and Woodland C., "Morphological Decomposition in Arabic ASR Systems" *Computer Speech and Language*, 2012.
- [16] Mousa A., Schlüter R., and Ney H., "Investigations on the use of morpheme level features in language models for Arabic LVCSR", ICASSP, 2012.
- [17] Liu, Chang, et al. "Evaluating Modeling Units and Sub-word Features in Language Models for Turkish ASR." 2018 11th International Symposium on Chinese Spoken Language Processing (ISCSLP). IEEE, 2018.
- [18] Rotovnik T., Maučec M., and Kačič Z., "Large Vocabulary Continuous Speech Recognition of an Inflected Language Using Stems and Endings," *Speech Communication*, vol. 49, no. 6, pp. 437-452, 2007.
- [19] Ablimit, Mijit, Tatsuya Kawahara, and Askar Hamdulla. "Morpheme Segmentation and Concatenation Approaches for Uyghur LVCSR." *International Journal of Hybrid Information Technology* 8.8 (2015): 327-342. From 5.
- [20] Donaj, Gregor, and Zdravko Kačič. "Speech Recognition in Inflective Languages." *Language Modeling for Automatic Speech Recognition of Inflective Languages*. Springer, Cham, 2017. 5-29.
- [21] Menacer, Mohamed, et al. "An enhanced automatic speech recognition system for Arabic." *The third Arabic Natural Language Processing Workshop-EACL 2017*. 2017.
- [22] Alkhairy, Maha, Afshan Jafri, and David A. Smith. "Finite State Machine Pattern-Root Arabic Morphological Generator, Analyzer and Diacritizer." *Proceedings of The 12th Language Resources and Evaluation Conference*. 2020.
- [23] Buckwalter T., "Buckwalter Arabic Morphological Analyzer," Version 2.0; Linguistic Data Consortium, December 2004.[22] AlGhamdi M., AlHargan F., AlKanhal M., Alkhairy A., Eldesouki M., and Alenazi A., "Saudi Accented Arabic Voice Bank," *Journal of King Saud University: Computer Sciences and Information*, vol. 20, pp. 43-58, 2008.
- [24] Young S. et al., *The HTK Book (for HTK Version 3.4)*, Cambridge University, 2006.
- [25] Blum A., Kalai A., and Langford J., "Beating the Hold-Out: Bounds for K-fold and Progressive Cross-Validation," *Proceedings of COLT/99*, pp. 203-208, 1999.

#### APPENDIX

The Independent Morpheme ASR parameterized model has no constraints imposed on the prefix-stem-suffix combinations either directly or indirectly, and hence allows invalid words in the vocabulary. The parameters of this model are the indexed morpheme listings Prefix, Stem, and Suffix. These models correspond to currently proposed models in the literature. The recognition grammar is illustrated below:

# {Word '&' }+ #'

Word -> Prefix Stem Suffix;

Stem -> 'mktb' | 'mdrsO' | 'ktb' | 'mktbO'...

Prefix -> prefix1 | prefix2 | ...;

Suffix -> suffix1 | suffix2 | ...;

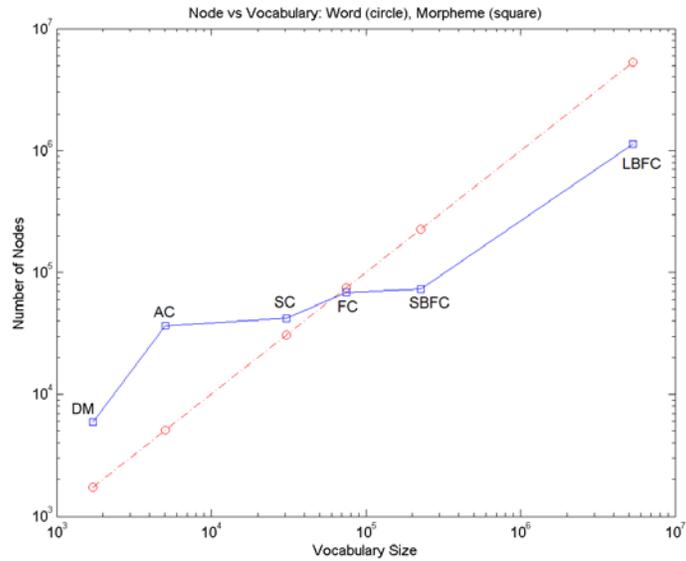


Fig. 1. Node vs Vocabulary. Comparison of the Relation between Number of Nodes and Size of Vocabulary in Word ASR Systems and Concatenative ASR Systems. Circles and Dashed Lines Represent Word ASR Systems; Squares and Solid Lines Represent Concatenative ASR Systems. [Left to Right: DM=Direct Morpheme, AC=Affix Category, SC=Stem Category, FC=Saavb Full Category, SBFC=Small Buck Full Category, LBFC=Large Buck Full Category (LBFC)]. The Figure Shows that Concatenative ASR Systems are more Efficient with Increasing Vocabulary Size, Surpassing Word ASR Systems for Vocabulary of more than 50,000 Words.

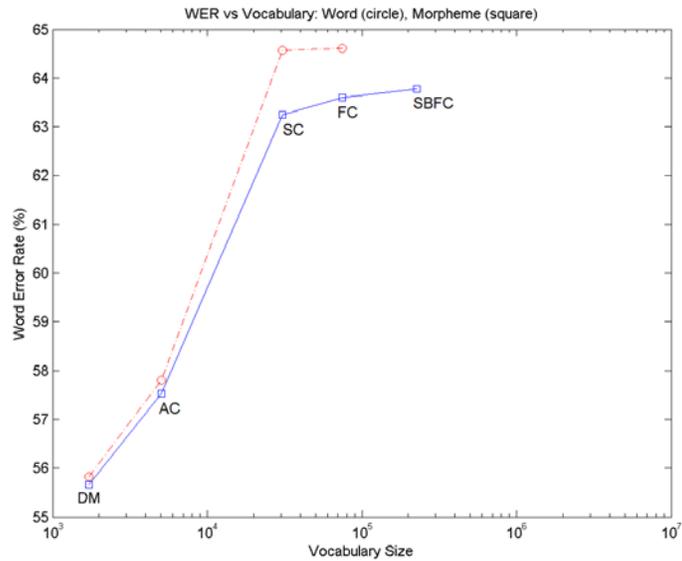


Fig. 2. WER vs. Vocabulary. Comparison of the Relation between Word Error Rate (WER) and Size of Vocabulary in Word ASR Systems and Concatenative ASR Systems. Circles and Dashed Lines Represent Word ASR Systems; Squares and Solid Lines Represent Concatenative ASR Systems. [Left to Right: DM=Direct Morpheme, AC=Affix Category, SC=Stem Category, FC=Saavb Full Category, SBFC=Small Buck Full Category]. The Figure Shows that WER of Concatenative ASR Systems are Lower than Word ASR Systems for Vocabulary Size Larger than 5,000 Words.

# Multiclass Vehicle Classification Across Different Environments

Aisha S. Azim<sup>1</sup>, Ashraf Alkhairy<sup>3</sup>  
King Abdulaziz City for Science and Technology  
Riyadh, SA

Afshan Jafri<sup>2</sup>  
College of Computer and Information Sciences  
King Saud University, Riyadh, SA

**Abstract**—Vehicle detection and classification are necessary components in a variety of useful applications related to traffic, security, and autonomous driving systems. Many studies have focused on recognizing vehicles from the point of view of a single perspective, such as the rear of other cars from the driving seat, but not from all possible perspectives, including the aerial view. In addition, they are usually given prior knowledge of a specific kind of vehicle, such as the fact that it is a car, as opposed to being a bus, before deducing other information about it. One of the popular classification techniques used is boosting, where weak classifiers are combined to form a strong classifier. However, most boosting applications consider complex classification problems to be a combination of binary problems. This paper explores in detail the development of a multi-class classifier that recognizes vehicles of any type, from any view, without prior information, and without breaking the task into binary problems. Instead, a single multi-class application of the GentleBoost algorithm is used. This system is compared to a similar system built from a combination of separate classifiers that each classifies a single vehicle. The results show that a single, multi-class classifier clearly outperforms a combination of separate classifiers, and proves that a simple boosting classifier is sufficient for vehicle recognition, given any type of vehicle from any perspective of viewing, without the need of representing the problem as a complex 3D model.

**Keywords**—Vehicle detection; vehicle recognition; multiclass learning; boosting; GentleBoost

## I. INTRODUCTION

The detection and classification of vehicles are essential steps in many important applications, including autonomous driving systems, traffic flow prediction for transport management, vehicular safety, criminal tracking, and intelligent transportation systems with implementations that range from security surveillance to traffic monitoring during the Hajj season, impacting millions of pilgrims at a time. Coupled with the fact that cameras and imaging technology have seen massive improvements in recent years, on-road vehicle detection has become an active research area with valuable progress for close to a decade.

A large number of vehicle detection studies concentrate on vehicles seen from a specific view or perspective, such as the rear view of vehicles as they appear from the ego vehicle's driving seat, or from a camera mounted on the ego vehicle. There are different forms of classification that can be used to detect vehicles: multi-view classification, which recognizes the same vehicle from different viewing perspectives or poses; and

multi-class classification, which recognizes vehicles in spite of variations in their shapes and sizes, based on belonging to different classes, such as buses and cars. There are systems that have been designed to recognize objects from different views, but they are often generalized object detectors [1], or else they focus either on vehicle detection through multi-view classification [2], or else through multiclass classification [3], [4]. But so far there have not been many serious studies on vehicle detection that support both multi-view and multi-class applications.

This paper will explore the development of a system that recognizes vehicles both across views as well as across classes, using cascaded boosting.

First introduced by Viola and Jones [5] to detect human faces, the cascaded boosted classification is one of the popular techniques in use for vehicle detection and recognition. It reaches high levels of classification accuracy by using weak classifiers which individually have low accuracy, but which are combined together to produce a strong classifier.

Studies in the concept of boosted classification began in the 1990s [6], and have since been picked up by researchers and applied to a rich variety of problems across different fields. Breiman, an expert in machine learning, claimed that "Boosting is the best off-the-shelf classifier in the world." [7].

Many vehicle detection systems have been built using boosted classification as well. These are often developed with different variations in the features used for classification, the exact boosting algorithm implemented, or an efficient combination of the features and the boosting classifier. However, the vast majority of these systems remain confined to binary classification; hence they often address simple questions as well. Two such questions would be: "is this vehicle a so-and-so model?", or "is this object a car from the rear view?" Note that questions like these are either (a) answered with a-priori information, or (b) limited in scope. For example, the first question was already provided with information that the object was a vehicle, and the second asked whether an object was the rear-view of a car, but not whether it was a car given any view of it.

This paper will attempt to recognize vehicles in a real-world scenario, using multi-class boosted classification, with no a-priori knowledge. That is, our system must be able to answer the complex question of whether an object is a vehicle, irrespective of (a) what type of vehicle it is (car, truck, bus), and (b) what perspective it is viewed from. In order to do this,

we will extend the binary classification problem to m-ary classification.

The rest of this work is organized as follows. Related literature is presented in Section II, starting from an overview of the field of object detection, then focusing on vehicle detection in particular, and then briefly covering work on multi-class classification. Section III highlights the contribution of this paper. The approach and system modeling of our study are described in detail in Section IV. The Boosting algorithm will first be introduced, followed by the formal modeling of our system, and then the two approaches that we take towards achieving Vehicle Classification. Section V describes the experimental setup, the tools, the data and the method in detail; and Section VI presents the experimental results and discussion. Section VII concludes this paper.

## II. RELATED WORK

### A. Background

Object detection is a vast field within computer vision. With wide applications across robotics, control systems, security systems and automation, much research has been conducted in order to develop systems that can recognize vast arrays of objects from a single image. The problem is challenging, but progress has been made towards systems that can recognize limited numbers of objects.

Vehicle detection is one specific application of object detection that has seen notable progress in the past decade.

Methods of detecting vehicles in computer vision broadly fall under two categories: motion-based and appearance-based. Motion-based methods require an input of a stream of images, and they recognize the movement of vehicles against a stationary background. Whatever does not change – or changes slowly – over the image stream is taken to be the background, with the remaining objects being considered as moving objects. Motion-based methods are useful for applications such as driving assistance systems, where the vehicle is running live on the road and has access to a stream of input images, or for automated driving [8], [9], [33].

However, the drawback of motion-based methods is that they can work only given a stream of images, but not with individual, static images. This limits their application since there are many instances in traffic surveillance or crime tracking when a stream of images is not available as input. In addition, the majority of the motion-based approaches in the literature are useful from the point of view of the ego vehicle or a fixed camera.

Appearance-based methods are able to detect objects based on their appearance in a single, static image. Given efficient algorithms, they can also be used in real-time applications in the same way that motion-based methods can be used, utilizing continuity of motion to further enhance performance. While the literature has explored appearance-based methods also from the point of view of the ego vehicle, it has also been used extensively to detect vehicles from other angles.

In addition to traffic surveillance, criminal detection requires vehicle recognition too, and not only from the ground but often from high altitudes, and over different environments.

While aerial view vehicle detection exists [10], it is specific to that application and not focused on accurate detection from the ground view.

This paper describes a system that is capable of recognizing different classes of vehicle, across different environments, and from different views — aerial or ground.

### B. Vehicle Detection

Under the appearance-based paradigm, different methods have been adopted for vehicle detection. We mention a few prominent ones below.

Behley et al [11] used a mixture model of bag-of-words representation of segments to classify segments from given input images. The system was specific for laser-based images and was particularly applicable to driving assistance for cars equipped for laser scan images.

Part-based models have also been used in vehicle detection, where the individual parts of a vehicle are used to detect the whole. This idea was used by Felzenszwalb et al [2] and Ye Li et al [12]. Felzenszwalb et al used latent Support Vector Machines to train mixtures of multi-scale, star-structured part-based models, relative to the “root” of the object. The parts were determined at a higher resolution using finer filters, while the root was detected using a coarse resolution. Scores were calculated to measure the relative distance of the parts from the root, using a feature pyramid representing the input image at different scales. While this method is capable of detecting vehicles despite variations including pose, it is limited to a range of angles, since deformable parts are not visible at all angles of a vehicle. For instance, the top or the side pose of a car are very different from the front view, and the detection of these views was not explored.

Similarly, Ye Li et al [12] used part-based models as well, using two-part vehicle models with a focus on tackling the occlusion challenge. The study focuses on urban environments and on vehicles in limited poses, while our work focuses on vehicles in multiple poses and across multiple environments.

Several other approaches have been used [13], [14], [15], [16], but one of the prominent approaches remains the boosted classification approach [6].

Boosted classification emerged as a powerful method of object detection after the instrumental work on face detection by Viola and Jones [5]. The Viola-Jones classifier gained its power and popularity by using classifiers which were individually only slightly more accurate than 50%, and hence did not require complex computations, but which together created a robust classifier when combined. Various boosting mechanisms have been used in vehicle detection as well, such as [17] and [18] that used online boosting, [19] and [34] which employed Adaboost including for active learning, and the various boosting studies in [20].

However, most of these methods have been focused on the detection of vehicles in limited poses and from limited perspectives, with the most common being vehicle rear-view detection from the perspective of the ego vehicle.

### C. Boosted Classification for Object Detection

Aside from vehicle detection in particular, multi-class classification in the context of general object detection has been studied earlier. Torralba et al [21] trained images using JointBoost, which employs GentleBoost for training but with shared stumps among classes. The shared feature-learning was introduced to take advantage of the similarity of object features during multi-view classification, which reduces the space and time complexity for learning individual binary classifiers. On the other hand, using shared regression stumps reduced the precision of intra-class classification.

Shalev-Shwartz et al [22] followed a similar approach, but used different heuristics per boosting round in order to improve intra-class classification.

However, in both cases, the multi-class classification problem was still fundamentally treated as a combination of binary classifiers.

### III. CONTRIBUTION

This work explores the development of a comprehensive vehicle classification system. Its contributions are three-fold.

First, multi-view vehicle classification will be attempted for the first time using multi-class Gentle Boosting, where most other studies on vehicle detection have traditionally implemented boosted classification by dividing the problem into binary problems, rather than treating it as an m-ary problem.

Secondly, the system will detect vehicles across two major dimensions: vehicle class, where the classes consist of (i) cars, and (ii) big vehicles; and vehicle perspective, or view. This system considers 25 likely perspectives for each vehicle, starting with the horizontal rear view of the vehicle, and moving around the vehicle with different angles of inclination, until the final top view. Most other studies focus on classifying the view of cars only, or they focus on different vehicle classes but from a single viewpoint.

Thirdly, since the literature tends to study techniques intended to tackle the individual issues related to vehicle detection, such as detection in spite of occlusions, a paper that comprehensively describes the implementation of a vehicle classification system will be a valuable contribution to the field of vehicle detection at this point.

### IV. APPROACH AND SYSTEM MODEL

#### A. Boosting

This paper describes the implementation of a multi-class boosting classifier for vehicle detection that treats the problem as inherently multi-class, rather than breaking it down into binary problems.

Boosting algorithms have been used for multi-class classification before. But before addressing multi-class classification, let us make a quick review of the basic boosting algorithm for binary problems.

Adaboost is one of the most basic boosting algorithms and was proposed by Freund and Schapire [6].

The crux of the algorithm is to use many weak learners, or classifiers with accuracy slightly better than 50%, and to combine them to build a strong classifier. The performance of weak classifiers are improved over a number of rounds on a given dataset, by noting which classifiers generated errors in previous rounds, and adjusting weights on misclassified training samples in order for the weak classifiers to “improve” classification in subsequent rounds.

AdaBoost, for a binary problem, is presented below as Algorithm 1 [23].

---

**Algorithm 1 Discrete AdaBoost**

---

1. Start with weights  $w_i = 1/N, i=1, \dots, N$

2. Repeat for  $m = 1, 2, \dots, M$ :

(a) Fit the classifier  $f_m(x) \in \{-1, 1\}$ , using weights  $w_i$  on the training data.

(b) Compute  $err_m = E_w[1_{(y \neq f_m(x))}]$ ,  $c_m = \log((1 - err_m)/err_m)$

(c) Set  $w_i \leftarrow w_i \exp[c_m 1_{(y \neq f_m(x))}]$ ,  $i=1, 2, \dots, N$ , and renormalize so that  $\sum_i w_i = 1$ .

3. Output the classifier  $sign[\sum_{m=1}^M c_m f_m(x)]$ .

---

In this algorithm,  $N$  represents the number of training samples, which are pairs of data points  $x_i$  and its corresponding true class  $y_i$ , which can be either -1 or 1. Training data is input as  $(x_1, y_1), \dots, (x_N, y_N)$ .  $M$  is the number of weak classifiers,  $f_1(x), \dots, f_M(x)$ , each of which can output either 1 or -1.  $E_w$  is the expectation of training data of weights  $w=(w_1, \dots, w_N)$ , and  $I\{S\}$  indicates the set  $S$ .

At the beginning of the algorithm, all training samples are given equal weights. Then, for each weak classifier  $f_m(x)$ , a constant,  $c_m$ , is computed to generate a weight for each data point, based on the error of the classifier. New weights are then calculated for each training sample in such a way that those samples that were misclassified have their weights increased by a factor that depends on the weighted training error.

The strong classifier,  $F(x)$  is defined as the sum of the products of  $c_m$  and  $f_m$ , a linear combination of all the weak classifiers. The final prediction is  $sign(F(x))$ .

However, because Adaboost concentrates weight exponentially on misclassified samples, it becomes sensitive to noise. In order to address this problem, GentleBoost was proposed [23]. It successfully overcomes the noise-sensitivity issue by updating the weak classifiers in bounded steps, rather than unbounded steps. GentleBoost classifiers are regression functions that return class probability estimates, which are then used in a factor for computing new weights to update the functions.

The GentleBoost algorithm is reproduced below in Algorithm 2.

---

**Algorithm 2 Gentle AdaBoost**

---

1. Start with weights  $w_i = 1/N, i=1, \dots, N, F(x) = 0$ .
  2. Repeat for  $m = 1, 2, \dots, M$ :
    - (a) Fit the regression function  $f_m(x)$  by weighted least-squares of  $y_i$  to  $x_i$  with weights  $w_i$ .
    - (b) Update  $F(x) \leftarrow F(x) + f_m(x)$ .
    - (c) Update  $w_i \leftarrow w_i \exp[-y_i f_m(x_i)]$ , and renormalize.
  3. Output the classifier  $\text{sign}[F(x)] = \text{sign}[\sum_{m=1}^M f_m(x)]$ .
- 

Multi-class classification using boosting algorithms was traditionally implemented by breaking a single problem down into binary classifications of many problems. Then final class selection was then made using comparisons among the selections of all the different binary classifiers.

This could be done using three techniques:

1) *One-versus-all approach*. [24] This approach takes a single class as the base class which each of the other classes is paired up against to form a binary problem. After all the binary problems have made predictions, the prediction with the highest score is chosen.

2) *All-versus-all approach*. [24] In this case, given  $N$  classes,  $N(N-1)$  classifiers are built, with one classifier for each combination of binary pairs that the problem can be decomposed into. Note that classifiers need to be trained to distinguish the object they are built to classify, separately from objects not of that class. Therefore they are generally trained on sets of positive samples of data, and negative samples. In the case of a car-classifier, positive samples would comprise data or images that represent cars, while negative samples might comprise data related to bicycles, people, or animals. In the All-versus-All approach, if  $f_{ij}$  is taken as the classifier where class  $i$  consists of positive examples and class  $j$  samples are negative, then the final classified result is:

$$f(x) = \text{argmax}_i (\sum_j f_{ij}(x))$$

3) *Error-correcting codes*. [25] This approach looks at the task as a decoding problem, where the correct output class is transmitted over a channel. A matrix representing the true prediction of each for each binary classifier is used as a reference of codewords against which the true class of the problem is then decoded.

Among the notable boosting algorithms for multiclass classification are:

1) *Adaboost.MH*. [26] – This is an implementation of the One-versus-All approach among several binary classifiers.

2) *SAMME*. [27] – This too is based on the original AdaBoost algorithm. However, it improves on Adaboost.MH by generically extending the algorithm to a multiclass problem without breaking down into binary problems.

3) *GAMBLE* [28] – “Gentle Adaptive Multiclass Boosting Learning”. In the same way that SAMME generalizes AdaBoost.MH to the multiclass problem, GAMBLE is the generalization of GentleBoost.MH. It uses Quasi-Newton smoothing on the loss function.

4) *GentleBoost.C*. – This is also a natural multiclass extension to GentleBoost, but offers an improvement over GAMBLE because of the introduction of a new, smooth loss function, C-loss, which also incorporates conditional class probabilities. [29] Because of its greater robustness and insensitivity to noise, we use Gentleboost as our boosting framework, and in particular we implement Gentleboost.C.

### B. Problem Formulation

We start by defining some important terms used in the rest of this paper:

- *Class*: The type of vehicle Car or Big Vehicle, such as a bus or truck.
- *View*: The view/perspective of vehicle. The total possible views explored in this paper are presented in Table I.
- *Environment*: The physical environment of the vehicle, i.e. “city” or “desert/mountain”.
- *HoG*: “Histogram of Oriented Gradients” (HoGs); these are the features that our system uses to represent the vehicles, based on the changes in color intensity in the image. The HoG features of an image are computed by first dividing the image into equal blocks, and then computing the orientation of the gradients in each. This shows how color levels change in different locations within the image. The information from each block is then concatenated to form a feature vector of oriented gradients. HoG descriptors were introduced by Dalal and Triggs [30] for the detection of humans in images, and have since become one of the standard and oft-used features for object detection and classification.

From [29], we model our problem as a multiclass extension to the binary GentleBoost algorithm.

Let training data  $X$  consist of  $x_1, \dots, x_n$  observations, where  $n$  is the number of training data samples.  $X$  represents the feature vectors of the observations. While any set of features could be used, in our implementation, we use HoG features. Each observation,  $x_i$ , is provided with its response  $y$ , indicating its true class, which is a combination of what kind of vehicle it is, and from which view is it being seen. Two possible examples of what a true class might represent are:

- (vehicle: car, azimuth: 000, angle of inclination: 00)
- (vehicle: bus, azimuth: 045, angle of inclination: 30)

Let  $m$  be the total number of classes that the data can be classified into.

The multi-class classification task is modeled as a combination of linear, weighted regression problems, where each class represents one regression function. The regression parameters represent the features in each observation. The

regression weights are calculated using a multiclass C-loss, which is a smooth coherence loss function described in [31]. C-loss is superior to regular hinge loss or logit loss not only because of its statistically desirable properties but because it encapsulates conditional class probabilities.

In the spirit of boosting algorithms, the regression parameters are fine-tuned over a number of boosting rounds. Each round generates a weak classifier, which additively influences the classifiers of the next round, until we have completed H boosting rounds of our choice, to arrive at the final strong classifier.

The algorithm, GentleBoost.C, is listed at the end of Section V.

We implement GentleBoost.C for each of the two classification approaches that we adopt, explained below.

### C. Two Approaches

Based on previous work by Viola and Jones [5], each view will require its own separate classifier. Training a single classifier with samples of all views of one object is likely to result in poor recognition [32].

Given our problem, we would like to see which level of detail is required to distinguish between views for accurate vehicle detection. We start with 25 views of the vehicle, and reduce the number of views until we reach the number that produces optimal results. We refer to this number as V.

The problem of complete detection can then be approached in two ways, illustrated in Fig. 1 and described below:

- Combine |C| vehicle class classifiers. Given an image, the system runs separate classifiers to identify the class of a vehicle,  $c \in C$ , which independently vote on the view of the assumed class. Take for instance the case of  $C = \{car, bus, truck\}$ , (so that  $|C| = 3$ ) and  $V=25$ , so that there are 25 views per vehicle class. First the 25-view car classifier will generate confidence scores for each view given an image, followed by the bus classifier and then the truck classifier. With each classifier providing its own confidence measure of the possible view of the given vehicle, we normalize the scores from each classifier in order to make a final decision based on all the scores combined, and we select the view and class with the highest score.
- Build a single  $V \times |C|$  multi-class classifier. In this case, a single  $V \times |C|$ -class classifier is used to classify objects in a single step. So in the case of 3 vehicle classes and 25 views, this classifier would be built to distinguish between  $25 \times 3 = 75$  possibilities, each possibility being a combination of vehicle class and view, plus one more possibility: not-a-vehicle. This particular case would therefore call for a 76-class classifier.

A third approach was considered, which first classifies the view of an image given |V| views, and then determines which of the |C| classes it belongs to. This approach was found not to be a viable option based on the HoG-based method employed (Section D: Method), which necessitates that objects of interest

across different images must be somewhat similar in size and position, relative to each image's center. Because large vehicles such as trucks and buses occupy images very differently from cars, then a classifier trained on images of cars and trucks would perform poorly, despite all vehicles being of the same view.

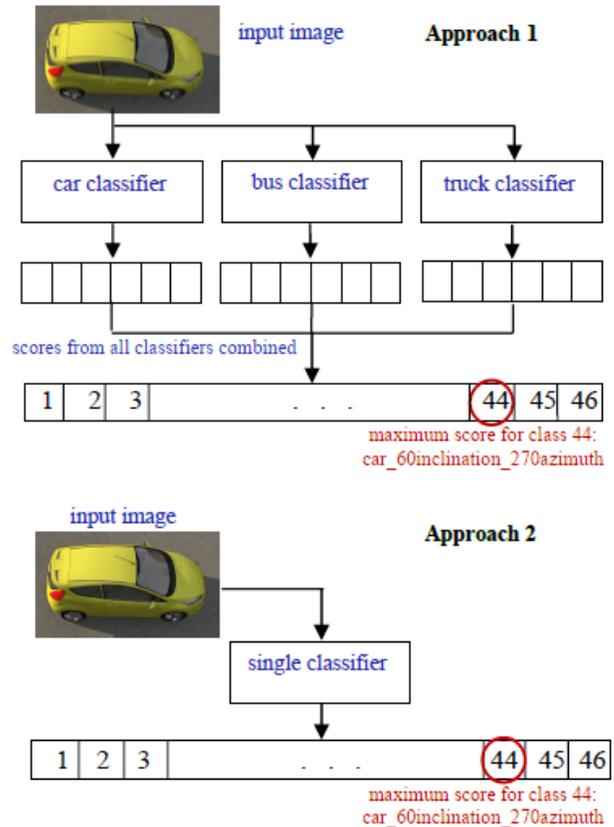


Fig. 1. Two Approaches to Multi-Class Vehicle Classification.

## V. CONTRIBUTION

### A. Experimental Setup

Our training data consisted of equally sized images of cars, buses and trucks, in different environments, in all their different views. The testing dataset comprised of similar data not present in the training samples. (Details are presented in Section C: Data Used).

In the first phase of our work, we determined the number V, i.e. how many views would be optimal for the classifier. Different sets of views were proposed (such as all 25 views of a vehicle, or only 11 views, and so on). These were proposed based on eyeballing the similarity among different sets of the 25 views: in spite of different azimuths and angles of inclination, some different views appeared somewhat similar and could potentially be collapsed into a single view. A randomly chosen subset of the training data was used to train a different classifier for each set of views proposed.

The accuracy for each classifier was recorded in order to determine which set of views yielded the best results. This final number of views was then used to train the full system in both of its approaches.

The full system was then evaluated against the test dataset (details in Section C: Data Used), and its results were compared against a baseline system, built using AdaBoost. This baseline and the results of the comparison are discussed further in Section VI: Results.

**B. Tools Used**

Given that training data would be difficult to obtain from the real world, owing to our specific requirements of vehicle models and classes, we opted to create 3D simulations. Sketchup, a 3D modeling software from Trimble, was used to create several models of vehicles in city and desert environments. Vehicle models were obtained either from the 3D Sketchup Warehouse or the Podium Browser. Sketchup was extended using SU Podium to render photorealistic images of the vehicle models.

The multiclass classification algorithm was written in Python, using the following libraries: Numpy (for all array manipulation), statsmodels (for weighted least squares regression), scikit-image (for extracting HoG features), and scikit-learn and OpenCV (for some utility functions).

**C. Data Used**

As mentioned above in Section B: Tools Used, photorealistic 3D images were generated for our experiments. However, any dataset of real-world images could be used as well, if it covered as comprehensive a range of views, vehicles models and classes, as we propose in this paper. The raw images simulated for this paper were 1300x600 pixels each, of single vehicles. Vehicle models were randomly assigned three possible backgrounds: City1, City2, Desert1. There were initially three classes of vehicles (car, bus, truck), nine models per class (such as Honda Civic or Ford Fiesta for car models), and 25 views per model.

The 25 views are shown in Table I, where each image has its azimuth labeled below it.

This produced 675 images of vehicles. In addition, some images with vehicles that had low contrast against the background were duplicated on monochrome or transparent backgrounds. With duplicates included, the total of raw vehicle images for training was 707.

326 negative samples were created from various city streets and desert scenes taken from the internet.

Once obtained, all samples were sheared and rotated to create further samples in order to simulate more data. This resulted in approximately 1000 samples per view. Table II below lists the complete training data used.

For testing data, an additional car model was simulated through the seen 25 views to create 25 raw images, and was further sheared and rotated to form a total of 90 images. For trucks, buses and negative samples, however, some images were simulated in unseen views from existing models and some were taken from the internet, due to time limitations. This combination of simulated and real-world images proved important: we note, in Section VI, that there is a difference in the classification results on simulated images as opposed to the results on a combination of images that are simulated or taken from the internet. This difference gives us an insight into the performance of our system on testing data that is similar to the training data versus data that is not.

In total, 90 test images were produced for each vehicle class, resulting in a training to testing ratio of 1: 0.3 in terms of raw images.

Table III lists the number of unseen samples of cars, buses, trucks, and negatives in the test dataset.

TABLE I. 25 VEHICLE VIEWS: ANGLES OF INCLINATIONS AND AZIMUTHS

<b>Inclination: 00</b>  000	 045	 090	 135	 180	 225	 270	 315
<b>Inclination: 30</b>  000	 045	 090	 135	 180	 225	 270	 315
<b>Inclination: 60</b>  000	 045	 090	 135	 180	 225	 270	 315
<b>Inclination: 90</b>  000							

TABLE II. TRAINING DATASET

	Class	Raw Images	Processed Totals
Positives	Car	243	25277
	Bus	239	24877
	Truck	225	23466
Negatives	City/Desert	326	979

TABLE III. TESTING DATASET

Cars	Buses	Trucks	Negatives
90	90	90	48

D. Method

The classification depends on extracting HoG features, which may produce feature vectors of different sizes depending on different HoG configurations, such as number of blocks that images were divided into, number of orientation bins, and so on. For calculation purposes, it was necessary to ensure that each feature vector extracted from an image was the same size. Hence, all training samples were cropped to an aspect ratio of 2:1 and were resized to 100x50 pixels. As suggested by Felzenszwalb and et al. [2], HoGs of 9 orientation bins, 8x8 pixels per cell with one cell per block were extracted. This generated a total of 648 features per image.

In order to build our classifiers, it was necessary to determine V, the optimal number of views to model. For this, a subset of the training data was used, with 2187 samples for cars, 2025 for trucks, 2151 for buses, and 978 negative samples.

A number of sets of views were proposed, shown in Table IV, and the classification accuracy on the 90-image test dataset for cars was recorded for each. The results, in Table V, showed that the selection of 15 views produced the highest accuracy.

The classification accuracy of trucks did not change, but the improvement for buses implied that 15 views was in fact a suitable choice. Hence, V was set to 15. Views were labeled from 0 to 15 in the order matching the angles and azimuths shown above in Section C: Data Used.

To ensure that this number improved accuracy across different types of vehicles, a subset of buses and trucks were also trained and classified on Sets 1 and 2.

Having concluded that the optimal number of views, V, was 15, three 15-view classifiers were trained, and one for each class of vehicle (car, bus, truck). This was for Approach 1, where separate classifiers were trained and then their combined scores compared. Each of these classifiers comprised 16 classes: 1 class to represent not-a-vehicle, and 15 to represent each of the different views of a vehicle.

For Approach 2, a single, 46-view classifier was trained. Again, one class was left for not-a-vehicle, and 45 classes were used for each of the different vehicles and their views. Table VI lists the results.

Classification accuracy refers to the classification of view (angle and azimuth). The Vehicle recognition accuracy refers to the classifier’s ability to recognize the class of the vehicle, (i.e. that it was a car). The confusion matrices are in Table VII.

These results showed a clear trend in the accuracy of the classifiers. The cars’ classifier performed best, followed by the buses’ classifier, while the trucks’ classifier had the poorest performance.

An analysis of the confusions revealed that the views of buses, to a certain extent, and trucks to a larger extent, were difficult to distinguish when the vehicles stood pointing to the left or to the right. Both classifiers had trouble in distinguishing the front of the big vehicle from its back.

The full test dataset was used to test Approach 1 (of separate classifiers) and compare it with Approach 2 (of a single classifier).

TABLE IV. CLASSIFICATION ACCURACY FOR DIFFERENT SETS OF VIEWS OF CARS

Views	Details	Accuracy
All 25 Views	None	91.1%
15 Views	0 degree inclination views 045, 090, 135 were collapsed into one view, “left”. Corresponding views for the “right” direction were collapsed. Additionally, no distinction was made between angles of inclinations 30 and 60 for views 45, 90, 135, 225, 270 and 315.	97.3%
13 Views (1)	0 degree inclination views 045, 090, 135 were collapsed into one view, “left”. Corresponding views for the “right” direction were collapsed.	93.3%
13 Views (2)	No distinction was made in a single view between angles of inclination 30 and 60. But for view 045, angles of inclination at 30 and 60 were collapsed into one view, and so on.	96.4%
11 Views	Views 045, 090, 135 were collapsed into one view, “left” for each angle of inclination (0, 30 and 60). Corresponding views for the “right” direction were collapsed.	95.6%

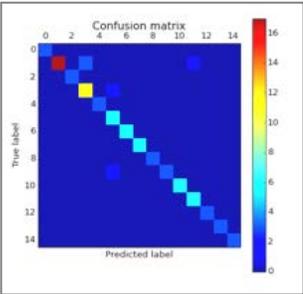
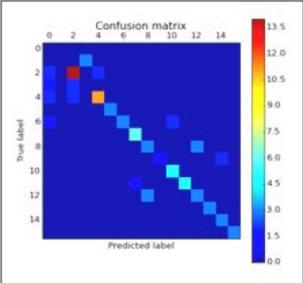
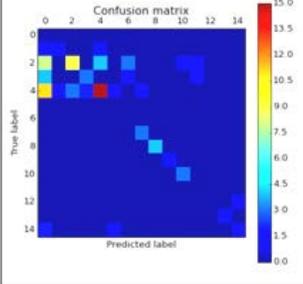
TABLE V. CLASSIFICATION ACCURACY FOR DIFFERENT SETS OF VIEWS OF BUSES AND TRUCKS

	Buses	Trucks
25 views	68.8%	80.3%
15 views	82.7%	80.3%

TABLE VI. PERCENTAGE ACCURACY OF INDIVIDUAL, 15-VIEW CLASSIFIERS

	View Classification Accuracy	Vehicle Recognition Accuracy
Cars classifier	92.2	100.0
Buses classifier	71.1	93.3
Trucks classifier	46.7	71.1

TABLE VII. CONFUSION MATRICES OF INDIVIDUAL, 15-VIEW

	Cars model (on cars' data)
	Buses model (on buses' data)
	Trucks model (on trucks' data)

For Approach 1, each classifier was given a vehicle image for which it generated confidence scores per view. Min-max normalization was then used to allow these scores to be compared across classifiers, and the highest score was selected to represent the final chosen class. The accuracy of this combined model was then compared with that of a single, 46-class classifier.

Tables VIII and IX compares the results of each approach, followed by the confusion matrix of the 46-class classifier in Fig. 2.

TABLE VIII. VEHICLE RECONIGNITION ACCURACY

	Cars	Buses	Trucks
<b>46-class model</b>	93.3	71.1	40.0
<b>Combined models</b>	85.6	42.2	42.2

TABLE IX. VIEW CLASSIFICATION ACCURACY. N-V REPRESENTS THE CLASS NOT-A-VEHICLE

	Cars	Buses	Trucks	N-V	Overall
<b>46-class model</b>	91.1	55.6	24.4	64.4	58.2
<b>Combined models</b>	81.1	34.4	66.7	68.8	51.6

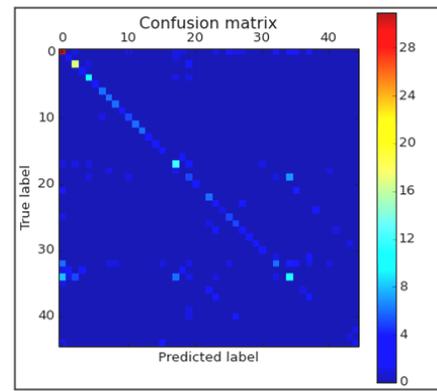


Fig. 2. 46-Class Model (on Full Test Data).

The accuracy drop of the classifiers when dealing with big vehicles was not only because of the trouble in distinguishing the front of a truck or bus from its back, but it was found that 33% of the errors in identifying trucks was caused by a confusion with identifying trucks as buses, and that 44% of the errors in identifying buses was caused by the converse. Examples of the confusions are shown in Fig. 3 and 4.

The greatest number of common confusions for both buses and trucks were in distinguishing whether they were facing towards the left or the right, i.e. at azimuths of 90 or 270.



Fig. 3. Confusion between Trucks in Similar Positions based on Difficulty in Distinguishing the Front of the Vehicle from the Back.



Fig. 4. Confusion between Trucks and Buses in Similar Positions.

Given the above results, buses and trucks would best be compressed into one class, Big Vehicles. Therefore the training data for buses and trucks was re-processed to produce the data displayed in Table X. The individual Cars' classifier retained 15 views, which were labeled from 1 to 15, with the 0 label used to refer to not-a-vehicle.

However, for the big vehicles, the views of vehicles standing facing left and right were compressed into one view. Therefore the Big Vehicles classifier was trained on 14 views, and one class for negatives.

For Approach 2, the single classifier was trained on 29 views. In this classifier, view 0 represented not-a-vehicle; views 1 to 15 represented the different views of a car, starting from a zero-angle of inclination and zero-azimuth; likewise, views 16 to 29 represented the views of a big vehicle. All the classifiers were tested on the same test data as before. The results are shown in Section VI.

TABLE X. UPDATED TRAINING SET

	Class	Raw Images	Processed Totals
<i>Positives</i>	Car	243	25277
	Big Vehicles	232	24177
<i>Negatives</i>	City/Desert	326	979

E. Limitations

A limitation of the method chosen is based on the selection of HoG features, which are dependent on image dimensions. Therefore, the results are most reliable when the testing data consists of vehicles of a similar size and position relative the center as those present in the training data.

A strength of the system is the use of GentleBoost as opposed to the more oft-used AdaBoost. This is because GentleBoost is not as easily affected by outliers.

VI. RESULTS AND DISCUSSION

The results of our system were compared against a baseline built using AdaBoost, in particular the SAMME.R version [27]. AdaBoost was chosen as a suitable comparison with our method because of its popularity in the object and vehicle detection fields [20]. The SAMME.R version is a real number-based multiclass classifier that, like our choice of GentleBoost.C, is based on cascaded boosting and does not break the classification problem into binary decisions. SAMME.R also generates sound confidence scores for each class during classification, which was useful when comparing the main system against Approach 1.

A. Individual Vehicle Models: Cars, Big Vehicles

Table XI compares the view classification and vehicle recognition accuracy of the individual car and big-vehicle models, which were trained on images of cars and big vehicles respectively. Except in the vehicle recognition of big vehicles, the GentleBoost version has a higher accuracy than the Adaboost baseline.

Tables XII to XIV compare the vehicle recognition and view classification accuracies of Approach 1 (combined classifiers) and Approach 2 (single classifier) respectively. Once again, the Gentleboost system outperforms the baseline. While the performance of the two approaches is somewhat similar with respect to cars, the single classifier was accurate 72.2% of the time and outperformed the first approach significantly in the case of big vehicles. This difference may be attributed to the difference between testing data for big vehicles and that for cars. Recall that part of the big vehicles' testing data was taken from photographs on the internet, unlike the cars' data, which was generated entirely using a 3D simulator. The results suggest that the single classifier is well-suited to situations where testing data includes samples that are significantly different from those in the training data, in turn suggesting a wider application than what the combined-classifiers model is capable of. Tables XIII and XIV show that all classifiers performed less accurately at View Classification.

The GentleBoost single classifier of Approach 2 performs best on cars, and the baseline system, albeit with lower numbers, had a similar trend.

The Gentleboost combined classifiers of Approach 1 performed best on cars again, and lowest on big vehicles. However, the combined baseline models do not maintain the same trend as the Gentleboost classifiers.

Table XV presents the precision of recall of both two approaches. Approach 2 (the single classifier approach) yields 0.92, an improvement over Approach 1.

Overall, Approach 2 using Gentleboost outperformed other classifiers in all experiments.

TABLE XI. PERFORMANCE OF INDIVIDUAL VEHICLE MODELS (%)

	Vehicle classification		Vehicle Recognition	
	GentleBoost	Baseline	GentleBoost	Baseline
<i>Cars</i>	<b>91.1</b>	46.7	<b>98.9</b>	96.7
<i>Big V</i>	<b>72.2</b>	58.3	89.4	<b>94.4</b>

TABLE XII. VEHICLE RECOGNITION ACCURACY: SINGLE VERSUS COMBINED MODELS (%)

	Cars		Big Vehicles	
	GentleBoost	Baseline	GentleBoost	Baseline
<i>29-class model</i>	<b>95.6</b>	73.3	<b>72.2</b>	48.9
<i>Combined models</i>	<b>91.1</b>	41.1	<b>55.0</b>	46.1

TABLE XIII. VIEW CLASSIFICATION ACCURACY (%): SINGLE 29-CLASS MODEL

	GentleBoost	Baseline
Cars	<b>91.1</b>	44.4
Big Vehicles	<b>61.1</b>	13.3
N-V	<b>75.0</b>	29.2
Overall	<b>71.7</b>	24.5

TABLE XIV. VIEW CLASSIFICATION ACCURACY (%): COMBINED MODELS

	GentleBoost	Baseline
Cars	<b>85.6</b>	21.1
Big Vehicles	<b>48.3</b>	26.7
N-V	<b>70.8</b>	83.3
Overall	<b>62.3</b>	22.3

TABLE XV. PRECISION/RECALL

	Precision		Recall	
	GentleBoost	Baseline	GentleBoost	Baseline
<i>29-class model</i>	<b>0.96</b>	0.89	<b>0.91</b>	0.85
<i>Combined models</i>	<b>0.96</b>	0.86	0.93	<b>0.99</b>

However, the big vehicles did not fare as well. Big vehicles were likely misclassified when seen in the initial views listed in Table I, starting with an inclination angle of 0 and azimuth of 000. Over 10% of the errors, it was found, were confusions between the side views of cars versus of big vehicles, and likewise with front views. This suggests a trade-off between accurate classification of views and of vehicles.

Although many systems explore vehicle detection in spite of occlusions, or from aerial views, and so on, at the time of writing, we do not know of other classification systems which recognize vehicles irrespective of view as well as vehicle class. No immediate comparisons could be made with the current state-of-the-art, since current systems often use datasets such as KITTI, Caltech, Pascal, or Toyota, which lack a comprehensive range of views.

## VII. CONCLUSION

This paper explored the development of a vehicle classifier that can distinguish vehicles regardless of class or view. The classifier was built using a multiclass GentleBoost boosting algorithm trained on 648-length arrays of image HoG features.

While 25 different views of vehicles were initially suggested, so many views were found unnecessary for accurate classification, and in fact likely to reduce accuracy. Therefore an optimal choice of 14-15 views was selected for training.

Another system was built with the same data and choice of views, but with independent classifiers that focused on each type of vehicle. The classifiers' votes were combined to choose the most likely class and view of a test vehicle.

The results showed a single classifier trained over many classes performing significantly better than the results from a combination of individual classifiers trained over subsets of all the training data. The single classifier's performance also showed that this is a better choice in the event that testing data consists of environments and views that are very different from that of the training data. This is because the testing data for big vehicles was different from its training data, and the improvement of performance of the single classifier over the combined classifiers was most pronounced over big vehicles.

The results also showed that large vehicles are more likely to be confused amongst each other than are cars, probably due to the dilution of dissimilar components by similar components.

The experiments in this paper conclude that, without using complex 3D models, a simple multiclass classifier can detect with high precision, various types of vehicles across different environments, and different views of the vehicle, including the top, aerial view.

## ACKNOWLEDGMENT

Thanks to Aurelian Tutuianu for his help in the GentleBoost.C implementation.

## REFERENCES

[1] Savarese, S., Li Fei-Fei, "3d generic object categorization, localization and pose estimation", *IEEE International Conference on Computer Vision*, 2007.

[2] Felzenszwalb, P. F., Girshick, R. B., McAllester, D., Ramanan, Deva, "Object Detection with Discriminatively Trained Part-Based Models", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2010.

[3] Clady, X, Negri, P., Milgram, M. and Poulencard, R., "Multi-class Vehicle Type Recognition System", *Proceedings of 3rd IAPR workshop on Artificial Neural Networks in Pattern Recognition*, 2008.

[4] Razavi, N., Gall, J., Van Gool, L., "Scalable Multi-class Object Detection", *Proceedings of the 2011 IEEE Conference on Computer Vision and Pattern Recognition*, 2011.

[5] Viola, P., Jones, M. J., "Robust Real-time Object Detection", *International Journal of Computer Vision*, 2001.

[6] Schapire, R. E., "A Brief Introduction to Boosting", *Proceedings of the 16th International Joint Conference on Artificial Intelligence*, Vol. 2, 1999.

[7] Hastie T., Tibshirani R., Friedman J, *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*, 2nd ed. Springer, New York, 2009.

[8] Jazayeri, A, Cai, H., Zheng, J. Y., Tuceryan, M., "Vehicle detection and tracking in car video based on motion model", *IEEE Transactions On Intelligent Transportation Systems*, Vol. 12, No. 2., 2011.

[9] Alonso, J. D., Vidal, E. R., Rotter, A., Muhlenberg, M., "Lane change decision aid system based on motion-driven vehicle tracking", *IEEE Transactions On Vehicular Technology*, Vol. 57, No. 5, 2008.

[10] Thuy Thi Nguyen, Grabner, H., Bischof, H., Gruber, B., "On-line Boosting for Car Detection from Aerial Images", *Proceedings of IEEE International Conference on Research, Innovation and Vision for the Future*, 2007.

[11] Behley, J., Steinhage, V., Cremers, A. B.: "Laser-based Segment Classification Using a Mixture of Bag-of-Words", *International Conference on Intelligent Robots and Systems*, 2013.

[12] Ye Li, Bin Tian, Bo Li, Gang Xiong, Fenghua Zhu, Kunfeng Wang, "Vehicle detection with a part-based model for complex traffic conditions", *IEEE International Conference on Vehicular Electronics and Safety*, 2013.

[13] Zehang Sun, George Bebis, Ronald Miller, "Monocular precrash vehicle detection: Features and classifiers", *IEEE Transactions On Image Processing*, Vol. 15, No. 7, 2006.

[14] Bin-Feng Lin et al, "Integrating appearance and edge features for sedan vehicle detection in the blind-spot area", *IEEE Transactions on Intelligent Transportation Systems*, 2012.

[15] Chi-Chen Raxle Wang, Lien, J.-J., "Automatic vehicle detection using local features: A statistical approach", *IEEE Transactions on Intelligent Transportation Systems*, 2008.

[16] Chan, Y.-M., Huang, S., Fu, L., Hsiao, P., Lo, M.-F.: "Vehicle detection and tracking under various lighting conditions using a particle filter", *Intelligent Transport Systems, IET*, Vol. 6, Issue. 1, 2012.

[17] Wen-Chung Chang, Chih-Wei Cho: "Online Boosting for Vehicle Detection", *IEEE Transactions ON Systems, Man, and Cybernetics—Part B: Cybernetics*, Vol. 40, No. 3, 2010.

[18] Thuy Thi Nguyen, Grabner, H., Bischof, H., Gruber, B., "On-line Boosting for Car Detection from Aerial Images", *IEEE International Conference on Research, Innovation and Vision for the Future*, 2007.

[19] Sivaraman, S., Trivedi, M.M., "A general active-learning framework for on-road vehicle recognition and tracking", *IEEE Transactions on Intelligent Transportation Systems*, 2010.

[20] Sivaraman, S., Trivedi, M. M., "Looking at Vehicles on the Road: A Survey of Vision-Based Vehicle Detection, Tracking, and Behavior Analysis", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 14, Issue 4, pp 1773 – 1795, 2013.

[21] Torralba, A., Murphy, K. P., Freeman, W. T.: "Sharing visual features for multiclass and multiview object detection", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, Issue 5, 2007.

[22] Shalev-Shwartz, S, Wexler, Y., Shashua, A.: "Efficient Multiclass Learning with Feature Sharing", *Advances in Neural Information Processing Systems*, 2011.

[23] Friedman, J., Hastie, T., Tibshirani, R., "Additive Logistic Regression: A statistical view of boosting", *The Annals of Statistics*, Vol. 28, No. 2, pp 337-407, 2000.

- [24] Rifkin, R., "Multiclass Classification", <http://www.mit.edu/~9.520/spring09/Classes/multiclass.pdf>, 2008.
- [25] Dietterich, T. G., Bakiri, G., "Solving multiclass learning problems via Error Correcting Output Codes", *Journal of Artificial Intelligence Research*, 1995.
- [26] Schapire, R., Singer, Y., "Improved Boosting algorithms using confidence-rated predictions", *Machine Learning*, Vol. 37, Issue 3, pp 297-336, 1999.
- [27] Zhu, J., Zou, H., Rosset, S., Hastie, T., "Multi-class AdaBoost", *Statistics and Its Interface*, Vol. 2, No. 3, 2009.
- [28] Huang, J., Ertekin, S., Song, Y., Zha, H., Giles, C. L., "Efficient Multiclass Boosting Classification with Active Learning", *Seventh SIAM International Conference*, 2007.
- [29] Zhang, Z., Chen, C., Dai, G., Li, W.-J., Yeung, D.-Y., "Multicategory Large Margin Classification Methods: Hinge Losses vs. Coherence Functions", *Artificial Intelligence*, Vol. 215, pp 55-78, 2014.
- [30] Dalal, N., Triggs, B., "Histograms of oriented gradients for human detection", *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2005.
- [31] Zhang, Z., Liu, D., Dai, G., Jordan, M. I., "Coherence Functions with Applications in Large-Margin Classification Methods", *Journal of Machine Learning Research*, 2012.
- [32] Jones, M., Viola, P., "Fast Multi-view Face Detection", *Tech. Rep. TR2003-96*, Mitsubishi Electric Research Laboratories, 2003.
- [33] Zhang, Y. et al, "Research on visual vehicle detection and tracking based on deep learning", *IOP Conf. Ser.: Mater. Sci. Eng.*, 2020.
- [34] J. Chen and L. Dai, "Research on Vehicle Detection and Tracking Algorithm for Intelligent Driving," *2019 International Conference on Smart Grid and Electrical Automation (ICSGEA)*, 2019.

# Arabic Sign Language Recognition using Faster R-CNN

Rahaf Abdulaziz Alawwad<sup>1</sup>, Ouiem Bchir<sup>2</sup>, Mohamed Maher Ben Ismail<sup>3</sup>

College of Computer and Information Sciences, King Saud University, Riyadh, KSA

**Abstract**—Deafness does not restrict its negative effect on the person’s hearing, but rather on all aspect of their daily life. Moreover, hearing people aggravated the issue through their reluctance to learn sign language. This resulted in a constant need for human translators to assist deaf person which represents a real obstacle for their social life. Therefore, automatic sign language translation emerged as an urgent need for the community. The availability and the widespread use of mobile phones equipped with digital cameras promoted the design of image-based Arabic Sign Language (ArSL) recognition systems. In this work, we introduce a new ArSL recognition system that is able to localize and recognize the alphabet of the Arabic sign language using a Faster Region-based Convolutional Neural Network (R-CNN). Specifically, faster R-CNN is designed to extract and map the image features, and learn the position of the hand in a given image. Additionally, the proposed approach alleviates both challenges; the choice of the relevant features used to encode the sign visual descriptors, and the segmentation task intended to determine the hand region. For the implementation and the assessment of the proposed Faster R-CNN based sign recognition system, we exploited VGG-16 and ResNet-18 models, and we collected a real ArSL image dataset. The proposed approach yielded 93% accuracy and confirmed the robustness of the proposed model against drastic background variations in the captured scenes.

**Keywords**—Arabic sign language recognition; supervised learning; deep learning; faster region based convolutional neural network

## I. INTRODUCTION

Gesturing is one of the earliest forms of human communication. Nowadays, Deaf and Hard of Hearing (DHH) people are the predominant users of the officially recognized sign language which consists of alphabets, numbers, and words typically used to communicate within and outside their community. Typically, a sign language consists of; (i) manual components, and (ii) non-manual component. Specifically, the configuration, the position, and the movement of the hands form the manual components. On the other hand, the facial expression and the body movement compose the non-manual components. Such sign language is perceived as a non-verbal communication way that is mainly intended to ease the communication for the DHH persons. However, the communication between a Deaf person and a hearing individual remains an open challenge for the community. In fact, approximately 466 million people who suffer from a moderate to profound hearing loss struggle with communication daily. In other words, deaf people cannot be considered as a linguistic minority which the language can be neglected.

A sign language includes designated hand gestures for each letter of the alphabet. These gestures are used to spell people names, places, and other words without a predefined sign. Besides, it is a common occurrence for the sign formation to resemble the shape of the written letter. Although the hand gestures exhibit some similarities due to the limited number of possible hand gestures, sign language is not universal. Specifically, there are 144 sign languages around the world [44]. They vary based on the region/country rather than the language itself. For instance, The Arabic Sign Language (ArSL) includes 30 identical alphabet signs. Fig. 1 shows the sign corresponding to the letter “V” in the British and American sign languages respectively.

Despite the variations noticed on the same sign gesture when performed by signers from different origins and/or having different background, the discrepancy remains minor and affects few letters only. Particularly, the “Ra” and “H” letters can be expressed either dynamically or statically depending on the signer preference. Also, the letter “Jeem” which is represented using a curved palm, can be performed using either a sharp or a soft palm. In order to overcome such discrepancies, a considerable effort was made to unify ArSL and come up with a standard language that can be understood and used by all Arab DHH [1]. Nevertheless, fingerspelling can still be used as a common and standard way of communication between Deaf Arabs.

The semantic meaning of the gesture is a main property of the ArSL. For example, the pointing finger in the three letters “Ba”, “Ta”, and “Tha” represents the number of dots that the letter has. Moreover, ArSL has the specificity of having similarities within the sign language alphabet. For instance, as depicted in Fig. 2, the letter pairs “T’a” and “Th’a”, “Ayn” and “Ghayn”, and “Dal” and “Thal” exhibit highly similar visual properties. This makes the recognition task even more challenging for these letters.

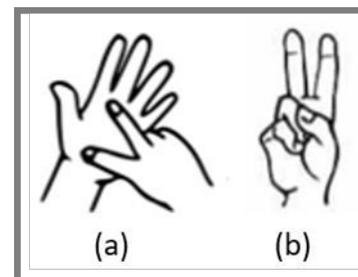


Fig. 1. Sign of Letter “V” (a) British Sign Language, (b) American Sign Language.



Fig. 2. Unified ArSL Alphabet.

Deafness can be a social barrier especially due to the hearing people's reluctance to learn a new language exclusively mastered and used by a minority. In fact, this unwillingness takes deaf persons to a state of isolation and detachment. However, the recent technological advances have promoted the development of sign language recognition systems [2-4] for different sign languages, such as Chinese Sign Language, British Sign Language, American Sign Language. One should mention that no such contributions have been achieved for the uniform Arabic Sign Language (ArSL) recognition due to the discrepancies between speakers from different Arab countries [5]. Despite this inconsistency at the language level, the hand gestures of the ArSL letters and numbers are identical for all DHH Arabs.

ArSL had its share of sensor-based systems, which the usability was mainly affected by the mandatory use of gadgets such as gloves. In other words, such solutions are intrusive and suffer from a lack of usability. Lately, image-based systems have alleviated this problem and provided a non-cumbersome solution where signs are translated using smart device cameras. Ideally, a real-time Arabic sign language recognition system would assist DHH persons and reduce their constant dependence on human translators. In particular, it would help them interact and socialize better with hearing persons. Typically, image-based solutions rely on image processing to segment the hand region, and use machine learning techniques to map the captured gestures into the pre-defined letter classes. Specifically, the image is conveyed as input, and the hand is then segmented to separate it from the background. Next, the obtained object is provided as input to the machine learning model. Note that to segment the hand, appropriate features need to be extracted from the image. These features are intended to ease the discrimination between the hand and its background. Similarly, in order to recognize the gesture, other features are used to differentiate between the different gestures classes. The choice of the appropriate features is not straightforward. It constitutes an issue for these image-based systems [4]. Moreover, the overall system performance depends on the accuracy of the segmentation task

which consists of isolating the hand region from the remaining image content. In particular, the high variability of the image visual properties, as well as the similarity between the hand and the face skin color, make the segmentation even more acute.

In order to choose the relevant visual descriptors and enhance the segmentation accuracy, we propose to design and implement a novel Arabic Sign Language recognition system based on the Faster Region Convolutional neural network (R-CNN). Actually, the Convolutional Neural Network (CNN) [6] is a deep learning based approach classically used for image classification [7]. The considerable learning ability of CNN is attributed to the multi-stage and hierarchical features extraction achieved by the network. The proposed CNN based approach can be perceived as an alternative to the manual feature extraction and selection needed for the segmentation and the sign recognition tasks. Furthermore, we exploit Faster Region Convolutional Neural Network (R-CNN) which performs both real-time object detection and classification to address the ArSL recognition problem.

## II. RELATED WORKS

Image-based Arabic Sign Language recognition systems have tackled critical technical challenges such as the hand segmentation and the choice of the visual descriptors. On the other hand, issues such as the visual similarity between the signs of some letters like "Ra" and "Za" are specific to the Arabic sign language. Several approaches have been reported in the literature to tackle the Arabic sign language recognition [8]. Some of them extract specific features from the image and feed them into a machine learning algorithm. In the following, we refer to such solutions as conventional approaches as opposed to the latest ones based on deep learning.

The Arabic Sign language recognition system introduced in [9] converts the input images to the YCbCr space in order to detect the hands and the face using the skin profile. A morphological operation [12] is then performed on the converted image to fill the gaps in the obtained regions. To extract features that are able to distinguish between similar signs, the Prewitt operator [10] was used to encode the edges of the hand region. Next, the Principle Component Analysis (PCA) [11] was deployed on the extracted features to reduce the dimensionality and determine the final feature. Besides, the classification task was performed using the K-Nearest Neighbor (KNN) [13] which yielded an accuracy of 97%. In [14], an ArSL finger spelling recognition system which relies on the SVM classifier [15] was proposed. The sign image was captured using a sensor that captures the image intensity and depth. The closest object to the sensor was assumed to be the signer. Another skin segmentation step is added for a better performance under complex background situations. Two features are then extracted from the segmented image. Namely, the Principle Component Analysis (PCA) [11], and the Histogram of Oriented Gradients (HOG) [16] were associated with the PCA to encode the visual properties of the image regions. The classification task was achieved using a multiclass Support Vector Machine (SVM) [15]. This yielded an outperformance of HOG-PCA due to its ability to discriminate between similar signs in addition to its robustness to local illumination

variation. Specifically, the accuracy reached 99.2% while PCA's performance attained 96.38%. In [17], the sign image is converted into the YCbCr color space for a more accurate hand segmentation. Besides, the contrast, the correlation, the energy, and the Local Homogeneity are computed from the Grey Level Co-occurrence Matrix (GLCM) [16]. The extracted feature is then fed into the Multiple Layer Perceptron [18] for skin detection. For the gesture recognition, both the outer and the inner edges are detected, and the Tchebichef [16] and Hue moments [19] are extracted. In addition, the computation of the relative area and the minimum and maximum relative distances were measured. The resulting features are then conveyed to an SVM [15] and a KNN [13] classifiers to map the input into the pre-defined classes. The proposed system was evaluated using our two ArSL datasets that include the 30 sign gestures. The first dataset was collected by 24 signers and a solid background was used for all captured scenes, while the second one which exhibits complex background was collected by 8 signers. The obtained results proved that KNN outperforms SVM with 94.67% accuracy for the first dataset and 89.35% accuracy for the second one. Similarly, the researchers in [20] compared two finger spelling recognition systems. The first one relies on KNN [13] as classifier while the second system uses the Multiple Layer Perceptron (MLP) [18] to categorize the sign images. The captured images include solid background. The signs were grouped into three categories based on the wrist orientation. One should mention that the matching operation of each sign was performed only within its allocated group. The authors introduced an edge feature to calculate the pairwise distances between the wrist and fifty equidistant contour points. The nearest neighbor and MLP were used for classification resulting in an accuracy of 91.3% and 83.7% respectively. Whereas the researchers in [22] proposed an ArSL recognition system based on the Scale-Invariant Features Transform (SIFT) [21]. Their algorithm can be summarized as: (1) convolve the image with Gaussian filter of different widths to create the difference of Gaussian function pyramid between filtered images, (2) Find the extrema in the Gaussian pyramids by comparing each point with its 26 neighbors, (3) Eliminate extrema key points that were suspected to be sensitive to noise or were located on an edge, (4) Assign orientation by forming a histogram from the gradient orientations of sample points within a region around the extrema points, and finally, (5) Create a descriptor for the local image region that is highly distinctive at each candidate. The dimensionality of obtained feature vector is then reduced using the Linear Discriminant Analysis (LDA) [23]. The reduced feature vector is fed to three different classifiers. Namely, the Support Vector Machine (SVM) [15], the one nearest neighbor, and the K-Nearest Neighbor (KNN) [13] were used to classify the input vectors. The results showed that SVM outperforms KNN with an accuracy of 98.9%.

In [24], an Adaptive Neuro-fuzzy Inference System (ANFIS) [25] intended to recognize the 30 alphabets of Arabic sign language was outlined. The input image was filtered using a median filter in order to reduce the noise and enhance the image for the segmentation. The latter is done using an iterative thresholding algorithm [16]. The architecture of ANFIS consists of five layers where the gesture is provided as input and the output layer indicates to the degree to what the

input satisfies the rule. The overall recognition system confirmed its robustness and invariance to size, position, and direction of the input sign. However, similar gestures such as "Dal" and "Thal" were misclassified which resulted in 93.5% accuracy. Lately, the authors in [26] used two different neural networks and four visual descriptors to address the sign language recognition problem. In particular, they used the 30 letters ArSL dataset in [24] in which all images have a solid background, and the hand is the only object within the image. As a preprocessing step, the image was filtered with a Canny edge detector [27]. Specifically, the four visual descriptors used in their work were the Hu Moments [19], the Local Binary Pattern [28], the Zernike Moments [29], and the Generic Fourier Descriptor [16]. These features were provided as input to two different neural networks: MLP and Probabilistic Neural Network (PNN) [30]. The descriptors were first tested individually, then various combinations were evaluated for three different datasets. The Local Binary Pattern (LBP) descriptor yielded 90.41% accuracy when associated with PNN classifier, and it attained 86.46% accuracy when combined with MLP. Similarly, in [31], the researchers considered five features to assess their ArSL recognition system performance. Namely, they compared the Histogram of Oriented Gradients (HOG), the Edge Histogram Descriptor (EHD), the Local Binary Pattern (LBP), the Gray-Level Co-occurrence Matrix (GLCM), and the Discrete Wavelet Texture Descriptor (DWT) [16]. The descriptors were extracted from the ArSL alphabet images and classified using a One versus All SVM classifier. Their dataset by 30 was collected by 30 different signers. It includes 30 static Arabic letters with a solid background captured using a phone camera and. The obtained experiments showed that the HOG descriptor overtakes the other descriptors with an accuracy of 63.5%.

In addition to the conventional approaches, existing Arabic sign language recognition systems rely on deep learning paradigms which the ability to learn the most relevant features was confirmed in a wide range of applications. In particular, the authors in [32] designed an ArSL alphabet and digits recognition system using convolutional neural networks. Their network inspired by LeNet-5 [6] is composed of two convolutional and Leaky ReLU layers, two Max pooling layer to reduce the image size, one 75% dropout layer to reduce overfitting, and three fully connected layers for classification. The network was trained using Adam Optimizer with a learning rate of 0.03. Different ratios of training data were tested and 80% gave the best results. The evaluation was made using a collection of 5839 images for the 28 letters of ArSL and 2030 images of the decimal digits. All images include a solid background which allowed the researchers to omit the segmentation step. The experiments results showed that the proposed system outperforms other systems, and attained an accuracy of 90.02%. Similarly, a deep Recurrent Neural Network (RNN) [33] was adopted in [34] to address the Arabic sign language recognition challenge. A collection of 30 ArSL alphabets images was collected by two signers with 15 repetitions. The signers had to wear a colored glove to allow the system capture the signs. The RGB images were converted into the Hue-Saturation-intensity Value (HSV) space [16]. Then, a Fuzzy C-mean (FCM) clustering algorithm [38] was deployed to segment the different fingers. Thirty features were extracted

from the fingertips positions and orientation. In addition, four neural networks were investigated, namely, the feedforward neural network [35], the Elman neural network [36], the Jordan neural network [37], and the fully connected Recurrent Neural Network (RNN) [33]. RNN outperformed the other networks with an accuracy of 95.1%, although, the letter “Ghayn” was highly misclassified.

In [39], a deep learning recognition architecture called PCANet was introduced. Taking as input the depth image, the hand is segmented by assuming it is the closest object to the sensor. Both the RGB component and the depth component were fed individually to two different PCANet networks to automatically extract the features. PCA [11] was also deployed at the convolutional layer to find the orthogonal filters from the local patches of the input images. The learned feature vectors were next conveyed to the SVM classifier [15]. The experiments showed that the depth component achieved a better performance than the intensity component with an accuracy of 99.5%. This can be attributed to the fact that the RGB component is affected by the lighting variations and cluttered backgrounds.

The conventional and deep learning based Arabic Sign language recognition approaches reported above show that the hand segmentation is typically the first step of any sign language recognition system. The hand segmentation is a challenging task due to the difficulty to adapt to all images which exhibit highly variant levels of illumination, background complexity, skin tones and shapes. ArSL recognition systems that have been reported in the literature tackled the problem using different ways. Some works [20][22][31][26] bypassed the segmentation stage by restricting the input images to have a uniform background resulting in easier extraction of hand shape. Other approaches opted to use external equipments to aid correct capturing of the hand gesture, such as in [14][39], a Kinect sensor that captures the intensity and the depth of the images was employed. In this case, the hand is segmented as the nearest object to the camera. Similarly, in [34] a colored glove indicating the five fingertips and the wrist was used in order to recognize the signer gesture. However, the approaches in [34][14][39] imposed an unrealistic restriction to sign language recognition systems due to the inconvenience of using expensive sensors or colored gloves. On the other hand, others proposed segmentation techniques relying on skin pixel's detection as in [9][17][22]. The skin segmentation alleviates the previously mentioned problems by detecting the hand from an RGB image which does not have a uniform background without the use of any accessory or expensive sensors.

Determining the appropriate visual descriptors allows the segregation between the hand pixels and the background pixels remains an open problem. Another problem faced by ArSL recognition systems is the unavailability of large benchmark data sets with non-uniform backgrounds. In fact, small datasets such as those in [9][20] would lead to unintentional overfitting during the model learning phase. In other words, evaluating the model using small datasets may not reflect the

real recognition performance. Additionally, the choice of the most suitable feature to describe the gesture can be achieved using deep learning as reported in [34][39][32]. However, to the best of our knowledge, only three works adopted deep learning to overcome the ArSL recognition challenge. All of them bypass the segmentation task by either using solid background, accessories, or depth sensors.

In this research, we propose a novel Faster R-CNN based recognition of the thirty letters of the Arabic Sign Language. The trained network is intended to segment the hand and recognize the sign gestures.

### III. PROPOSED METHOD

In this research, we aim to recognize the hand gestures of the Arabic sign language using two-dimensional images, and translate them into text. The proposed system is intended to support non-hearing people in their communication with others either they master or not the ArSL language. This would lessen the social hardship this community withstands daily. Moreover, the proposed system is not a bothersome for the user since it does not require any accessory or sophisticated sensors or cameras. Specifically, we propose a faster R-CNN based approach to localize and classify the thirty letters of the Arabic sign language. In particular, a deep learning network that is designed as a typical CNN architecture is utilized as a feature extractor. The rationale behind the choice of the proposed Region CNN (R-CNN) is its noticeable impact on the object recognition field. In fact, the region proposals generation using an intelligent selective search yields to relax the need for a separate image segmentation stage. Nevertheless, some limitations were noticeable concerning the efficiency of the method, more specifically, the large number of proposals that are conveyed to the network represents a major drawback. Therefore, the more recent version fast R-CNN [40] was introduced to enhance the performance by integrating a Region of Interest (ROI) pooling layer and thus reducing the processing time required by the network. Despite this enhancement, the main issue still persists, laying within the time-consuming selective search used for proposal generation. Consequently, the latest incarnation of region CNN, namely the faster RCNN [40], was considered adapted in this research to exploit the Region Proposal Network (RPN) originally designed for real-time object recognition as depicted in Fig. 3.

The architecture of the proposed network is illustrated in Fig. 4. As it can be seen, the CNN network is utilized as feature extractor through the processing of the input image using the convolutional layers designed to produce a feature map. The Region Proposal Network (RPN) slides a window over the obtained feature maps while calculating the objectness score and the bounding box coordinates for each object (gesture) in order to produce several candidate object/regions. Lastly, given these candidate regions, the sign gesture classification task is performed by the detection network which is composed of fully connected layers.

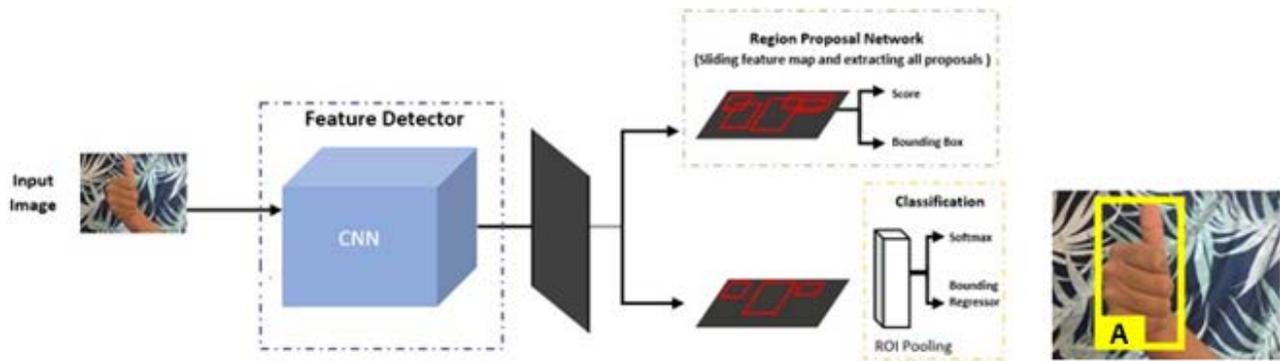


Fig. 3. The Network Architecture of the Proposed Approach.

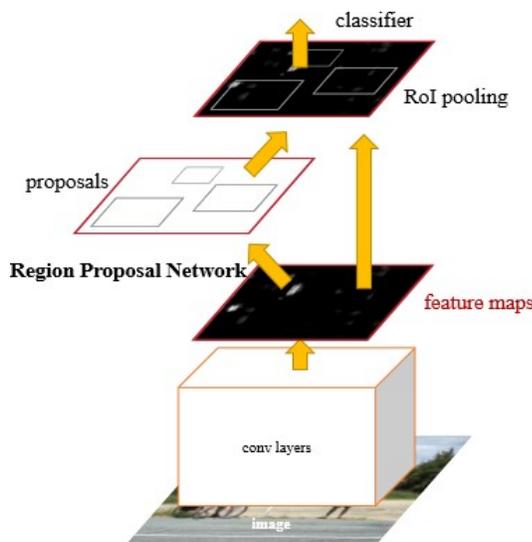


Fig. 4. Faster R-CNN Architecture.

The Region Proposal Network (RPN) in Fig. 3 can be perceived as a small pre-trained network that consists of one main convolutional layer with a  $3 \times 3$  receptive field. It receives the feature map as input and outputs a specified number of potential region proposals. This network requires a hyperparameter  $k$  which indicates the number of rectangle boxes (anchors) of diverse ratios and scales, thereby, addressing the issue of different possible sizes of an object within the image. The initial state for each anchor is negative and it is only set to positive if the Intersect over Union (IoU) with respect to the ground truth is larger than a specified threshold. Furthermore, to contain the number of generated proposals, a Non-Maximum Suppression (NMS) is employed to remove proposals that overlap with other high score proposals. The top regions obtained using NMS are fed into the ROI layer where each region proposal includes the object scores, indicating whether the anchor containing an object, and four coordinates for the bounding box centroid as  $[x, y]$  and the width and height of the bounding box.

In this work, we investigate two architectures; The first one associates the deep VGG-16 model [41] to the faster R-CNN [40], while the second architecture relies on the Res-Net architecture [42] which proved to have a faster and more accurate recognition in the ImageNet contest. These two ar-

chitectures along with the pre-trained models are meant to be trained using our own ArSL gesture images. For this purpose, the top dense layer is replaced by a  $1 \times 1 \times 31$  layer that indicates the 30 classes of ArSL letters and one class for non-gesture objects.

For the training phase, the RGB image collection of the sign gestures are resized to  $224 \times 224$  and fed to the network. The weights of the original Faster R-CNN are the starting point for our ArSL recognition network. However, the fully connected layers including the Softmax classifier and the regression box estimator are initialized from two zero-mean Gaussian distributions with a standard deviation of and 0.001 respectively. The captured images are conveyed to the feature extraction network to generate the feature maps. These maps are fed to the Region Proposal Network (RPN) in order to generate potential hand gestures. The output of the RPN contains the coordinates of the bounding box and a score indicating the existence or absence of a hand. The proposals generated by RPN are conveyed to the ROI pooling layer alongside the feature map generated by the feature extraction network. The scaled feature maps, including both bounding box and score, are fed to a fully connected layer for classification.

#### IV. RESULTS

In order to conduct a comprehensive evaluation of the proposed approach, a dataset with non-uniform background and no color restrictions was collected using non-depth cameras. Specifically, our dataset includes RGB images of ArSL gestures captured using mobile cameras from both deaf and hearing signers with different hand sizes and skin tones. One should note that the existing datasets do not comply with these conditions. Fig. 5 shows sample images that correspond to the letter “Ghayn” sign. Different signers, from different nationalities, sex, and age group, performed the thirty ArSL sign gestures in various backgrounds and illumination and variation according to their sign preference. This resulted in a collection of 15,360 images of size  $720 \times 960 \times 3$ . The ground truth for each image consists in the label of the gesture which is the corresponding alphabet, and the coordinates of the upper left corner  $(x,y)$  and the  $(width, height)$  of the bounding box that tightly engulfs the hand gesture. Both, the labels and the bounding box coordinates are provided and used in the learning process.



Fig. 5. Sample Images the Letter "Ghayn" from our Collected ArSL Data.

To evaluate the performance of the proposed approach to recognize each ArSL class, four standard performance measures were adopted, namely, the accuracy, the precision, the recall and the F-1 measure were used in our experiments. Note that although the detection of the hand is a critical task achieved by the proposed approach, the ultimate purpose remains the gesture recognition. Therefore, a clear focus is made on the overall recognition performance to assess the obtained results.

The models considered in this research were trained on the collected ArSL dataset. Specifically, the dataset was first split into three parts: 12,240 images (60 %) were used for training. On the other hand, 20% of the image collection was dedicated for a 3-fold cross-validation. Finally, 3060 images (20%) were reserved for testing. The resulting subsets were used to train both the VGG-16 and ResNet based networks. In order to conduct a fair comparison, we secured a uniform hyperparameter setting for VGG-16 and ResNet-18. Particularly, the starting learning rate is set to 1e-3 with a Stochastic Gradient Descent (SGD) optimizer of 0.9 momentum and a minibatch size of 1. Since a high number of epochs may lead to an accidental overfitting, a zero-patience stopping criteria was adopted in our experiments. This technique reduces the over-

fitting risk and provides an insight on the recognition progress during the training phase. In other words, the validation accuracy is monitored after each epoch, and at first sign of degradation the training is set to halt.

For a more objective assessment, a 3-folds cross-validation was adopted for validation in our experiments. Each fold contains 8160 images for training and 4080 images for testing. Besides, the anchor box hyperparameter, which is a critical factor for the recognition performance, was evaluated using all training images and their corresponding bounding boxes in order to find the optimal value that yields the highest IoU. Empirically, setting the number of anchor boxes to 9 yielded the best performance. Table I reports the results obtained using the two considered models; VGG-16 and ResNet-18. As it can be seen, both models yield a good performance with an accuracy around 93% with a slight edge for ResNet-18.

Although the results for both models reflect an extremely close performance, in term of training time, ResNet outperforms VGG-16. In fact, ResNet achieved its highest performance after 371 epochs while VGG-16 achieved it after 516 epochs. In order to investigate further the two models performances, we analyzed their recognition results with respect to each class. Particularly, Fig. 6 and Fig. 7 report the confusion matrix, and the performance measures obtained using the VGG16 and ResNet respectively.

As it can be seen, simple gestures like "Alef" and "Lam", are recognized correctly despite the intra-class variation noticed in the dataset as illustrated in Fig. 7. Moreover, the two classes "Dhad" and "Ya" that exhibit similar gestures have a total of three misclassified instances only. However, similar letters like "Ra" and "Za" have relatively lower recognition rate of 86% and 83% respectively. Another letter with a low performance was "Ghaf" with an average of 83%. This is due to high similarity between "Ghaf" and the letter "TM", despite the fact that the latter had good average recognition of 93%.

On the other hand, as shown in Fig. 8, ResNet is able to distinguish between similar letters like "Sheen" and "Seen" with only one misclassified instance. However, letters like "Ayn" and "Ghayn", although having a high recognition rate of 90%, the 10% misclassified instances were classified as unsimilar letters. In fact, few instances of the letter "Ayn" are classified as "Jeem" and "Thal" by both models. This can be attributed to the high variance of these "Ayn" instances. The lowest recognition rate obtained by ResNet model is for the class "Za" with a value of 84%. This due to the high visual similarity between the two letters "Za" with "Ra".

TABLE I. PERFORMANCE MEASURES OBTAINED USING VGG-16 AND RESNET-18

	Validation				Testing			
	Accuracy	Precision	Recall	F1	Accuracy	Precision	Recall	F1
ResNet-18	98.6%	98.5%	98.6%	98.5%	93.4%	93.3%	94.3%	93.7%
VGG-16	97%	97%	97%	97%	93.2%	93.6%	93.5%	93.5%

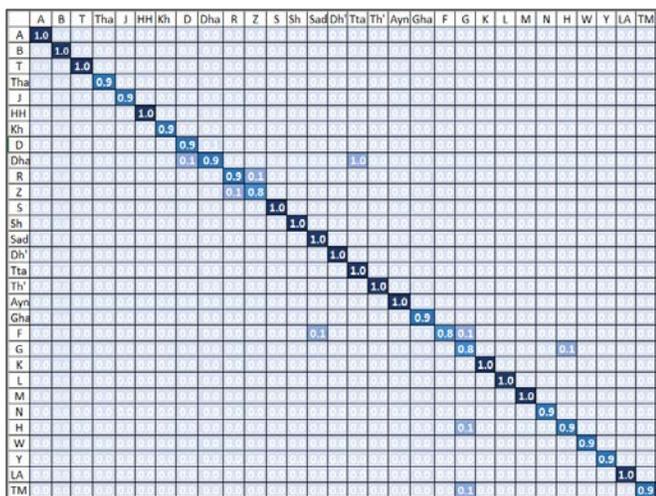


Fig. 6. Confusion Matrix for VGG-16 Obtained using the Test Set.

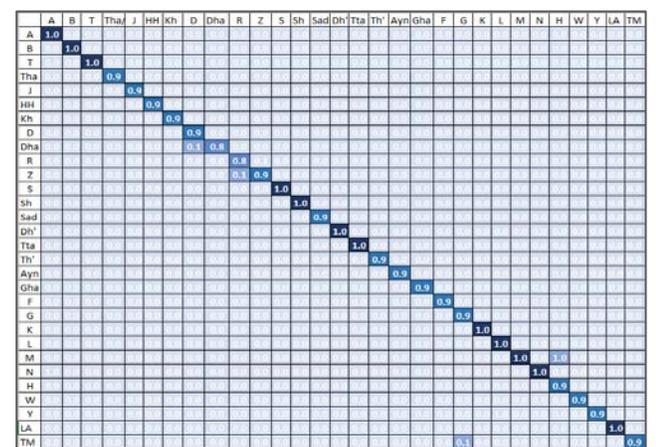


Fig. 7. Confusion Matrix for ResNet-18 Obtained using the Test Set.

Sample results for four sign gestures obtained using different models are displayed in Fig. 9. As it can be seen, in the reported result images, the sign gestures are contoured with the bounding box along with the associated confidence. One can notice that although the bounding box does not fit exactly the hand sometimes, the recognition confidences are still high.

Moreover, we compared the proposed recognition system to the most relevant state-of-the-art works that reported the highest accuracy for ArSL recognition using non-uniform background images. Specifically, we compared the results obtained by VGG-16 and ResNet to two nearest neighbor classifiers proposed in [9][17] which are based on Skin Profiling and MLP skin segmentation respectively. Table II depicts the performance comparison between the KNN based approaches [9][17], and the two Faster R-CNN approaches based on VGG-16 and ResNet respectively. The obtained results show a huge gap between the proposed Faster R-CNN approaches and the existing work in [9]. In fact, the work in [9] achieved a low detection accuracy of only 4% when implemented with the dataset we collected.

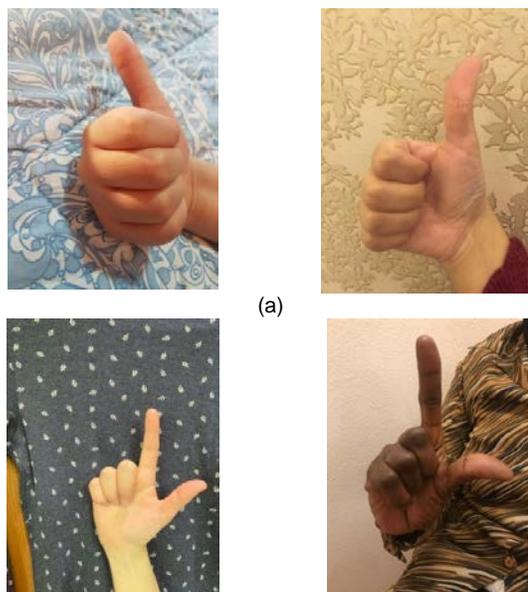


Fig. 8. Dissimilarities between the Letters: (a) “Alef”, and (b) “Lam”.

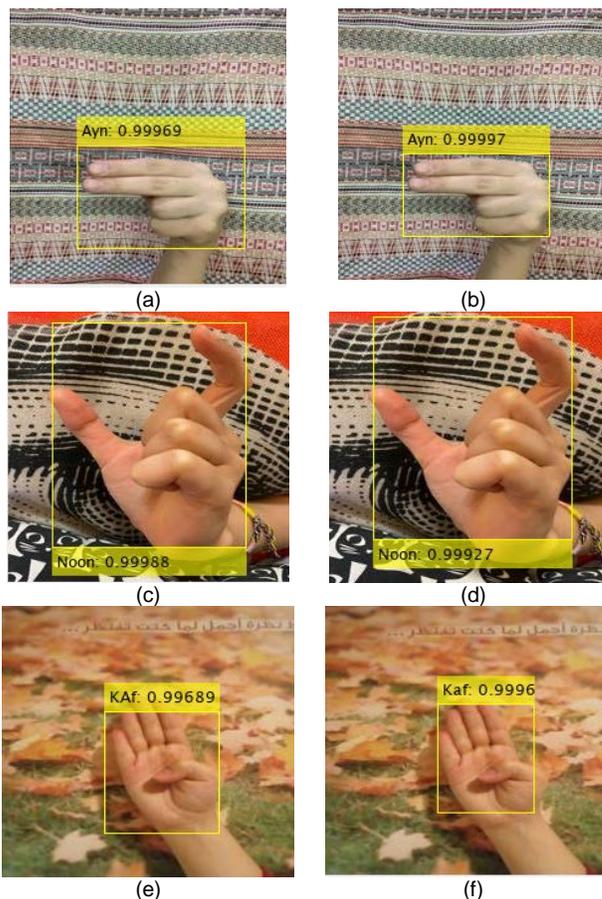


Fig. 9. Sample Recognition Results Obtained using ResNet-18 and VGG-16 for the Letters “Ayn”, “Noon”, and “Kaf”. (a) Recognition of “Ayn” using ResNet-18,(b) Recognition of “Ayn” using VGG-16,(c) Recognition of “Noon” using ResNet-18,(d) Recognition of “Noon” using VGG-16,(e) Recognition of “Kaf” using ResNet-18, and (f) Recognition of “Kaf” using VGG-16.

TABLE II. PERFORMANCE COMPARISON BETWEEN THE PROPOSED MODELS AND THE EXISTING WORK IN [34] AND [40].

Model	Accuracy %	Precision %	Recall %	F1 %
KNN & Skin-Profile based Approach [9]	14	13.2%	13.2	12.4
KNN & MLP based Approach [17]	41	40%	40.5	40.5
VGG_16 based Approach	93.2	93.3	94.3	93.7
ResNet-18 based Approach	93.4	93.6	93.5	93.5

To verify the performance of the skin-profile based approach [9], we tuned the number of neighbors from 1 to 200 with a step size of five. This proved that the number of neighbors is not the factor that affects recognition rate. To further illustrate the difference in performance, we show in Fig. 10 a sample image with a complicated background in which the signer has similar clothing and skin color, while our models were able to detect the hand and recognize the gesture with confidence of 0.63 and 0.58 using VGG-16 and ResNet respectively. The existing work [9] confused the clothing and the skin which lead to an incorrect classification.

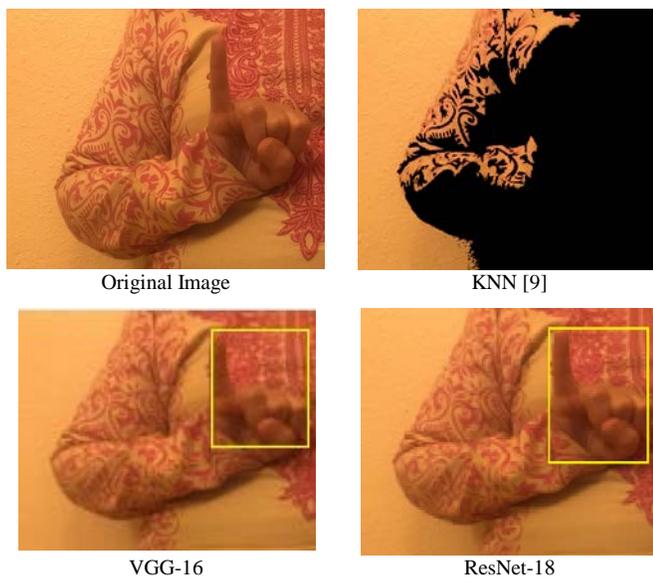


Fig. 10. Recognition of the Letter "Meem" using the Work in [9], R-CNN based on VGG-16 and R-CNN based on Resnet18.

The relatively poor performance of the existing work [9] can be attributed to the simple skin segmentation technique adopted by the authors. In fact, they adopted a YCbCr static skin segmentation which cannot handle different skin tones, lighting, and complex backgrounds. Moreover, the difference between the performance reported in [9] which attains 97%, and the one obtained using our dataset (14%) can be explained by the potential overfitting of their model when used with a very small dataset including 150 images only [9]. Furthermore, the second comparison was done with the work in [17] which outlined a substantial extension of the contributions in [9] that were affected by the considered skin segmentation technique. Specifically, a trained MLP was deployed to detect skin pixels in the images. Despite the ability to handle highly variant skin color and lighting, the system in [17] failed to distinguish the hand from a skin-colored background. In particular, the imag-

es that exhibit less complex background (i.e. non-skin color background) were correctly classified due to the three features extracted from the image. However, the majority of our dataset contains extremely complex background which yielded an accuracy of 41% for the work in [17]. Thus, one can claim that the experiments conducted in this research confirmed the ability of faster R-CNN to recognize efficiently the Arabic sign language. Moreover, they proved that the proposed system outperforms the relevant state of the art solutions in [9][17].

## V. CONCLUSIONS

Arabic Sign Language is the primary form of communication within the Arab Deaf community. However, the sign language is not widely used and/or mastered outside this community which resulted in a real social barrier between Deaf and hearing people. In order to reduce this struggles for the Arab Deaf, researchers introduced ArSL recognition systems able to capture and recognize the hand gesture from images. Despite this effort, most of the reported works use datasets with uniform background in order to by-pass the image segmentation issue. Alternatively, ArSL recognition systems based on deep learning paradigms emerged to alleviate the concern of choosing the most relevant features. Taking into consideration the strengths and weaknesses of the state-of-the art contributions, we designed and implemented a novel ArSL recognition system that is able to localize and recognize the alphabet of the Arabic sign language using a Faster Region-based Convolutional Neural Network (R-CNN). Specifically, faster R-CNN was adapted to extract and map the image features, and learn the position of the hand in a given image. Moreover, the proposed system was assessed using a collection of 15,360 images, containing hand gestures with different backgrounds, captured using standard phone cameras. The association of the proposed architecture with ResNet and VGG-16 models achieved a recognition rate of 93% for the collected ArSL images dataset.

As future works, we propose to investigate the YOLO deep learning architecture [43] instead of Faster R-CNN for ArSL letter recognition. Unlike Faster R-CNN, YOLO can be adapted to conduct the classification and the bounding box regression simultaneously. It proved to achieve accurate and fast recognition when the objects of interest are not too small [43].

## ACKNOWLEDGMENT

This work was supported by the Research Center of the college of Computer and information Sciences at King Saud University, Riyadh, KSA. The authors are grateful for this support.

REFERENCES

- [1] Adam R. 2015. Standardization of Sign Languages. *Sign Language Studies* 15:432–445. DOI: 10.1353/sls.2015.0015.
- [2] Ahmed MA, Zaidan BB, Zaidan AA, Salih MM, Lakulu and MM bin. A Review on Systems-Based Sensory Gloves for Sign Language Recognition State of the Art between 2007 and 2017. *Sensors*. DOI: 10.3390/s18072208.
- [3] Neiva DH., Zanchettin C. 2018. Gesture recognition: A review focusing on sign language in a mobile context. *Expert Systems with Applications* 103:159–183. DOI: 10.1016/j.eswa.2018.01.051.
- [4] Suharjito., Wiryana F., Kusuma GP., Zahra A. 2018. Feature Extraction Methods in Sign Language Recognition System: A Literature Review. 2018 Indonesian Association for Pattern Recognition International Conference (INAPR). DOI: 10.1109/inapr.2018.8626857.
- [5] Abdel-Fattah MA. 2005. Arabic Sign Language: A Perspective. *Journal of Deaf Studies and Deaf Education*. DOI: 10.1093/deafed/eni007.
- [6] Lecun Y., Bottou L., Bengio Y., Haffner P. 1998. Gradient-based learning applied to document recognition. *Proceedings of the IEEE* 86:2278–2324. DOI: 10.1109/5.726791.
- [7] Egmont-Petersen M., Ridder DD., Handels H. 2002. Image processing with neural networks—a review. *Pattern Recognition* 35:2279–2301. DOI: 10.1016/s0031-3203(01)00178-9.
- [8] Mohandes M., Liu J., Deriche M. 2014. A survey of image-based Arabic sign language recognition. 2014 IEEE 11th International Multi-Conference on Systems, Signals & Devices (SSD14). DOI: 10.1109/ssd.2014.6808906.
- [9] Hemayed EE., Hassanien AS. 2010. Edge-based recognizer for Arabic sign language alphabet (ArS2V-Arabic sign to voice). 2010 International Computer Engineering Conference (ICENCO). DOI: 10.1109/icenco.2010.5720438.
- [10] Prewitt J.M.S. 1971. Picture processing and psychopictorics. *Icarus* 15:563–564. DOI: 10.1016/0019-1035(71)90136-9.
- [11] Hotelling H. 1933. Analysis of a complex of statistical variables into principal components. *Journal of Educational Psychology* 24:498–520. DOI: 10.1037/h0070888.
- [12] Serra J. 1993. *Image analysis and mathematical morphology*. London: Academic.
- [13] Altman NS. 1992. An Introduction to Kernel and Nearest-Neighbor Nonparametric Regression. *The American Statistician* 46:175. DOI: 10.2307/2685209.
- [14] Hamed A., Belal NA., Mahar KM. 2016. Arabic Sign Language Alphabet Recognition Based on HOG-PCA Using Microsoft Kinect in Complex Backgrounds. 2016 IEEE 6th International Conference on Advanced Computing (IACC). DOI: 10.1109/iacc.2016.90.
- [15] Cortes C., Vapnik V. 1995. *Machine Learning* 20:273–297. DOI: 10.1023/a:1022627411411.
- [16] Velho L., Frery AC., Gomes J., Gomes J. 2009. *Image processing for computer graphics and vision*. New York, NY: Springer.
- [17] Dahmani D., Larabi S. 2014. User-independent system for sign language finger spelling recognition. *Journal of Visual Communication and Image Representation* 25:1240–1250. DOI: 10.1016/j.jvcir.2013.12.019.
- [18] Rosenblatt F. 1961. Principles Of Neurodynamics. *Perceptrons And The Theory Of Brain Mechanisms*. DOI: 10.21236/ad0256582.
- [19] Hu M-K. 1962. Visual pattern recognition by moment invariants. *IEEE Transactions on Information Theory* 8:179–187. DOI: 10.1109/tit.1962.1057692.
- [20] El-Bendary N., Zawbaa HM., Daoud MS., Hassanien AE., Nakamatsu K. 2010. ArSLAT: Arabic Sign Language Alphabets Translator. 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM). DOI: 10.1109/cisim.2010.5643519.
- [21] Lowe DG. 2004. Distinctive Image Features from Scale-Invariant Keypoints. *International Journal of Computer Vision* 60:91–110.
- [22] Tharwat A., Gaber T., Hassanien AE., Shahin MK., Refaat B. 2015. SIFT-Based Arabic Sign Language Recognition System. *Advances in Intelligent Systems and Computing Afro-European Conference for Industrial Advancement*:359–370. DOI: 10.1007/978-3-319-13572-4\_30.
- [23] Fisher RA. 1936. The Use Of Multiple Measurements In Taxonomic Problems. *Annals of Eugenics* 7:179–188. DOI: 10.1111/j.1469-1809.1936.tb02137.x.
- [24] Al-Jarrah O., Halawani A. 2001. Recognition of gestures in Arabic sign language using neuro-fuzzy systems. *Artificial Intelligence* 133:117–138. DOI: 10.1016/s0004-3702(01)00141-2.
- [25] Jang J-S. 1993. ANFIS: adaptive-network-based fuzzy inference system. *IEEE Transactions on Systems, Man, and Cybernetics* 23:665–685. DOI: 10.1109/21.256541.
- [26] Sadeddine K., Djeradi R., Chelali FZ., Djeradi A. 2018. Recognition of Static Hand Gesture. 2018 6th International Conference on Multimedia Computing and Systems (ICMCS). DOI: 10.1109/icmcs.2018.8525908.
- [27] Canny J. 1987. A Computational Approach to Edge Detection. *Readings in Computer Vision*:184–203. DOI: 10.1016/b978-0-08-051581-6.50024-6.
- [28] He D-C., Wang L. 1990. Texture Unit, Texture Spectrum And Texture Analysis. 12th Canadian Symposium on Remote Sensing Geoscience and Remote Sensing Symposium. DOI: 10.1109/igarss.1989.575836.
- [29] Zernike VF. 1934. Beugungstheorie des schneidener-fahrens und seiner verbesserten form, der phasenkontrastmethode. *Physica* 1:689–704. DOI: 10.1016/s0031-8914(34)80259-5.
- [30] Specht DF. 1990. Probabilistic neural networks. *Neural Networks* 3:109–118. DOI: 10.1016/0893-6080(90)90049-q.
- [31] Alzohairi R., Alghonaim R., Alshehri W., Aloqeely S. 2018. Image based Arabic Sign Language Recognition System. *International Journal of Advanced Computer Science and Applications* 9. DOI: 10.14569/ijacsa.2018.090327.
- [32] Hayani S., Benaddy M., Meslouhi OE., Kardouchi M. 2019. Arab Sign language Recognition with Convolutional Neural Networks. 2019 International Conference of Computer Science and Renewable Energies (ICCSRE). DOI: 10.1109/iccsre.2019.8807586.
- [33] Jain LC., Medsker L. 2000. *Recurrent neural networks: design and applications*. Boca Raton, FL: CRC Press.
- [34] Maraqa M., Abu-Zaiter R. 2008. Recognition of Arabic Sign Language (ArSL) using recurrent neural networks. 2008 First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT). DOI: 10.1109/icadiwt.2008.4664396.
- [35] Zell A. 2003. *Simulation neuronaler Netze*. München: Oldenbourg.
- [36] Elman JL. 2020. Finding structure in time. *Connectionist psychology: A text with readings*:289–312. DOI: 10.4324/9781315784779-11.
- [37] Jordan MI. 1986. Serial order: a parallel distributed processing approach. La Jolla, CA: Institute for Cognitive Science, University of California, San Diego.
- [38] Dunn JC. 1973. A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters. *Journal of Cybernetics* 3:32–57. DOI: 10.1080/01969727308546046.
- [39] Aly S., Osman B., Aly W., Saber M. 2016. Arabic sign language finger-spelling recognition from depth and intensity images. 2016 12th International Computer Engineering Conference (ICENCO). DOI: 10.1109/icenco.2016.7856452.
- [40] Ren S, He K, Girshick R, Sun J. 2016. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. DOI: 10.1109/tpami.2016.2577031.
- [41] Simonyan K, Zisserman A. 2015. Very Deep Convolutional Networks for Large-Scale. *ICLR*.
- [42] He K., Zhang X., Ren S., Sun J. 2016. Deep Residual Learning for Image Recognition. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). DOI: 10.1109/cvpr.2016.90.
- [43] Redmon J., Divvala S., Girshick R., Farhadi A. 2016. You Only Look Once: Unified, Real-Time Object Detection. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). DOI: 10.1109/cvpr.2016.91.
- [44] Ethnologue. 2019. Languages of the World. Available at [http://www.ethnologue.com/15/show\\_family/90008/](http://www.ethnologue.com/15/show_family/90008/) (accessed April 1, 2019).

# Attack Resilient Trust and Signature-based Intrusion Detection Systems

Boniface Kabaso<sup>1</sup>, Saber A. Aradeh<sup>2</sup>, Ademola P. Abidoye<sup>3</sup>

Department of Information Technology, Cape Peninsula University of Technology  
Cape Town, South Africa

**Abstract**—Wireless sensor networks have been widely applied in many areas due to their unique characteristics. These have exposed them to different types of active and passive attacks. In the literature, several solutions have been proposed to mitigate these attacks. Most of the proposed solutions are too complex to be implemented in wireless sensor networks considering the resource-constraint of sensor nodes. In this work, we proposed a hierarchical trust mechanism based on clustering approach to detect and prevent denial of service attacks in wireless sensor networks. The approach was validated through simulation using Network Simulator (NS2). The following metrics were used to evaluate the proposed scheme: packet delivery ratio, network lifetime, routing delay, overhead, and number of nodes. The proposed approach is capable of detecting compromised sensor nodes vulnerable to a denial of service attacks. Moreover, it is able to detect all sensed data that have been compromised during transmission to the base station. The results show that our method can effectively detect and defend against denial of service attacks in sensor wireless sensor networks.

**Keywords**—Wireless sensor network; routing attacks; public-key cryptography; packet dropping; denial of service attacks

## I. INTRODUCTION

The self-organized Wireless Sensor Network (WSN) is used predominantly in tracking and monitoring applications, and it is made of battery-powered sensor nodes that communicate through a wireless medium [1]. WSNs are initially used in military operations for monitoring enemies' movements in a particular area. However, since the development of the Internet of Things (IoT), WSNs have been widely applied in many areas such as automobile industries, aviation, environmental monitoring, and many more areas [2]. The fast-growing sensor network has reached its presence in almost every sector replacing human intervention. The primary concerns of WSN are the utilization of sensor node resources, provision of security against malicious attacks, and the provision of efficient data delivery. The WSN adopts a clustering algorithm and routing protocol for avoiding the overutilization of the sensor node's resources. The clustering algorithm divides the nodes and performs routing activities based on the role of the cluster leader and members. It significantly reduces the energy consumption of each node. The routing protocols select a suitable path that does not impact the performance metrics of WSN and also provides energy efficiency. The routing protocols must be resistant to communication delay and packet losses. The function of sensor nodes is to sense, process, and transfer the data to the desired location while maintaining their reliability and confidentiality

[3]. Both these parameters are affected due to the security threats in the networks. The resource vulnerabilities in the sensor network impact the design of effective security mechanisms. Several security mechanisms help in avoiding the attacks that target the routing functionality of sensor nodes.

### A. The Conventional Security Mechanisms in WSN

One of the major concerns of security mechanisms in WSN is to provide secure transmission of data from the sender to the receiver end without much utilizing the sensor node resources. The security in traditional routing protocols placed in a dynamic environment is complicated, and communication is not adequately secured [4]. The design of security mechanisms must involve both proactive and reactive methodologies while protecting against attacks. When a malicious intruder attacks the network, the compromised nodes have to resist in a way that does not influence other legitimate nodes to fall for the attack. The difficult task of resisting the attack is to know the source of the adversary, and it can be done using Intrusion Detection Systems (IDS) [5]. Most of the security requirements are built on cryptographic schemes, IDS, and trust-based schemes. The trust-based mechanisms provide a secure transfer of data through trustworthy nodes in the network. The use of efficient cryptographic schemes along with robust intrusion detection systems can enhance security schemes [6]. Security management is also crucial for managing the security level and its energy consumption. The security mechanism introduced in the network must be compatible with all the components of the network otherwise it becomes the target for the attack [7]. Fig. 1 presents the types of conventional security mechanisms [8].

### B. Trust-Based Management

Trust management is a required parameter in routing protocols and security mechanisms. It is used to determine whether a node is faithful enough to forward the data packets and store important keys [9]. It is used primarily to quantify the trustworthiness and reliability of individual nodes based on their behavior and past experiences [10]. A node is considered trustworthy depending on the packet forwarding rate, energy consumption, delay, and other factors depending on the application. The trust values must be accurately measured to provide reliable and robust security services the traditional trust management utilizes more energy and sensor node resources. The lightweight trust-based mechanisms need to be developed to overcome the issues of resource utilization and to provide efficient trust management. The trust-based management

scheme that helps in secure data transmission for WSN is presented in Fig. 2.

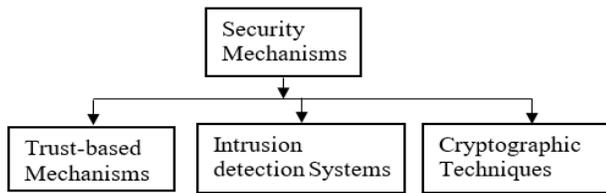


Fig. 1. The Conventional Security Mechanisms in WSN.

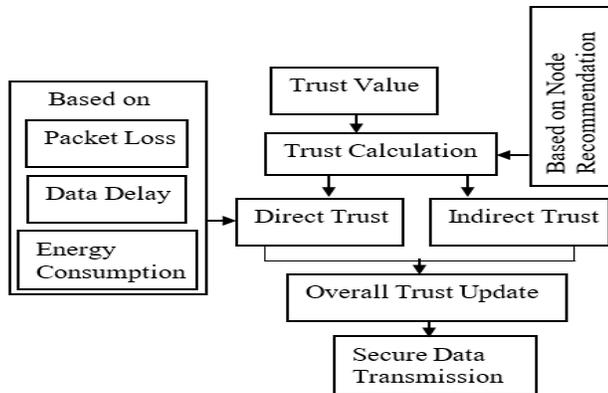


Fig. 2. Trust Management.

The trust-based mechanisms in WSN face some challenges during trust establishment [11]. Due to the storage and energy restriction in sensor nodes, the complexity of the trust value calculation must be less as possible. The validity of the trust value and the status of the node must neither be a long or short interval. The trust evidence has to be collected only during specific time intervals to avoid malicious attacks and wastage of energy resources. The level of trust requirements of the nodes must depend on the role it performs in the network. For example, the task of the cluster head is to carry all the essential information collected from the members to the base station, and hence the next-hop nodes of the cluster head through which it transmits the data to the destination must be more trustworthy.

Trust management schemes must be at least robust against the most common attacks as they will degrade the security requirements such as confidentiality and privacy of the network. The trust establishment process must occur in a secure channel as the integrity of the trust value is important to determine the node's honesty. The trust establishment methods must be flexible to dynamic topology networks and node behavior. As the location of nodes is hidden for security reasons in sensitive applications such as enemy monitoring in military applications, it is difficult to establish trust management mechanisms in an anonymous sensor network.

### C. Hierarchical Routing Protocol

In the hierarchical routing protocols, the distribution of nodes is in the form of a tree-based structure, where nodes are assigned to perform specific roles based on the energy

capability. For instance, the high-energy nodes are assigned important roles compared to low energy nodes [12]. The hierarchical routing protocol is more advantageous for real-time applications as it enhances the network lifetime by decreasing the transmission distance between the neighbor nodes used for transmitting the data to the destination. The hierarchical routing protocol can be cluster-based or chain-based. In cluster-based routing protocols, the nodes are classified based on energy capability as cluster heads and member nodes. The nodes with high energy are selected as cluster heads. The member nodes send the data to their respective cluster heads, and the cluster head then aggregates the information and forwards it to the base station.

### D. Problem Statement

The routing protocols play a significant role in transferring the data packets to a destination in an efficient way, and data aggregation helps in reducing overall energy consumption and limited utilization of sensor node resources. In routing and data aggregation, the trustworthiness of nodes is a required parameter. Several trust-based schemes have been developed to achieve data forwarding by trustworthy nodes. In the traditional IDS schemes, the trust measurement is determined using a single metric, which in turn resulted in inaccurate detection. Thus, to overcome this issue, the use of multidimensional trust values such as Interactive Trust (IT), Honesty Trust (HT), and Content Trust (CT) is introduced during the trust calculation to improve the accuracy of the attack detection. IT is determined by the number of interactions between nodes in the network. The HT is determined based on the number of successful and unsuccessful interactions in the network while the CT is determined based on the capacity such as energy and the amount of data

### E. Research Objectives

- To Develop and data delivery by energy-efficient security mechanism which provider trade o between utilization of sensor nodes.
- To evaluate the efficiency of the proposed scheme for achieving secure routing, the data packet dropping and modification attack model is designed.

### F. Contributions

The contributions of this research are presented as follows:

- 1) The proposed contribution is built on an IDS model and is called IDS using Hierarchical Trust Measurement (IDSHT), where the trust measurement is done based on multidimensional factors such as IT, HT, and CT.
- 2) The signature-based mechanism is used for preventing common attacks, and the signature generation and verification are performed using the Rivest–Shamir–Adleman (RSA) algorithm.

## II. RELATED WORK

The energy-efficient routing protocols are surveyed mainly using three categories such as data-centric routing, hierarchical routing, and location-based routing. The location-based energy-aware reliable routing protocol (LEAR) [13] is a type of location-based routing protocol, which follows the

clustering algorithm. LEAR aims to reduce energy consumption by adopting geographical positioning and clustering technique. The routing table of each node is constructed using a distance of the neighboring nodes which in turn calculate the location information collected by Global Positioning Systems (GPS). When a node needs to send data, it refers to its routing table and thereby forwards the data to a neighboring node, which has the shortest distance. In [14], the authors proposed the Geographic and Energy Aware Routing protocol (GEAR) which deals with the use of geographic information while disseminating queries to required locations. The main idea of GEAR is to restrict the number of interests by sending interests to specific regions rather than the whole network. Each node in GEAR keeps an estimated cost and learning cost for reaching the destination through neighboring nodes.

Sensor Protocols for Information Via Negotiation scheme (SPIN) was proposed in [15]. It is a type of data-centric routing protocol which uses metadata negotiations to eliminate the transmission of redundant data throughout the network.

In [16] a systematic analysis of the threat posed by the Sybil attack in WSN is presented. The Sybil attack is defined as the malicious node legitimately taking on multiple identities of a node in the network. These attacks can affect the redundancy mechanism of the distributed data storage systems in peer to peer network. The authors highlight that the Sybil attack is a threat to essential functions such as routing, resource allocation, and misbehavior detection that can cause severe effects. The taxonomy of Sybil attacks is presented to understand and analyze the threat and its countermeasures in the network. The authors also discuss the different defense mechanisms against Sybil suited for WSN. The two methods presented are direct validation and indirect validation. The denial of service (DoS) attack is defined as any event that diminishes or eliminates network capacity to perform its expected function [17]. The different DoS attacks are jamming, collision attacks, unfairness attacks, black hole attacks, neglect and greed attack, homing attack, and misdirection attacks. The countermeasures for the jamming attack are by using spread spectrum, priority messages, and lower duty cycle.

The authors in [18] discussed the countermeasures taken against selective forwarding attacks. The analysis highlights that the security and on-time transmission of packets is the basic need for sensor network and the selective forwarding attacks targets these requirements.

The encryption schemes in WSN are categorized mainly into two types and they are symmetric key encryption schemes [19-22], and asymmetric key encryption schemes [23]. The authors in [24] introduced two building block security protocols such as SNEP (Secure Network Encryption Protocol) and Timed Efficient Streaming Loss-Tolerant Authentication TESLA. The SNEP protocol ensures data confidentiality, two-party authentication, and evidence of data freshness. The protocol is used to ensure authenticated broadcast for the resource constraint sensor network. Each node shares a secret key with the base station. During data communication, the two nodes consider an intermediate node such as a base station for setting a new key between them. The advantages of SPINS are

resilient to node capture attacks, where any node does not leak any information about other sensor nodes, and it is easy to revoke key pairs in case of attacks.

In [25] the author proposed the Ambient Trust Sensor Routing (ATSR) protocol, which uses a trust management system for providing secure routing of data packets in the network. Each node in the network sends the periodic broadcast messages with node Identity (ID) and energy availability. A multicast message such as a reputation request message is sent periodically to the neighboring nodes for obtaining the indirect trust information, and the reply is gathered from unicast messages. The trust metrics used by nodes to evaluate the adjacent nodes are forwarding data rate, residual energy, and distance. The advantage of the ASTR scheme is that the data packets are forwarded based on the energy metric of the next-hop node thereby achieving energy conservation.

The authors in [26] presented a reputation-based event-triggered formation control (RETF) in which trust-related information about neighbor nodes is resolved and stored in the form of a set of modules by each node in the network. Several IDS mechanisms-based schemes have been introduced based on the types of attacks and application requirements to provide efficient detection of attacks before causing severe damage to the systems [27]. The authors presented an IDS survey based on the target WSN, detection technique, collection process, trust model, and analysis technique.

### III. FRAMEWORK FOR THE PROPOSED SCHEME

This section presents the framework for the proposed scheme based on based IDS-hierarchical trust (IDSHT) model. It adopts a cluster-based network using a two-tier hierarchical trust mechanism to reduce the energy consumption of the nodes in the system.

The nodes in the cluster-based network are classified into cluster head (CH), sensor nodes (SN), and base station (BS). In each cluster, the CH is selected based on the residual energy and transmission distance, and it forwards the data packets from the member nodes to the base station in an efficient manner the CH has more energy than the member nodes that communicate with their respective CH and have minimum energy. CH aggregates the data sent by the sensor nodes before sending it to the BS. The CH transmits the aggregated data to the base station directly. Each SN has a unique identity and belongs to a single cluster. The cluster head stores the data in the form of queues that are collected from the SN before forwarding it to the BS as shown in Fig. 3.

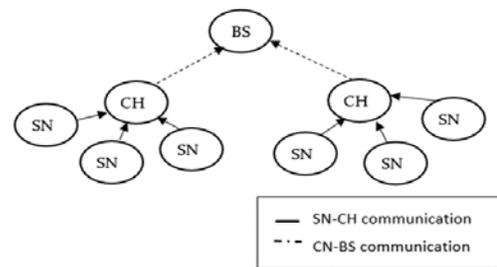


Fig. 3. Hierarchical Cluster-based Topology of Proposed IDSHT Scheme.

In the proposed scheme, each node in the network broadcasts the control information by attaching its ID and residual energy for identifying its neighbors. When the neighboring nodes receive the transmitted hello message, the neighbor nodes take the particular node as a neighbor and update the same in the adjacent table. The conventional security mechanisms that are used for detecting attacks in the network have used only single metrics for evaluating trust in WSN. The main issue faced during the trust evaluation is the lack of accuracy in detection. The first level of trust in WSNs is the SN trust evaluation, which is done by CH in a particular cluster using the following multidimensional metrics discussed below.

1) *Interactive Trust Evaluation of SNs (IT)*: The IT is calculated using the number of interactions of the SN in the network. The interactions of the SN include the sending and receiving data packets between the nodes and requests sent or forwarded from other nodes. The IT at the CH level is calculated using some interactions between CH and BS.

2) *Content Trust Evaluation of SNs (CT)*: The CT is based on the trust evaluation of the observing data, and it is the data-centric trust evaluation calculated using a CH. The primary purpose of SNs is to sense the different parameters such as temperature, humidity, air pressure, and light intensity and transmit the observing data to the respective CHs.

3) *Honesty Trust evaluation of SNs (HT)*: The HT is calculated using the number of successful and unsuccessful interactions between the CH and SN in the network. In HT, the CH overhears the SN when the interaction is unsuccessful. The trust evaluation at the CH level considers only the direct trust calculation using BS-CH evaluation. The trust evaluation in CH is similar to the SN level trust evaluation, and it includes multidimensional factors such as IT, CT, and HT. The IT, CT, and HT are calculated using the BS-CH evaluation while the CT includes the proximity of aggregated data and effective average observing data.

4) *Content Trust Evaluation of CH (CT)*: The CT is defined as the trust value obtained by the deviation between sensing data and an effective average of observed data. The CT of CH is calculated by BS according to the proximity of fusion data and effective average observing data of SN in the cluster. The overall trust of CH is calculated using BS by aggregating the multidimensional factors such as CT<sub>CH</sub>, HT<sub>CH</sub>, and IT<sub>CH</sub> evaluated for CH and is shown in equation 1. If the node launches the selfish attack, it will forward a false energy value in the control information to avoid being selected as a CH to preserve its energy.

$$OT_{ch} = W1 * IT_{ch} + W2 * HT_{ch} + W3 * CT_{ch} \quad (1)$$

where  $W_1=0.2$ ,  $W_2=0.4$ ,  $W_3=0.4$ .

Thus, the main issue faced with IDS schemes is that even after removing the malicious nodes, further attacks such as impersonation attacks are induced in the network. The impersonation attacks are serious attacks, where the adversary successfully uses one of the identities of legitimate nodes to provide a gateway for other types of attacks. The signature generation and verification using RSA algorithm security of

the proposed IDSHT scheme can be improved by using signature generation, and verification mechanism, and it is termed as S-IDSHT. In S-IDSHT, each SN generates the public key and private key using the RSA algorithm. The SN forwards the data packet to their respective CHs after encrypting the data using the public key shared among the member nodes. After the data packet reaches the CH, the encrypted data is then decrypted using the private key, which is a secret key allocated for CH. Then, the CH aggregates all data along with the RSA signature collected from the member nodes and forwards it to the base station. The data aggregation during this process reduces the energy consumption of the overall network. The BS collects the data from all the CHs and decrypts the aggregated data using the unique private key and verifies the received data signature is the same as the original data. If the signature of the original data is not the same as that of the received data, then the node is said to be an adversary, and it is an impersonation attacker. If the signature of the original data is the same as the signature of receiving data, the node is said to be legitimate.

#### IV. PROPOSED SCHEME STRUCTURE

The proposed IDSHT-S scheme adopts a hierarchical cluster-based structure to ensure secure and efficient data transmission during the routing and data aggregation process. The trust evaluation in the proposed scheme is based on the two-tier hierarchical trust mechanism, and the two levels of trust evaluation include the SN level and CH level. The trust value is calculated using multidimensional factors such as IT, CT, and HT. These multidimensional factors are used for finding the overall trust for SN and CH where the data is verified using signatures. The signature generation and verification in the proposed scheme are done using the RSA algorithm. SNs encrypt the data before transferring the data to the CH, which acts as an intermediate node and aggregator. The simulation scenario of the IDSHT-S scheme is constructed using the Network Simulator (NS2) tool. The proposed scheme is developed by modifying the Ad-hoc On-Demand Distance Vector (AODV) protocol files in NS2. In the experimental phase, the node formation is the first phase. After the selection of a source node and a destination node, the best path from the source to reach the destination is estimated by the AODV protocol. The AODV protocol is modified according to the application requirement. In the proposed scheme, the AODV protocol is modified the routing protocol based on IDSHT and IDSHT-S scheme objectives.

##### A. Hierarchical Trust Mechanism in IDSHT Scheme

One of the major concerns of security mechanisms in WSN is to provide secure transmission of data from the sender to the receiver end without much utilizing the sensor node resources. The security in traditional routing protocols placed in a dynamic environment is complicated, and communication is not adequately secured. In the proposed IDSHT scheme, the two-tier hierarchical mechanisms are introduced, and the trust evaluation for routing behavior and data aggregation is done using multidimensional metrics such as IT, T, and HT. The two levels of trust evaluation are done such as SN trust evaluation and CH trust evaluation. The first level of trust evaluation is simple, as the SN evaluation is done through

direct communication between CH and SN in a cluster. The second level consists of the trust evaluation at the cluster head level is explained along with its multidimensional factor evaluation.

### B. Signature Based IDSHT Scheme

The main issue faced in IDS schemes is that even after removing the malicious nodes, further attacks such as impersonation attacks are induced in the network. The impersonation attacks are one of the serious attacks, where the adversary successfully uses one of the identities of legitimate nodes, and it uses these fake identities to provide a gateway for other types of attacks. The main aim of the impersonation attacks is to obtain confidential information that should be kept secret during the entire data transmission. Every node in the network encrypts its data and abstracts the information, which includes the data sending time, node ID, and ID of the data. After attaching the signature, the aggregated data is then sent to the BS. Through this method, the aggregated data can be verified by BS and confirm that every data forwarded to it is valid.

### C. Signature Generation and Verification using RSA Algorithm

Signature generation and verification mechanisms are used as another security layer to improve the security of the proposed scheme. Thus, each SN generates the public key and private key using the RSA algorithm. The role of cryptographic techniques is to prevent any leakage or modification of confidential data in WSNs [28]. The leakage of data is prevented by encrypting the data using keys and sending the encrypted data to the destination. As most of the encryption and key management schemes require complex computation and increased costs, the need for designing lightweight cryptographic schemes and achieving a trade-off between providing security and limited utilization of resources has become a necessity [29]. The two types of cryptographic keys used for authentication and encryption are a public key and a private key. The public key is known by designated nodes, while private keys are kept secret by specific nodes. A digital signature is used for authentication and maintaining the message's integrity. The digital signature involves three algorithms such as key generation, signing, and signature verifying algorithm. The advantage of using a digital signature is that it is difficult to forge a user's signature without knowing the private key. Both IDS and trust-based schemes make sure that the attacks are not initiated in the network. The cryptographic schemes alone cannot provide an effective security mechanism, and it has to be combined with other security mechanisms to achieve all the security requirements of WSN. The data aggregation during this process reduces the energy consumption of the overall network. The BS collects the data from all the CHs and decrypts the aggregated data using the unique private key and verifies that the received data signature is the same as the original data. If the signature of the original data is not the same as that of the received data, then the node is said to be an adversary, and it is an impersonation attacker. If the signature of the original data is the same as the signature of receiving data, the node is said to be legitimate. In the proposed scheme, the data integrity and confidentiality of

the data are secured, and efficient data transmission is achieved.

### D. The Simulation Components for Network Scenario

NS2 Tool: The NS2 is an open-source event-driven simulator tool that is used in studying the dynamic nature of communication networks. The NS2 simulation tool is used for performing simulations in both the wired and wireless sensor networks.

C++: C++ is a high-level programming language used for graphical applications, and it is used in the back-end mechanism in NS2 tool. The C++ programming language is used for running the simulation, and all the C++ files are compiled and linked to create an executable file.

OTCL: The OTCL is a scripting language used for the configuration and setup of the simulation in NS2 tool. In NS2, the C++ objects are made available to the OTCL interpreter and can be controlled by OTCL level.

Network Animator (NAM) Output: The NAM is used to represent the network and packet traces graphically. It supports topology layouts, packet-level animation, and data inspection tools.

X-Graph: The X-graph program draws the graph on an X-display such that the data read from either data files or standard input if no files are displayed. The network scenario in the proposed IDSHT-S scheme is built in a hierarchical structure, and the cluster-based routing is used to provide efficient data transmission as shown in Fig. 4.

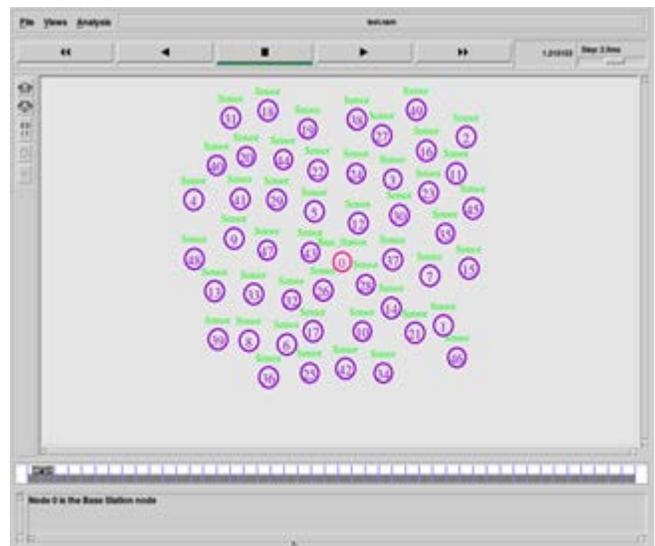


Fig. 4. The Network Scenario of the Proposed IDSHT-S Scheme.

## V. RESEARCH FINDINGS

Since there is a possibility to launch the impersonation attacks by the malicious nodes in WSN, the RSA is used for signature generation and verification processes. The proposed IDSHT-S modifies the AODV routing protocol files such as aodv.cc file concerning the proposed scheme. Comparison is made between the IDSHT-S and the existing IDSHT. Both are evaluated using the same simulation settings and compared to their outputs. The following metrics were used for the

evaluation: Packet Delivery Ratio (PDR), Network lifetime, Delay, and Overhead. The numbers of nodes are varied from 40 to 70 at 10 intervals each. Graphs are plotted for performance metrics using X-graph in NS-2.

1) *Packet Delivery Ratio (PDR)*: The ratio between the total number of delivered packets to the base station and the total number of transmitted packets from the sensor nodes.

2) *Network lifetime*: The network lifetime represents the remaining energy of a node, which has minimum energy in the network.

3) *Delay*: Every node follows the secure routing protocol to deliver the data packets to the base station. Delay of a packet is defined as the average time taken by a node to deliver the data packets to the base station.

4) *Overhead*: The overhead is defined as the total number of control packets used in the network. The routing protocols exploit control packets to detect the routing paths to the base station. More control packets tend the sensors to spend a lot of energy and so maintaining the overhead while providing network security is essential.

5) *Number of Nodes vs Packet Delivery Ratio*: The packet delivery ratio depends on the number of data packets received at the base station and the number of packets forwarded by the CH after the aggregation process. The graph of the simulation result is drawn by plotting the number of nodes in the X-axis and packet delivery ratio on the Y-axis as shown in Fig. 5. The packet delivery ratio values are expressed in percentage for both the existing IDSHT scheme and the proposed IDSHT-S scheme.

6) *Number of Nodes Vs Delay*: The delay in WSN is the time taken by the data to reach the destination, i.e., base station. The delay of data packets affects the performance of the network. The delay in the system is mainly caused due to the dropping of the data packet. Node collision depends on the time taken for trust evaluation and other factors. The simulation graph for the delay is shown in Fig. 6 by taking the number of nodes on the X-axis and the delay expressed in seconds on the Y-axis.

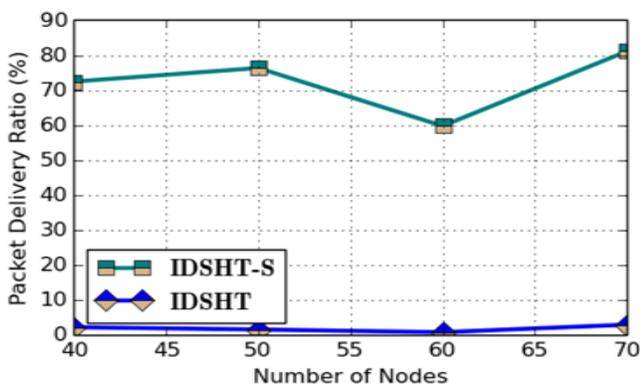


Fig. 5. The Simulation Graph for Number of Nodes vs Packet Delivery.

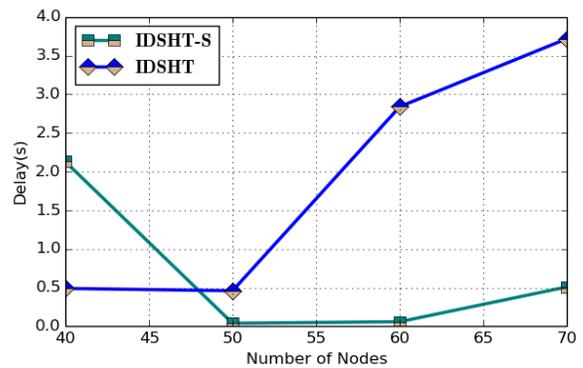


Fig. 6. The Simulation Graph for Number of Nodes vs Delay.

7) *Number of Nodes vs Network Lifetime*: The network lifetime is indirectly proportional to the energy consumption in the network. When energy consumption is large, the network lifetime is drastically reduced. The battery exhaustion in attacks occurs mainly due to malicious attackers and the proposed scheme aims at revoking these malicious attacks. The simulation results are presented in graphical form as shown in Fig. 7.

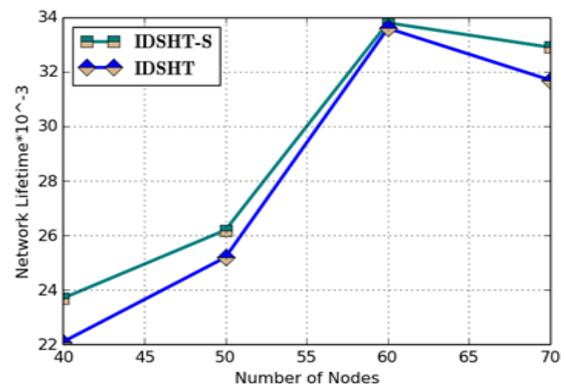


Fig. 7. The Simulation Graph for Number of Nodes vs Network Lifetime.

## VI. CONCLUSION

Several trust-based security mechanisms have been developed to provide secure routing and data aggregation in WSN. The trade-off between energy efficiency and accurate trust calculation is one of the major concerns while developing intrusion detection schemes in WSN. In the proposed IDSHT scheme, a multi-dimensional two-tier hierarchical trust-based mechanism is adopted, which includes interactive trust, honesty trust, and content trust for cluster head selection during data aggregation. The IDSHT scheme supports the WSN dynamic environment, transition state of nodes, and variation in trust values. IDSHT includes both direct evaluations for trust calculation in a fixed hop range. The trust evaluation is maintained at two levels, where the multidimensional trust of the sensor node is maintained by the cluster head and the multidimensional trust of the cluster head is calculated from the base station and cluster head interaction, feedback evaluation from one-hop neighbors, and interactions with other cluster heads. The honesty trust is calculated using the number of successful and unsuccessful interactions between the two

nodes. The content trust is calculated based on the observing data by cluster heads and it is a network relates to trust. The interactive trust is evaluated by calculating the number of interactions between the nodes and cluster heads.

In future, we intend to implement the proposed scheme in a real test-bed.

## VII. FUTURE WORK

In the future, we intend to implement all the algorithms in a real test-bed using the above metrics.

## DECLARATION OF INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

## AUTHORS' CONTRIBUTIONS

All authors contributed and approved the final manuscript.

## DATA AVAILABILITY

The raw data of the IoT devices used to support the findings of this study are available from the corresponding author upon request.

## CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

## REFERENCES

- [1] Y. Yuan, L. Huo, Z. Wang, and D. Hogrefe, "Secure APIT localization scheme against Sybil attacks in distributed wireless sensor networks," *IEEE Access*.vol. 6, pp. 27629-27636, 2018.
- [2] R. Priyadarshi, B. Gupta, and A. Anurag, "Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues," *The Journal of Supercomputing*, pp. 1-41, 2020.
- [3] Y.-G. Yue and P. He, "A comprehensive survey on the reliability of mobile wireless sensor networks: Taxonomy, challenges, and future directions," *Information Fusion*.vol. 44, pp. 188-204, 2018.
- [4] J. Tang, A. Liu, J. Zhang, N. N. Xiong, Z. Zeng, and T. Wang, "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks," *Sensors*.vol. 18, no. 3, p 751, 2018.
- [5] J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," *IEEE Access*.vol. 7, pp. 33859-33869, 2019.
- [6] A. G. Finogeev and A. A. Finogeev, "Information attacks and security in wireless sensor networks of industrial SCADA systems," *Journal of Industrial Information Integration*.vol. 5, pp. 6-16, 2017.
- [7] M. Ge, K.-K. R. Choo, H. Wu, and Y. Yu, "Survey on key revocation mechanisms in wireless sensor networks," *Journal of Network and Computer Applications*.vol. 63, pp. 24-38, 2016.
- [8] T. C. Jesus, P. Portugal, F. Vasques, and D. G. Costa, "Automated methodology for dependability evaluation of wireless visual sensor networks," *Sensors*.vol. 18, no. 8, p 2629, 2018.
- [9] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies*.vol. 26, no. 2, pp. 107-130, 2015.
- [10] Z. Ye, T. Wen, Z. Liu, X. Song, and C. Fu, "An efficient dynamic trust evaluation model for wireless sensor networks," *Journal of Sensors*.vol. 2017, 2017.
- [11] S. Sharma and S. K. Jena, "Cluster based multipath routing protocol for wireless sensor networks," *ACM SIGCOMM Computer Communication Review*.vol. 45, no. 2, pp. 14-20, 2015.
- [12] X. Liu, "Atypical hierarchical routing protocols for wireless sensor networks: A review," *IEEE Sensors Journal*.vol. 15, no. 10, pp. 5372-5383, 2015.
- [13] R. Alasem, A. Reda, and M. Mansour, "Location based energy-efficient reliable routing protocol for wireless sensor networks," *Recent Researches in Communications, Automation, Signal processing, Nanotechnology, Astronomy and Nuclear Physics*, WSEAS Press, Cambridge, UK. pp. 180-185, 2011.
- [14] S. Roychowdhury and C. Patra, "Geographic adaptive fidelity and geographic energy aware routing in ad hoc routing," in: *Proceedings - international conference*, 1, pp. 309-313, 2010.
- [15] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks," *Wireless Networks*.vol. 8, pp. 169 - 185, 2002.
- [16] N. Alsaedi, F. Hashim, A. Sali, and F. Z. Rokhani, "Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)," *Computer communications*.vol. 110, pp. 75-82, 2017.
- [17] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*.vol. 6, pp. 6975-7004, 2018.
- [18] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Transactions on Wireless Communications*.vol. 15, no. 5, pp. 3718-3731, 2016.
- [19] P. Sinha, V. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," in: *Proceedings - 2017 International Conference on Signal Processing and Communication (ICSPC)*, pp. 288-293, 2017.
- [20] H.-J. Liao, C.-H. R. 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, 2013.
- [21] I. S. Gawdan and Q. I. Sarhan, "Performance Evaluation of Novel Secure Key Management Scheme over BAN Wireless Sensor Networks," *Journal of University of Duhok*.vol. 19, no. 1, pp. 179-188, 2016.
- [22] A. Khan, S. W. Shah, A. Ali, and R. Ullah, "Secret key encryption model for Wireless Sensor Networks," in: *Proceedings - 2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 809-815, 2017.
- [23] D. H. Kurniawan and R. Munir, "Double Chaining Algorithm: A secure symmetric-key encryption algorithm," in: *Proceedings - 2016 International Conference On Advanced Informatics: Concepts, Theory And Application (ICAICTA)*, pp. 1-6, 2016.
- [24] B. Mbarek and A. Meddeb, "Energy efficient security protocols for wireless sensor networks: SPINS vs TinySec," in: *Proceedings - 2016 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1-4, 2016.
- [25] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless personal communications*.vol. 69, no. 2, pp. 805-826, 2013.
- [26] F. M. Zegers, M. T. Hale, J. M. Shea, and W. E. Dixon, "Reputation-Based Event-Triggered Formation Control and Leader Tracking with Resilience to Byzantine Adversaries," in: *Proceedings - 2020 American Control Conference (ACC)*, pp. 761-766, 2020.
- [27] R. Mitchell and R. Chen, "A survey of intrusion detection in wireless network applications," *Computer Communications*.vol. 42, pp. 1-23, 2014.
- [28] S. Alneyadi, E. Sithirasanen, and V. Muthukkumarasamy, "Detecting data semantic: a data leakage prevention approach," in: *Proceedings - 2015 IEEE Trustcom/BigDataSE/ISPA*, 1, pp. 910-917, 2015.
- [29] H. Tawalbeh, S. Hashish, L. Tawalbeh, and A. Aldairi, "Security in Wireless Sensor Networks Using Lightweight Cryptography," *Journal of Information Assurance & Security*.vol. 12, no. 4, 2017.

# Factors Influencing the Use of Wireless Sensor Networks in the Irrigation Field

Loubna HAMAMI<sup>1</sup>, Bouchaib NASSEREDDINE<sup>2</sup>

Computer, Networks, Mobility and Modeling Laboratory  
Faculty of Sciences and Technology, Hassan 1st University, Settat, Morocco

**Abstract**—Battle control, natural disasters discovery, water monitoring, smart homes, agricultural applications, health care, weather forecasts, smart buildings, intrusion detection, medical devices, and more are the application areas of wireless sensor networks (WSNs). WSNs can help bring about revolutionary changes in important areas of our world. As a result, this technology has become a particularly interesting technology, which can be used to meet the specific requirements of a particular application because of its distinctive characteristics. In this context, WSNs are a promising approach in the agricultural sector and irrigation in particular for overcoming the world's major problems (e.g., the global water crisis). When implementing WSN in the irrigation field, many factors, like limited sensor node resources, limited sensor node power, costs, hardware constraints, and type of deployment environment, must be taken into account in order to improve WSN performance and achieve the desired results. In this paper, we will study and analyze the main factors that affect WSNs in the irrigation field. We will also provide a set of measures and solutions that need to be taken to overcome the challenges of deploying a WSN in irrigation. In this regard, we will also highlight several factors for improvement to achieve an efficient and consistent irrigation system using WSN.

**Keywords**—Cost; energy consumption and management; irrigation; smart irrigation; wireless sensor network; WSN deployment

## I. INTRODUCTION

The need to control and supervise hostile or remote environments, reducing the size, the availability of a wide range of diverse sensor types. In addition to the three basic functions performed by the sensor network [1], [2], i.e., computation, detection, and communication, and the features provided by WSNs [3]-[5], e.g., dynamic topology, scalability, self-monitoring, and flexibility. All this has led to the involvement and development of WSNs as a potential application in various domains [6]-[8] like medical, industry, environment, agriculture, and military. Wireless sensor networks have been deployed in several agricultural applications to support agricultural services [2], [9], [10] (e.g., pesticide spraying, irrigation, horticulture, and fertilization) and improve agricultural production. One of the most vital services in the agricultural domain is irrigation, as irrigation is an indispensable element in this domain and plays a very significant role in improving yields and raising agricultural production [11], [12]. Therefore, irrigation is considered one of the most agricultural services where WSNs are applied successfully to realize numerous gains and provide economical and effective solutions for water utilization efficiency and

water saving, thus helping to alleviate the world water crisis [13].

WSNs have been widely used in the irrigation field, and this usage has been greatly appreciated in recent years. A set of research and works focused on the application of WSN to control and manage irrigation practices has been identified from the literature and discussed in [13]. Avatade and Dhanure [14] have developed an automated irrigation system using WSN, an ARM microcontroller, and GPRS. This system is designed based on an integrated platform that uses the ARM microcontroller to control the water irrigation system. It can measure and monitor the soil moisture level and temperature through multiple ARM microcontroller-based wireless sensor nodes. Moreover, it enables remote monitoring of the status of the sensors used. Applications for irrigation systems using WSN and ZigBee have been proposed in [15]-[18]. The system proposed by Angelopoulos et al. [16] consists of IRIS motes employed for electro-valves control and TelosB motes equipped with EC-5 and SHT11 sensors that monitor a set of environmental conditions. Domestic irrigation was demonstrated in this work. An automatic irrigation system was proposed by Chikankar et al. [17] based on monitoring a set of the parameters through the usage of WSN and ZigBee. This includes LM-35, SY-HS-220, and soil moisture sensors that measure temperature, air humidity, and soil moisture. Other applications of WSN have been proposed in irrigation systems using GPRS and ZigBee technologies in [19], [20]. An automated irrigation system using WSN and other technologies to optimize and manage water use for agricultural crops was proposed by Gutiérrez et al. [19]. This system is composed of a control unit to store, evaluate, and identify the collected data, and to manage the automatic activation of irrigation using a developed. It is also composed of a distributed wireless network with numerous temperature and moisture sensors to monitor and control soil parameters. A sprinkler irrigation automation system using a WSN was designed by Nagarajan and Minu [20]. Besides, this system uses ZigBee technology for transmitting data and GPRS technology for storing and analyzing data. A system for improving the management of a variable rate irrigation system based on WSN has been presented that uses a system for identifying the criteria for placement of moisture sensors [21]. In [22], a WSN-based automated irrigation system has been proposed, explaining the workflow of the suggested system and illustrating the different relationships and interactions between the elements of this system. Utilizing GSM, Raspberry Pi, and Wi-Fi technologies, an automatic water supply system has been proposed to well control a WSN-based irrigation system [23]. In this system, a

set of sensors is used to monitor and detect the soil moisture, soil water level, and daylight intensity. The measured data is sent as a digital signal via Wi-Fi to the Raspberry Pi. The use of smartphones in WSN-based irrigation systems has also been presented in [24], [25]. An automated irrigation sensor was developed by Jagüey et al. [25], which allows the capture and processing of digital soil images based on the use of smartphones. An application for smartphones was also developed by Bartlett et al. [24] with the aim of extending the use of cloud-based irrigation scheduling. This app provides a quick visualization of weather measurements and soil water deficit. Decision support systems for an irrigation system based on WSN have also been presented in [26], [27]. Khan et al. [27] presented a WSN-based decision support system for efficient water use. Irrigation management and outlier detection system using WSN that helps farmers to control the irrigation procedures of crops. A low-cost decision support system was also proposed by Viani et al. [26] to control the efficiency of the irrigation system and thereby save water.

The use of wireless sensor networks supports different areas of human life, including irrigation service practices. Nevertheless, a variety of factors influence the implementation and design of WSNs [28], like limited sensor node resources, limited sensor node power, costs, hardware constraints, and the type of environment. As a result, researchers are confronted with many issues and problems such as power consumption, location, architecture, deployment, and security [29]-[31] when implementing this type of network. Similarly, when implementing WSN in the irrigation field, we find that many factors are influencing this application that needs to be taken into consideration to improve the performance of WSN and achieve the desired results. However, available studies have not comprehensively and accurately addressed the factors affecting the use of wireless sensor networks in irrigation. To this end, this study aims to identify, study, and analyze the main factors that influence WSNs in the irrigation field. It also aims to provide a set of measures and solutions to be followed to overcome the challenges of designing and deploying a WSN in irrigation, while identifying improvement factors to achieve an efficient and consistent irrigation system using WSN. In this way, and through this work, we address the gaps in this area by presenting a study on the main factors affecting wireless sensor networks in the irrigation field. To conduct this study, the following research questions were considered: What are the main factors to consider when designing a wireless sensor network in the irrigation field? What measures and solutions should be taken? Are there any factors for improvement to achieve an efficient and consistent irrigation system using WSN?

Many studies and works have been presented in the irrigation field based on wireless sensor networks in recent decades. Therefore, it is significant to pay attention to the many factors that affect the use of WSNs in irrigation to improve the performance and achieve the desired results. The purpose of this paper is to provide a study and analysis of the main factors affecting WSN in the irrigation field. The paper is structured as follows. Section 1 provides an introduction. In Section 2, we present and explain the wireless sensor network technology. In Section 3, we highlight WSN technology's importance in the

irrigation field by showing the advantages of using this technology in irrigation. In Section 4, we identify, study, and analyze the main factors that need to be considered when designing a WSN in the irrigation field, while proposing a set of measures and solutions that need to be taken. In Section 5, we present a discussion and synthesis. A series of improvement factors in this context are presented in Section 6. Finally, Section 7 concludes the paper.

## II. SENSORS AND WIRELESS SENSOR NETWORK

### A. Wireless Sensor Network

WSNs are composed of a large number of detection elements, called sensor nodes, which communicate through wireless communication with each other for information interchange and processing in cooperation. Sensor nodes are widely deployed near or within the being studied phenomenon that are low-cost, autonomous, and low-power multifunctional nodes [28]. A WSN is a network of nodes that can together reveal the physical environment, especially remote or hostile environments, to control and monitor such environments. In general, the sensor network achieves three fundamental functions [1], [2]:

- Sensing and Detection; the nodes collect the necessary data.
- Calculation via programs, microcontroller, hardware, and algorithm.
- Communication; the nodes communicate between them and with base station as well as base station communicates to the controller.

In the WSN [28], [32]-[35], the sensor nodes are dispersed over the field in a sensor area where each node utilizes its capabilities to detect, collect, and route data to generate a global view of the monitored area. The collected data is digitized and these values are routed directly or through other nodes according to a multiple hop architecture to a collection point, called a base station, for further treatment. The base station also functions as a gateway node whenever there is a requirement to connect to the external network for decision-making and data analysis. Fig. 1 illustrates the architecture of WSN in agricultural applications.

### B. WSNs vs. Ad-hoc Networks

The WSN is a particular kind of Ad-hoc network. However, there are several reasons that make the difference between traditional wireless Ad-hoc networks and WSNs [36], [37]. The majority of Ad-hoc networks rely on the any-to-any communication model, while wireless sensor networks primarily are based on the communication model many-to-one. The nodes of the wireless sensor network collaborate to reach a targeted objective, whereas in an Ad-hoc network each node has its goal. WSN's topology is dynamic with frequent changes. The number of nodes in WSN is significantly higher than in Ad-hoc. Sensor nodes do not have any global identification (e.g., IP addresses) unlike nodes in Ad-hoc networks.

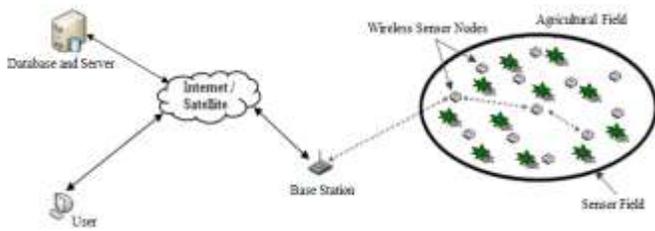


Fig. 1. Wireless Sensor Network Architecture for Agricultural Applications.

In addition, the energy consumption for sensor nodes is a determining factor, since these nodes have irreplaceable power sources because of their unassisted remote use in hostile environments. Unlike traditional Ad-hoc networks, the factor of the energy consumption is of secondary importance, since the batteries of the mobile units used can be easily replaced.

### C. WSN Characteristics

Certain of the key features of WSN [3], [5], [13] that have made it a potential tool in numerous agricultural services (e.g., pesticide spraying, fertilization, and irrigation) are as follows:

- Collaboration between sensor nodes to reach a target objective,
- Capacity to deal with node failures,
- Capacity to adapt to different environments,
- Heterogeneity of nodes deployed in WSN,
- Little or no infrastructure,
- Ability to operate unattended in remote or hostile areas,
- Dynamic topology,
- Detection and wireless communication,
- Scalability,
- Simple to utilize,
- A high number of sensor nodes, i.e., from a few tens to thousands.

### D. Sensor Nodes

As already mentioned above in Section 2.1, WSN is considered a distributed network of small-sized and inexpensive nodes having computing and processing resources. A sensor node is a microelectronic and microelectromechanical system that detects or measures a physical attribute (e.g., temperature and humidity) in a controlled environment and converts it into signals for monitoring and transmission [13], [28]. In general, sensor nodes emerge as miniaturized autonomous systems with advanced sensation capabilities and they are the core elements of WSN.

Since the sensor node is used in various applications, the appropriate choice of nodes requires many parameters such as the type of event to be detected, the nature of the event, the monitored environment, the nature of the signal emitted, and the cost.

As shown in Fig. 2, sensor node comprises four basic units [38], [39]:

- A sensing unit: This unit includes two subunits an Analog/Digital Converter (ADC) and a sensor. Sensor gets measurements of the monitored environment. An ADC converts the measured attribute and transmits it to the processing unit. This is the core unit of a sensor node.
- A processing unit: This unit is composed of a processor (i.e., computing unit) that perform simple calculations for collaboration with other nodes, in addition to a memory (i.e., storage unit) that integrates a specific operating system. The processing unit also ensures the analysis of the detected data.
- A transmission unit: This unit is used to connect the sensor node to WSN. It is responsible for all receptions and transmissions of acquired data in WSN through a wireless communication medium. It may be radio frequency type, e.g., MICA2 [40], or optical type, e.g., Smart Dust [41].
- A power unit: This unit is considered one of the critical elements of the sensor node. Each node is equipped with a battery to power all its components. Because of the small size of the node, the node battery is limited and generally irreplaceable.

Sensor node can add optional modules, e.g., an external memory, a location system, and a mobilization module, as well as its main components (listed above) if required. Fig. 2 shows the different components of a sensor node.

## III. ADVANTAGES OF WSN IN THE IRRIGATION FIELD

The use of WSN in the agriculture sector is now reaching an advanced level. There are many potential applications of WSN in the field of irrigation. In the following, we highlight the main advantages of utilizing WSNs in irrigation.

### A. Water Savings

The traditional irrigation practices employed only aim to control water distribution to the required places without compromising water needs, thereby losing a large amount of water in each irrigation process [11]. While we note that, the main objective of using WSNs in the irrigation field is to assure rational and efficient utilization of water, thereby achieving significant water savings.

Numerous works and research have proven that WSN is an ideal way to realize important water savings. Gutiérrez et al. [19] have shown that the utilization of WSN can lead to significant water savings in comparison to traditional irrigation practices of up to 90%. In another study conducted by González-Briones et al. [43], a 15.06% reduction in water consumption has been reported in automotive irrigation processes thanks to the use of WSN and the multi-agent system. Tests realized by Katyara et al. [44] have also reported successful results regarding the reduction of water utilized for irrigation, saving about 2150 cusecs of water per year. Other tests suggested by Difallah et al. [45] indicate a 28.51% water consumption reduction.

### B. Increasing Yields and Improving the Quality of Agricultural Production

When the right timing of irrigation is well defined, there is great potential to increase yields and improve the quality of agricultural production. While any delay in irrigation can lead to losses ranging from US\$ 62 / ha to US\$ 300 / ha [46]. Thus, another objective of using WSNs in the irrigation field is to determine the irrigation requirements in a particular area at the right time, thereby increasing yields and improving the quality of agricultural production.

The results of Abd El-kader and El-Basioni [47] showed an increase in potato yields and a 2 billion pounds loss was compensated in a year through the utilization of WSN in potato fields. Tests carried out by Katyara et al. [44] have also showed positive results in terms of increasing the productivity of agricultural land, i.e., an increase of about 20 to 25%. In another work by Khan and Kumar [48], it has been reported that the use of a mobile sink in WSN to supervise fields of ambient crops helps to increase crop yields. Nagarajan and Minu [20] have also concluded that a soil characteristics surveillance system utilizing a wireless sensor network to automate the sprinkler irrigation could improve yields with high quality and control water supply.

### C. Savings in Labor, Money, and Energy

Traditional irrigation systems on most farms require a lot of labor, money, and energy to operate properly. Farmers are always trying to undermine these three factors. The many benefits of the WSN have allowed it to provide cost-effective and efficient strategies to improve and support irrigation systems [13]. Thus, another objective of using WSN in the field of irrigation is to offer economical and efficient solutions, thereby achieving savings in labour, money, and energy.

Experimental studies were conducted by Khan and Kumar [48] to monitor ambient crop fields using a mobile sink in WSN. It was reported that reduction in energy consumption was 0.0115 Joules in the network. Işık et al. [50] have shown that important savings in energy and costs can be realized. Tests carried out by Nikolidakis et al. [51] have also showed an improvement in the lifetime of the WSN using the Equalized Cluster Head Election Routing Protocol, i.e., up to 1825 minutes.

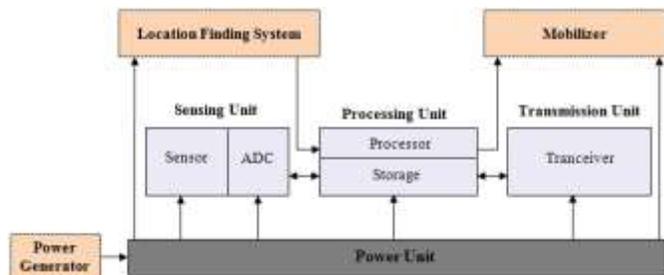


Fig. 2. Sensor Node Architecture.

## IV. FACTORS AFFECTING WSNs IN THE FIELD OF IRRIGATION

The recent years have been marked by a radical shift in the agricultural domain. Thanks to this change, new solutions have been found to develop and improve this domain, while solving its problems. The WSN is widely used successfully in various agricultural services, especially in irrigation service. This is mainly due to the importance of having an automated and accurate irrigation system, which helps maintain water resources and enhance the performance and efficiency of irrigation [13].

Nevertheless, in many scenarios, sensor nodes can be located in an unsupervised and open environment. In addition, agriculture can be practiced in agricultural fields of several hundred hectares and can encompass different climates, resources, and lands, which poses many implementation and design challenges. In this section, we discuss and analyze the main factors that need to be considered when designing WSN in the irrigation field, while proposing a set of measures and solutions to be taken. Fig. 3 shows the main factors affecting wireless sensor networks in irrigation.

### A. Placement of Sensor Node

The placement of sensor nodes according to the demanded needs is one of the critical factors in the design and implementation of WSN in the field of irrigation. It serves a very important role in ensuring that the wireless sensor network operates reliably and independently. Therefore, great care should be taken when placing the sensor nodes in the area to be irrigated, so that the sensor is placed at the proper location and height to measure the parameters without obstructions and in such a way that the area to be irrigated must be completely covered. In addition, suitable devices (i.e., fixture) must be installed to support the nodes to avoid the node position change that could result from rainwater, water currents, and strong winds.



Fig. 3. Main Factors Affecting WSN in the Irrigation Field.

In the area to be irrigated, soil moisture sensors should be placed, for example, as near to the soil as possible to obtain precise measurements, thus starting the irrigation process if the soil moisture is lower than the threshold values. Whereas air temperature sensors should be in an elevated location to correctly measure air temperature. Moreover, to manage properly the position of each node in the area to be irrigated, an appropriate method of deploying sensor nodes in WSN is necessary.

#### B. Sensor Node Housing

In the area to be irrigated, the deployed sensor nodes may be damaged due to human or animal abuse and may also be subject to a variety of harsh environmental conditions, e.g., strong winds, extreme heat, extreme cold, high pressure, and rainwater. Therefore, the sensor nodes must be enclosed in a protective housing that enables them to withstand the above-mentioned conditions as much as possible.

In addition, the housing used must be adapted and designed in such a way that its internal components never exceed a temperature higher than that which the nodes' batteries can withstand under realistic circumstances. It is recommended to utilize a means of internal temperature control and double-walled construction in the housing used to improve the efficiency of irrigation systems based on WSNs [52].

#### C. Sensor Node Size and Deployment

The size of the sensor node is another factor that plays a very important role in the design and implementation of WSNs in the field of irrigation. Therefore, that it must be small and suitable for deployment in the area to be irrigated.

To increase the performance of WSN-based irrigation systems, an appropriate method of deploying sensor nodes is necessary to manage correctly the position of each node in the area to be irrigated. The deployment of sensor nodes can be deterministic or random [53]-[55]. With deterministic deployment, sensor nodes propagate into pre-defined locations. Random deployment enables sensor nodes to be randomly deployed, typically in large-scale areas with inaccessible or unknown details. Deployment in WSN of large numbers of nodes makes these nodes vulnerable to failure. Thus, maintaining the sensor network topology before, during, and after deployment is a very complicated task that requires good management [28].

#### D. Fault Tolerance

Another critical factor in the design and implementation of WSNs in the field of irrigation is fault tolerance. Fault tolerance is the ability to retain the functionalities of the sensor network in the event of a failure, due to a fault in one or more nodes, without interruption [28], [56]. Given that in the area to be irrigated, a large number of sensor nodes are deployed in an open environment where these nodes may be damaged and/or fail. Sensor node failure in a WSN can arise for many reasons [57].

Sensor node dislocation, transmission link instability, environmental interference, battery depletion, defective sensor calibration, physical damage due to mishandling by humans or animals in agricultural land, software problems, extreme

environmental conditions, and failure of the node hardware components are among the important reasons that can cause node failure in a WSN-based irrigation system. Such failures, nevertheless, should not affect the functioning of the entire network, based on the fault tolerance principle that aims at improving the reliability and availability of WSNs [58]. Different fault-tolerance strategies, including clustering-based mechanisms, deployment-based mechanisms, and redundancy-based mechanisms, enhance network reliability [59]. Moreover, in large-scale deployments, data aggregation and topology management plans must be fault-tolerant.

In several irrigation scenarios [19], [20], [60], solar-powered sensor nodes were used to decrease the risk of node failure caused by battery depletion. In addition, in [19], node fault tolerance and communication failure were included for irrigation. The default irrigation program is followed, in the event of a problem.

#### E. Energy Consumption and Management

In WSN, a sensor node is composed mainly of four basic units: a sensing unit, a transmission unit, a power unit, and a processing unit. Event recognition and data transmission and processing are the main tasks of every sensor node [28]. An extra task of data routing can also be performed when it is a multi-hop network. Each of these functions consumes a lot of power. Typically, a sensor node has a restricted and limited power source, such as lithium or alkaline batteries, so the lifetime of a sensor node is largely dependent on the lifetime of the battery. Since a sensor node's battery supplies limited energy, it is critical to make sure that the power consumption of the node elements must be at a certain minimum. Minimizing the power consumption of the transmission unit, especially because it requires higher power consumption than other sensor node elements, can help alleviate this problem [51].

Energy is also an important factor in the design and implementation of WSN. Therefore, the management of energy is an essential part of any system that relies on wireless sensor networks, including irrigation systems. An adequate strategy of energy management (i.e., mechanisms and algorithms) can be implemented in both software and hardware to prolong the life of the battery by several additional months.

In irrigation scenarios, longer sensor node life can be achieved by also taking into account the use of available energy harvesting solutions [61]-[63] like wind power, thermal power, and solar power when designing WSN-based irrigation systems, a solution considered to be costly. Besides, sensor nodes can operate with replaced batteries because they are usually well-defined in terms of location and access [64].

#### F. Collection and Transmission of Data

In every detection, measurement, transmission, and processing of data, energy is expended, thus using up a large part of the battery life. Therefore, it is necessary to program improved and effective data aggregation techniques and sampling rates to ensure that energy is not wasted while collecting useful and pertinent data. Furthermore, acquiring data frequently will send a massive number of packets and this rapidly depletes the batteries. The data acquisition sampling

rate in the field of irrigation is generally not high. Nevertheless, it can be modified depending on the resources available for irrigation, the type of crops to be irrigated, and the environment.

To reduce the number of transmissions, a strategy for data transmission can also be developed, which saves energy, so that this strategy can involve intelligent data transmission, such as aggregated or modified values, and local storage of data in sensor nodes. In addition, implementing a sleep/wake-up feature can improve the performance of the network through energy savings, so that transmitters are only woken up when necessary. Reliable communication links require sensor nodes to be located close to each other to guarantee reliable multi-hop communication. Nevertheless, the characteristics of the land to be irrigated can be an obstacle to such reliable communication.

#### G. Cost of the System

In general, the final user, i.e., the farmer, looks at the cost and if he can bear it. Therefore, the budget for an irrigation system based on WSN is seen as one of the key priorities towards efficient utilization of the WSN. The total cost of sensor node hardware and software is a very significant factor when designing a WSN in the irrigation field.

Sensor node design for irrigation applications must be inexpensive while showing good performance. Therefore, it is always preferable to design a low-cost application so that it is available for usage by the markets of low and middle-income countries (LMIC) through minimizing the cost of software and hardware and optimizing system output [10].

### V. SYNTHESIS AND DISCUSSION

Traditional irrigation is the common method used by the majority of farmers to irrigate agricultural land, which lacks efficient use of available resources (e.g., water). While smart irrigation is a knowledge-based method that offers flexible and reliable irrigation possibilities to farmers. It allows adapting irrigation schedules and durations to meet the specific needs of each crop through real-time monitoring. These systems greatly improve the efficiency of irrigation water use and reduce labor and time, etc.

To develop and improve irrigation systems, a range of needs and requirements must be taken into consideration including:

- It is necessary to collect soil and crop information,
- Weather information should also be collected,
- It must gather information on crop growth,
- There are different types of crops in a single field,
- Water requirements for irrigation vary depending on crop needs,

- The needs of each crop vary according to soil and weather conditions,
- Proposal and development of proactive solutions for the irrigation system,
- The condition of irrigation system equipment and components should be monitored.
- The location of irrigation system components should also be monitored.

To achieve this objective (i.e., improvement and development of irrigation systems), it is necessary to find a solution that can automate these systems and allows intelligent decision-making in order to obtain an application and processing with a parallel and distributed feature.

Sensors are the most commonly used devices in the physical and environmental data collection scenario. Especially in the field of irrigation, sensors are used to measure and detect different data according to the necessities [42] (e.g., sensors are used to measure water level, temperature sensors, humidity sensors, soil moisture sensors, and density sensors). The detected and collected data by sensors make it possible to characterize and identify the controlled environment and their status. These data are very useful for developing and improving irrigation systems. Therefore, the wireless sensor network is considered one of the most useful technologies in various applications when it is necessary to collect and process data from the environment, and thus WSN can play a vital role in irrigation management [2], [9], [10], [49] and obtain several benefits according to all the specific characteristics of this network. All of this leads us to consider WSN as a high-priority way to collect, process, and monitor critical information and react to various situations in irrigation systems [13].

The WSN-based irrigation system includes several techniques and tools utilized to automate and monitor irrigation processes in real-time. Fig. 4 shows an illustration of an automated irrigation system using WSN and its components, which we suggested in our previous work [22].

WSNs have attracted worldwide attention in recent years, making them widely and successfully used in various irrigation systems. Above, we have discussed and analyzed several key factors to consider when deploying and designing WSN in agricultural lands to be irrigated, some of which are cost, node location, energy consumption and management, sensor node size, and fault tolerance, as well as a set of measures to overcome these. In Table I, we summarize a set of factors and proposed measures to overcome the challenges of designing and deploying a WSN in the irrigation field.

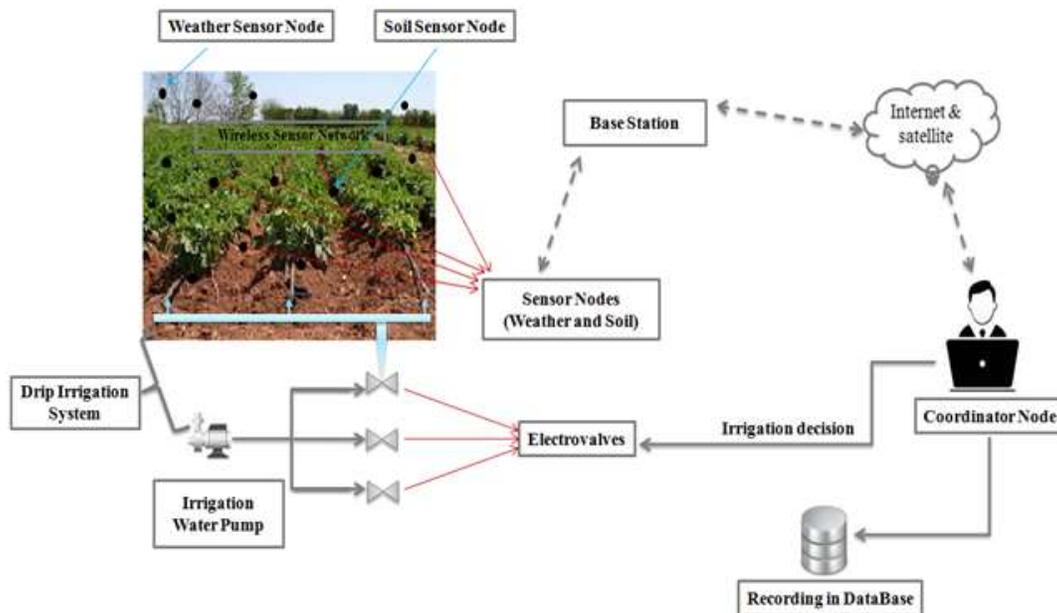


Fig. 4. Schematic Diagram of the Design for an Automated Irrigation System using WSN [22].

TABLE I. FACTORS AFFECTING WSN IN IRRIGATION AND PROPOSED MEASURES

Factors influencing	Causes of problems	Measures / Proposed solutions
Placement of Sensor Node	<ul style="list-style-type: none"> <li>• Sensor nodes incorrectly placed in the area to be irrigated</li> <li>• Change of sensor node position after deployment</li> </ul>	<ul style="list-style-type: none"> <li>- Place the sensor node in the appropriate position and height</li> <li>- Installing node support devices to prevent any change in position</li> <li>- Appropriate deployment method for sensor nodes to correctly manage the position of each node</li> </ul>
Sensor node housing	<ul style="list-style-type: none"> <li>• Damage to deployed sensor nodes due to human or animal abuse</li> <li>• Exposure of deployed sensor nodes to extreme environmental conditions (e.g. strong winds and rain)</li> </ul>	<ul style="list-style-type: none"> <li>- Enclosing the sensor node in a protective housing</li> <li>- Design of the housing used in such a way that the internal contents of this do not reach very high temperatures</li> <li>- Use of an internal temperature control system</li> <li>- Use of a double-walled construction</li> </ul>
Sensor node deployment and size	<ul style="list-style-type: none"> <li>• Node size</li> <li>• Network deployment problem</li> <li>• Dynamic network topology</li> </ul>	<ul style="list-style-type: none"> <li>- Sensor node should be designed small and suitable to be deployed in the area to be irrigated</li> <li>- Appropriate deployment method for sensor nodes</li> <li>- Random deployment / Deterministic deployment</li> <li>- Topology maintenance of the sensor network before, during and after deployment</li> </ul>
Fault tolerance	<ul style="list-style-type: none"> <li>• Sensor node dislocation</li> <li>• Communication failure</li> <li>• Physical damage &amp; Blockage</li> <li>• Resource depletion (e.g., energy)</li> <li>• Extreme environmental conditions</li> <li>• Environmental interference</li> </ul>	<ul style="list-style-type: none"> <li>- Clustering-based mechanisms</li> <li>- Redundancy-based mechanisms</li> <li>- Deployment-based mechanisms</li> <li>- Tolerance of data aggregation and topology management schemes in large-scale deployment</li> <li>- Use of solar-powered sensor nodes to reduce node battery depletion</li> </ul>
Energy consumption and management	<ul style="list-style-type: none"> <li>• Data detection</li> <li>• Data processing</li> <li>• Data transmission</li> <li>• Data routing</li> <li>• Restricted and limited power source</li> </ul>	<ul style="list-style-type: none"> <li>- Appropriate energy management strategy to prolong the life of the battery</li> <li>- Utilization of available energy harvesting solutions such as wind, thermal, and solar energy</li> <li>- Sensor nodes with replaced batteries</li> </ul>
Collection and transmission of data	<ul style="list-style-type: none"> <li>• Data detection</li> <li>• Too much power consumption by the transmission unit</li> <li>• Unreliable communication links due to the characteristics of the land to be irrigated</li> </ul>	<ul style="list-style-type: none"> <li>- Data aggregation techniques and sampling rates</li> <li>- Data transmission strategy to reduce the number of transmissions</li> <li>- Implementation of a sleep/wake mode for sensor nodes</li> <li>- Placement of sensor nodes in close proximity to each other to ensure reliable multi-hop communication</li> </ul>
Cost of the system	High cost of hardware and software used	<ul style="list-style-type: none"> <li>- Design of low-cost, high-performance sensor nodes for irrigation applications</li> <li>- Reduction of software and hardware costs</li> </ul>

## VI. IMPROVEMENT FACTORS

Looking ahead, we must pay more attention to several factors related to irrigation solutions based on wireless sensor networks to achieve an efficient and consistent irrigation system. Below, we highlight the most important of these factors, as shown in Fig. 5.

### A. Efficient use of Energy

As mentioned in Section 4.5, an important issue in irrigation systems using wireless sensor networks is the management of energy. Therefore, future solutions must also become more energy efficient through the integration of intelligent algorithms to ensure a longer lifetime of the system.



Fig. 5. Key Improvement Factors Associated with WSN-based Irrigation Solutions.

### B. Cost

The high materials, programs, and systems costs related to wireless sensor networks, where equipment imported from abroad is used, is the major obstacle to the utilization of WSN in irrigation in LMICs. Therefore, we see an urgent need for cost-effective solutions to raise the application of WSN in irrigation to enhance its widespread utilization and access among farmers and stakeholders. In this context, current efforts in development and research should focus on decreasing software and hardware costs while at the same time improving system performance, which would decrease the total cost of a WSN-based irrigation system; thus, making these systems available to markets in LMICs.

### C. System Maintenance

As mentioned earlier, the high overall cost of an irrigation system based on a WSN is one of the primary barriers to the widespread use of WSN in the field of irrigation. In addition to lowering the software and hardware costs used in wireless sensor networks, low system maintenance is required. An irrigation system based on a wireless sensor network must be designed with maintenance as low as possible, which will definitely reduce the average total cost over the long term.

### D. Autonomous Functioning

Autonomous functioning is a very important feature that allows for simple and advanced operation in most WSN-based irrigation applications, especially in remote areas to be

irrigated. Therefore, future WSN-based irrigation solutions must incorporate the ability to continue to operate autonomously without control while extending the period of autonomous operation for a longer period.

### E. Intelligence Factor and Real-time Monitoring

Many crops are sensitive to climatic conditions, which require farmers to closely and continuously monitor changing weather conditions to avoid unexpected problems in the farmland to be irrigated. Thus, in addition to an autonomous functioning, future solutions for WSN-based irrigation must also be developed with inherent intelligence with real-time monitoring capability to interact proactively to meet a variety of challenges such as yield improvement, real-time response, and energy conservation.

### F. Ease of use

In most cases, the final users of irrigation applications are nontechnical individuals. Therefore, future irrigation solutions based on the WSN should provide simple, easy-to-use applications for effective communication with the end-user. Besides, elements of these solutions, such as the communication interface, must be comprehensible, simple, and easy to operate.

### G. Comprehensive Planning and Robust Architecture

Because of the large number of different nodes distributed over the WSN, it must be deployed on farmland to be irrigated according to a carefully defined plan. In future irrigation solutions based on the WSN, comprehensive planning and robust fault tolerant architecture, taking into account the structure of the farmland and the needs of the farmers, will be essential to ensure long-term operation while minimizing costs and improving system performance.

## VII. CONCLUSION

Irrigation is a context-rich field in which the potential for utilizing wireless sensor network technology lies very large. Adapting irrigation systems that use WSNs on a large scale necessitates paying attention to many factors that affect the use of WSN in irrigation, in order to efficiently use available resources (e.g., water) while improving performance and achieving desired results. This paper attempted to address the gaps in this area by presenting a study on the main factors affecting wireless sensor networks in the irrigation field, as we have not found studies that accurately and adequately address the factors that affect this type of application. The present paper presents a study and an analysis of the main factors that influence WSN in the irrigation field. It presents a set of measures and solutions that need to be followed to overcome the challenges of designing and deploying WSN in irrigation. A number of improvement factors have also been identified to achieve an efficient and consistent irrigation system using WSN. In addition, the importance of WSN technology in irrigation was highlighted by outlining the advantages of this application.

## REFERENCES

- [1] L. Hamami and B. Nassereddine, "Integration of irrigation system with wireless sensor networks: prototype and conception of intelligent irrigation system," In Lecture Notes in Engineering and Computer Science, vol. 2238, pp. 56–62, Newswood Limited, 2018.

- [2] A. Ur Rehman, A. Z. Abbasi, N. Islam, and Z. A. Shaikh, "A review of wireless sensors and networks' applications in agriculture," *Computer Standards & Interfaces*, vol. 36, no. 2, pp. 263-270, 2014.
- [3] S. Mishra and H. Thakkar, "Features of WSN and Data Aggregation techniques in WSN: A Survey," *Int. J. Eng. Innov. Technol. (IJEIT)*, vol. 1, no. 4, pp. 264-273, 2012.
- [4] P. Bakaraniya and S. Mehta, "Features of wsn and various routing techniques for wsn: a survey," *International Journal of Research in Engineering and Technology*, vol. 1, no. 3, pp. 349-354, 2012.
- [5] M. S. Manshahia, "Wireless sensor networks: a survey," *International Journal of Scientific & Engineering Research*, vol. 7, no. 4, pp. 710-716, 2016.
- [6] R. E. Mohamed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Survey on wireless sensor network applications and energy efficient routing protocols," *Wireless Personal Communications*, vol. 101, no. 2, pp. 1019-1055, 2018.
- [7] T. Arampatzis, J. Lygeros, and S. Manesis, "A survey of applications of wireless sensors and wireless sensor networks," *Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control*. IEEE, pp. 719-724, 2005.
- [8] J. A. Stankovic, A. D. Wood, and T. He, "Realistic applications for wireless sensor networks," *Theoretical Aspects of Distributed Computing in Sensor Networks*, Monographs in Theoretical Computer Science, An EATCS Series, Chapter 25, Springer-Verlag Berlin Heidelberg, pp. 835-863, 2011.
- [9] D. Thakur, Y. Kumar, A. Kumar, and P. K. Singh, "Applicability of wireless sensor networks in precision agriculture: A review," *Wireless Personal Communications*, vol. 107, no. 1, pp. 471-512, 2019.
- [10] T. Ojha, S. Misra, and N. S. Raghuvanshi, "Wireless sensor networks for agriculture: the state-of-the-art in practice and future challenges," *Comput. Electron. Agric.* vol. 118, pp. 66-84, 2015.
- [11] L. Hamami and B. Nassereddine, "Towards a smart irrigation system based on wireless sensor networks (WSNs)," In : *Proceedings of the 1st International Conference of Computer Science and Renewable Energies - Volume 1: ICCSRE*, ISBN 978-989-758-431-2, pp. 433-442, SciTePress Digital Library, 2018.
- [12] FAO, IFAD, UNICEF, WFP and WHO. The state of food security and nutrition in the world 2018: Building climate resilience for food security and nutrition. Rome, FAO, 2018.
- [13] L. Hamami and B. Nassereddine, "Application of wireless sensor networks in the field of irrigation: A review," *Comput. Electron. Agric.*, vol. 179, pp. 105782, 2020.
- [14] S. S. Avatade and S. P. Dhanure, "Irrigation system using a wireless sensor network and GPRS," *International Journal of Advance Research in Computer and Communication Engineering*, vol. 4, no. 5, pp. 521-524, 2015.
- [15] M. Dursun, and S. Ozden, "A wireless application of drip irrigation automation supported by soil moisture sensors," *Scientific Research and Essays*, vol. 6, no. 7, pp. 1573-1582, 2011.
- [16] C. M. Angelopoulos, S. Nikolettseas, and G. C. Theofanopoulos, "A smart system for garden watering using wireless sensor networks," In: *Proceedings of the 9th ACM international symposium on Mobility management and wireless access*, pp. 167-170, 2011.
- [17] P. B. Chikankar, D. Mehrete, and S. Das, "An automatic irrigation system using ZigBee in wireless sensor network," In: *2015 International Conference on Pervasive Computing (ICPC)*. IEEE, pp. 1-5, 2015.
- [18] Y. Zhou, X. Yang, L. Wang, and Y. A. Ying, "wireless design of low-cost irrigation system using ZigBee technology," In: *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*. IEEE, vol. 1, pp. 572-575, 2009.
- [19] J. Gutiérrez, J. F. Villa-Medina, A. Nieto-Garibay, and M. Ángel Porta-Gándara, "Automated irrigation system using a wireless sensor network and GPRS module," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 1, pp. 166-176, 2014.
- [20] G. Nagarajan and R. I. Minu, "Wireless soil monitoring sensor for sprinkler irrigation automation system," *Wireless Personal Communications*, vol. 98, no. 2, pp. 1835-1851, 2018.
- [21] W. Zhao, J. Li, R. Yang, and Y. Li, Y., "Determining placement criteria of moisture sensors through temporal stability analysis of soil water contents for a variable rate irrigation system," *Precision Agriculture*, vol. 19, no. 4, pp. 648-665, 2018.
- [22] H. Loubna and N. Bouchaib, "Wireless sensor network application for intelligent irrigation system," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12 (3 Special Issue), pp. 163-173, 2020.
- [23] A. Imteaj, T. Rahman, M. K. Hossain, and S. Zaman, "IoT based autonomous percipient irrigation system using raspberry Pi," In: *2016 19th International Conference on Computer and Information Technology (ICCIT)*. IEEE, pp. 563-568, 2016.
- [24] A. C. Bartlett, A. A. Andales, M. Arabi, and T. A. Bauder, "A smartphone app to extend use of a cloud-based irrigation scheduling tool," *Computers and Electronics in Agriculture*, vol. 111, pp. 127-130, 2015.
- [25] J. G. Jagüey, J. F. Villa-Medina, A. López-Guzmán, and M. A. Porta-Gándara, "Smartphone irrigation sensor," *IEEE Sensors journal*, vol. 15, no. 9, pp. 5122-5127, 2015.
- [26] F. Viani, M. Bertolli, M. Salucci, and A. Polo, "Low-cost wireless monitoring and decision support for water saving in agriculture," *IEEE Sensors Journal*, vol. 17, no. 13, pp. 4299-4309, 2017.
- [27] R. Khan, I. Ali, M. Zakarya, M. Ahmad, M. Imran, and M. Shoaib, "Technology-assisted decision support system for efficient water utilization: A real-time testbed for irrigation using wireless sensor networks," *IEEE Access*, vol. 6, pp. 25686-25697, 2018.
- [28] L. Hamami and B. Nassereddine, "A study of the main factors affecting wireless sensor networks," In: *2019 Third International conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC)*. IEEE, pp. 211-215, 2019.
- [29] A. J. Swati and R. Priyanka, "Wireless sensor network (WSN): Architectural design issues and challenges," *International Journal on Computer Science and Engineering*, vol. 2, no. 9, pp. 3089-3094, 2010.
- [30] E. P. K. Gilbert, B. Kaliaperumal, and E. B. Rajsingh, "Research issues in wireless sensor network applications: A survey," *International Journal of Information and Electronics Engineering*, vol. 2, no. 5, pp. 702, 2012.
- [31] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," In *2013 International Conference on Machine Intelligence and Research Advancement*. IEEE, pp. 58-62, 2013.
- [32] M. Tubaishat and S. K. Madria, "Sensor networks: an overview," *IEEE Potentials*, vol. 22, no. 2, pp. 20-23, 2003.
- [33] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE communications magazine*, vol. 40, no. 8, pp. 102-114, 2002.
- [34] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer networks*, vol. 52, no. 12, pp. 2292-2330, 2008.
- [35] I. F. Akyildiz and M. C. Vuran, *Wireless sensor networks*. Vol. 4. John Wiley & Sons, 2010.
- [36] C. Perkins, *Ad hoc networks*. Reading: Addison-Wesley, 2000.
- [37] V. Mhatre and C. Rosenberg, "Design guidelines for wireless sensor networks: communication, clustering and aggregation," *Ad hoc networks*, vol. 2, no. 1, pp. 45-63, 2004.
- [38] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393-422, 2002.
- [39] M. A. Matin and M. M. Islam, "Overview of wireless sensor network," *Wireless Sensor Networks-Technology and Protocols*, pp. 1-3, 2012.
- [40] Crossbow, *MICA2 Datasheet*. [Online]. Available on: [http://www.investigacion.frc.utn.edu.ar/sensores/equipamiento/wireless/MICA2\\_Datasheet.pdf](http://www.investigacion.frc.utn.edu.ar/sensores/equipamiento/wireless/MICA2_Datasheet.pdf), accessed December 2020.
- [41] Kristofer, Pister, *SmartDust*. [Online]. Available on: <http://robotics.eecs.berkeley.edu/~pister/SmartDust/>, accessed December 2020.
- [42] S. A. Kumar and P. Ilango, "The impact of wireless sensor network in the field of precision agriculture: a review," *Wireless Personal Communications*, vol. 98, no. 1, pp. 685-698, 2018.

- [43] A. González-Briones, Y. Mezquita, J. A. Castellanos-Garzón, J. Prieto, and J. M. Corchado, "Intelligent multi-agent system for water reduction in automotive irrigation processes," *Procedia Computer Science*, vol. 151, pp. 971-976, 2019.
- [44] S. Katyara, M. A. Shah, S. Zardari, B. S. Chowdhry, and W. Kumar, "WSN based smart control and remote field monitoring of Pakistan's irrigation system using SCADA applications," *Wireless Personal Communications*, vol. 95, no. 2, pp. 491-504, 2017.
- [45] W. Difallah, K. Benahmed, B. Draoui, and F. Bounaama, "Linear optimization model for efficient use of irrigation water," *International Journal of Agronomy*, vol. 2017, 2017.
- [46] G. Vellidis, M. Tucker, C. Perry, C. Kvien, and C. Bednarz, "A real-time wireless smart sensor array for scheduling irrigation," *Comput. Electron. Agric.*, vol. 61, no. 1, pp. 44-50, 2008.
- [47] S. M. Abd El-kader and B. M. M. El-Basioni, "Precision farming solution in Egypt using the wireless sensor network technology," *Egyptian Informatics Journal*, vol. 14, no. 3, pp. 221-233, 2013.
- [48] T. H. F. Khan and D. S. Kumar, "Ambient crop field monitoring for improving context based agricultural by mobile sink in WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 4, pp. 1431-1439, 2020.
- [49] L. Ruiz-Garcia, L. Lunadei, P. Barreiro, and I. Robla, "A review of wireless sensor technologies and applications in agriculture and food industry: state of the art and current trends," *Sensors*, vol. 9, no. 6, pp. 4728-4750, 2009.
- [50] M. F. Işık, Y. Sönmez, C. Yılmaz, V. Özdemir, and E. N. Yılmaz, "Precision Irrigation System (PIS) using sensor network technology integrated with IOS/Android application," *Applied Sciences*, vol. 7, no. 9, pp. 891, 2017.
- [51] S. A. Nikolidakis, D. Kandris, D. D. Vergados, and C. Douligeris, "Energy efficient automated control of irrigation in agriculture by using wireless sensor networks," *Computers and Electronics in Agriculture*, vol. 113, pp. 154-163, 2015.
- [52] J. Balendonck, J. Hemming, B. A. J. Van Tuijl, L. Incrocci, A. Pardossi, and P. Marzalletti, "Sensors and wireless sensor networks for irrigation management under deficit conditions (FLOW-AID)," 2008.
- [53] H. Subir, G. Amrita, S. Sanjib, D. Avishek, and D. Sipra, "A lifetime enhancing node deployment strategy in WSN," In *International Conference on Future Generation Information Technology*. Springer, Berlin, Heidelberg, pp. 295-307, December 2009.
- [54] S. Mini, S. K. Udgata, and S. L. Sabat, "Sensor deployment and scheduling for target coverage problem in wireless sensor networks," *IEEE sensors journal*, vol. 14, no. 3, pp. 636-644, 2013.
- [55] G. Tuna, T. V. Mumcu, K. Gulez, V. C. Gungor, and H. Erturk, "Unmanned aerial vehicle-aided wireless sensor network deployment system for post-disaster monitoring," In *International Conference on Intelligent Computing*. Springer, Berlin, Heidelberg, pp. 298-305, July 2012.
- [56] I. F. Akyildiz and M. C. Vuran, *Factors influencing WSN design*, 2010.
- [57] M. Younis, I. F. Senturk, K. Akkaya, S. Lee, and F. Senel, "Topology management techniques for tolerating node failures in wireless sensor networks: A survey," *Comput. Networks*, vol. 58, no.1, pp. 254-283, 2014.
- [58] H. Alwan and A. Agarwal, "A survey on fault tolerant routing techniques in wireless sensor networks," In *2009 Third International Conference on Sensor Technologies and Applications*, IEEE, pp. 366-371, 2009.
- [59] G. Kakamanshadi, S. Gupta, and S. Singh, "A survey on fault tolerance techniques in wireless sensor networks," In *2015 international conference on green computing and internet of things (ICGCIoT)*. IEEE, pp. 168-173, October 2015.
- [60] N. G. Shah, U. B. Desai, I. Das, S. N. Merchant, and S. S. Yadav, "In-field wireless sensor network (WSN) for estimating evapotranspiration and leaf wetness," *Int. Agric. Eng. J.* vol. 18, no. 3-4, pp. 43-51, 2009.
- [61] J. M. Gilbert and F. Balouchi, "Comparison of energy harvesting systems for wireless sensor networks," *International Journal of automation and computing*, vol. 5, no. 4, pp. 334-347, 2008.
- [62] F. I. Simjee and P. H. Chou, "Efficient charging of supercapacitors for extended lifetime of wireless sensor nodes," *IEEE Trans. Power Electron.*, vol. 23, no. 3, pp. 1526-1536, 2008.
- [63] F. K. Shaikh and S. Zeadally, "Energy harvesting in wireless sensor networks: A comprehensive review," *Renewable and Sustainable Energy Reviews*, vol. 55, pp. 1041-1054, 2016.
- [64] H. M. Jawad, R. Nordin, S. K. Gharghan, A. M. Jawad, and M. Ismail, "Energy-efficient wireless sensor networks for precision agriculture: a review," *Sensors*, vol. 17, no. 8, pp. 1781, 2017.

# Deep Learning Algorithm for Classification of Cerebral Palsy from Functional Magnetic Resonance Imaging (fMRI)

## Classification of Cerebral Palsy from Functional Magnetic Resonance Imaging

Pradeepa Palraj<sup>1</sup>

Department of Electrical and Electronics Engineering, School of Engineering and Technology, Jain University, Bangalore, India

Gopinath Siddan<sup>2</sup>

Department Electronics and Communication Engineering Swarnandhra Institute of Engineering and Technology Andhra Pradesh, India

**Abstract**—Cerebral palsy is a disorder of neurology that may be caused by prenatal, perinatal or postnatal reasons that result in the failure of motor functioning in children besides mental well-being. Referring to the location of brain injury and the effect of it on the muscle tone, cerebral palsy is classified into subgroups namely spastic, non-spastic etc. Each type of palsy varies in symptoms and hence the therapy planning and rehabilitation are decided depending on the factors involved in each type. This urges the requirement of a suitable technique to classify the type of Palsy at the earlier stages to effectively plan therapy. Functional MRI of the neonatal brain helps in imaging and classification of cerebral palsy. The deep neural network is a subset of machine learning that is widely used in image classification applications. This technique is applied to the functional magnetic resonance brain images of infants to classify the type of cerebral palsy using a deep convolutional network of modified AlexNet architecture that helps the physician further in a planned rehabilitation to facilitate the lifestyle of the affected children.

**Keywords**—Cerebral palsy; deep neural network; functional magnetic resonance image

### I. INTRODUCTION

Cerebral palsy is a disorder in neurology caused due to non-progressive brain injury or any malformation due to underdevelopment of the brain in preterm infants. This primitively affects motor actions and muscle coordination. The World Health Organization (WHO) reports that 10% of the total population is estimated to be affected, by any of the types of cerebral palsy and 3.8% of Indian population is a victim of this neurological disorder [1]. Diagnosis of cerebral palsy is highly challenging in infants. The fMR image of a cerebral palsy affected infant is shown in Fig. 1. When there is any delay in the motor or cognitive responses during the growing phase of the child, cerebral palsy may be diagnosed. But diagnosis after the elapsing of the critical period will not be effective in rehabilitation. Early diagnosis of cerebral palsy at the infant level will help the physicians to plan for oculomotor rehabilitation, which suitably helps in the Neuroplasticity and eventually improves the lifestyle of the cerebral palsy affected child [2].

The scientific verity of the intellectual organ, namely brain can be demonstrated by neuroimaging techniques like Functional Magnetic Resonance Imaging (fMRI) and Positron Emission Tomography (PET) scans. The functional magnetic resonance imaging helps in recording the brain activity with respect to the changes occur because of the variation in the blood flow.

fMRI is also widely used to study on the reorganization of the neural connectivity after early brain injuries and also viewed as a most vital tool in investigating neuroplasticity. Recent research have proved that even though fMRI is widely used in adults, there are few challenges observed when used in children especially in infants with lack of head stability during scanning and excessive anatomical variations in whole brain mapping etc. This increases the complexity in analyzing the fMRI and also classifying accordingly [3].

The existing methods of classification of cerebral palsy widely use the cerebral magnetic resonance imaging techniques that are majorly dependent on the grades of severity in periventricular (PVL) anomalies. MRI based classification mainly focus on the irregular ventricular dilation, widening of the inter hemispheric fissure, long lasting hemorrhage. Some researchers have also attempted to classify cerebral palsy with respect to the motor abnormalities namely diplegia, dyskinesia, spastic etc. The results were promising and the classification accuracy was good when the experimentation carried is between ages 2 to 6. It is also observed that very limited approaches are available to classify palsy before the age of two. The study has also complemented that diagnosing and classification of cerebral palsy at earlier stages is challenging owing to the factors like gross motor functions cannot be analyzed for the infants under this age group [4].

This paper [5] aims at diagnosing cerebral palsy at the earlier stages of infant, preferably six to twelve weeks old by comparing the fMRI of these infants and their oculomotor responses. Further, to classify the type of cerebral palsy namely spastic, dyskinetic, ataxic and mixed cerebral palsy using deep neural network [6]. The obtained fMRI images are subjected to removal of noise using fuzzy adaptive filter and then the type of cerebral palsy is classified by the three layer deep neural

network trained with tensor flow. After the training phase the testing of the obtained images resulted in the classification of the type of Palsy with increased accuracy.

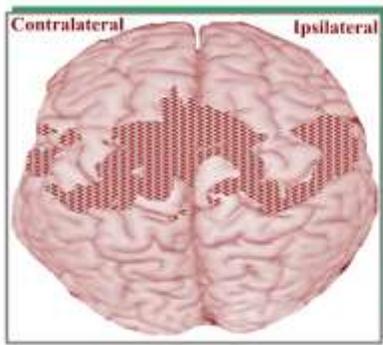


Fig. 1. FMR Image of Cerebral Palsy Affected Infant.

Section II of the paper discusses on the literature review and the research challenges existing in the classification of palsy. Section III describes the methodology of the proposed method and the results obtained are discussed in Section IV.

## II. LITERATURE REVIEW

First, Research on Cerebral Palsy has started in the early 1940's when Arnold E. Joyal indicated that Cerebral Palsy is one of the major reasons for the slow and poor growth in children. The factors that affect the cognitive functioning of children with a mean age of nine and affected with cerebral palsy were discussed by Paul E. Polani in 1958. Patricia Myers in 1965 reported the language disabilities in cerebral palsy affected children. M. V. Durkin et al in 1976 analyzed the history of the mentally retarded subjects to identify the pathogenesis of cerebral palsy. This work was also funded by USPHS Grants and the Wisconsin Department of Health's Grant to CWC - Central Wisconsin Colony and Training School in support of the Genetic Counseling Unit and CWC Diagnostic. Ruth Koheil et al in 1987 studied the effect of EMG auditory feedback training of the orbicularis oris using a biofeedback trainer and there was a considerable increase in the motor actions by the patients after the training.

In 1993, D. F. Parker et al. Measured the level of interrelation between the motor actions and the physiological fitness of the cerebral palsy affected children. Robert Palisano et al. in 2008 insisted on the necessity of a standardized system for gross motor function classification in children affected by cerebral palsy. Donna S. Hurley published a research registry on cerebral palsy in 2011 to fill the gap between the clinical research and the patients and to promote fruitful research in this area. Sophia Gosling, in 2016 reviewed the recent developments in the pediatric neuropsychological rehabilitation of cerebral palsy affected children. Kristine Stadskleiv in 2018 reviewed the neurophysiology profiles of the cerebral palsy affected children. Deepa Jeevanantham et al. in 2018 attempted the subgrouping of cerebral palsy affected children in developing two different body function index for them that aids in exploring the difference between the gross motor functions.

Anupam Gupta et al. in 2008 assessed the effectiveness of single stage multilevel soft tissue surgery for the CP affected

patients for their active locomotion. Ruchi Kothari et al. in 2010 investigated the connection between findings of BAEP and VEP abnormality with different clinical factors in children having spastic cerebral palsy. Vykuntaraju K Gowda et al. studied the clinical patterns, co-morbidities and predisposing factors of cerebral palsy affected children in 2015. The study was concluded that out of 100 affected children, 12% of hypotonic, 81% of spastic, 2% of mixed CP, and 5% of dystonic cases. The mean presentation age was 2 years, 2 months, and it is in the ratio of 1:2 for male to female. S Surender et al in 2016 focused on the cerebral palsy impact on HRQOL of children and their families, relationship with the dysfunction of gross motor [7, 8].

The rehabilitation council of Indian Academy of CP has acknowledged that there is positive growth in the medical interventions provided to CP affected patients. However, more scientific research and studies based on systematic documentation and validated reference materials in India may help the rehabilitation of the rural population.

But it is evident from the literature that the classification of the type of cerebral palsy from the fMRI analysis is challenging owing to the factors like the understanding of the functional connectivity of brain and requires much more investigations on the anatomical details regarding the classification on the type of Palsy [9, 10]. These real time challenges requires a robust method to analyse the fMRI obtained from the infants irrespective of the nonlinear and complex changes in the neurons and classify accurately to aid in the therapy planning that results in better rehabilitation planning at the earlier stages.

## III. METHODOLOGY

This research attempts to diagnose cerebral palsy at the earlier stages, particularly in the age group of six to sixteen months and also to classify the types of cerebral palsy [11] that helps in planning for better rehabilitation by overcoming the existing challenges in correlating the gross motor responses and the fMRI analysis. The overall flow of the proposed method is shown in the below Fig. 2.

### A. Overview

Functional Magnetic Resonance Imaging is used in measuring brain activity with respect to the blood flow measurement. This non-invasive imaging technique is capable of even detecting a small change associated with neuron activities. This imaging is based on the Blood Oxygen Level Dependency (BOLD) of the brain cells and widely used in medical diagnosis owing to the high spatial resolution in the activated brain regions, their visibility with respect to the neighboring cells. Repeated stimuli also help in eliminating the imaging noise much better than in normal MR images besides the fact that, fMR image quality is increased by using spin echo pulse in accordance with the magnetic field strength. The fMR images of the cerebral palsy affected children are acquired. The BOLD signal is highly complex and non-linear because of the transient changes in the neurons and vascular structures. The images are preprocessed for the removal of random and other noises acquired because of image acquisition and the subjects themselves, being a neonatal group.

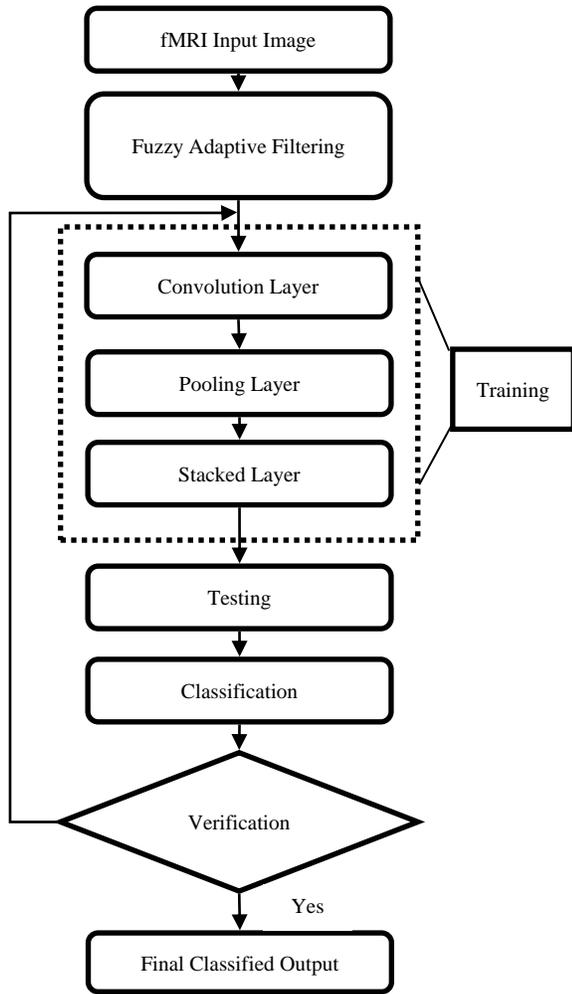


Fig. 2. Overall Flow of the Proposed Method.

Also, the amplitude of the thermal noise increases with respect to the strength of the magnetic field. Fuzzy adaptive median filters are used in eliminating the noise from these test images [12]. Fuzzy adaptive filters reduce the additive, salt and pepper or impulse noise, but preserve the image details compared to the adaptive median filters.

### B. Fuzzy Adaptive Filtering

Fuzzy adaptive filtering is a modified version of median filters that improve the visibility of an image by intensifying the smoothing effect besides removing the noise factors when compared to other traditional filtering techniques. This method involves the identification and comparison of each pixel in the input image and replacing the noise affected pixel with the median value according to the intensity of the local noise with increased flexibility. The intensity differences are measured using a sliding window function and the mean square error is calculated as follows,

$$MSE = \left[ \frac{1}{MN} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \hat{f}(m,n) - f(m,n) \right]^2 \quad (1)$$

The noise-free image is now fed into the training phase of the deep learning networks framed of convolution, pooled and

stacked layers and the architecture of the proposed method is shown in Fig. 3.

### C. Deep Learning

Computer Aided diagnosis plays a vital role in medical imaging since 1990 for the detection of micro calcifications, lung nodules, pulmonary embolism and mitotic cells. In the recent years Computer aided diagnosis uses the extended version as the convolution neural networks (CNN) in the classification of pancreas, brain tumor and other medical applications. The major advantage of CNN is the ability to transfer the data interpreted in the pre trained layers to the next level. This transfer learning ability of CNN can be used for two different applications in medical imaging. The first application uses the pre trained CNN to generate the features required for training phase. On the other hand the pre trained CNN can be used in image classification by replacing the fully connected pre trained CNN layers by the logistic layer and the training is done only for the newly added layers. LeNet, AlexNet and GoogLeNet are the three major CNN that is implemented widely in image analysis specifically in medical image classification. AlexNet was introduced in 2012 by Alex Krizhevsky et al with a unique feature of introducing non linearity into the network through ReLU during the training phase that increases the speed when compared with the saturating nonlinear function including hyperbolic and sigmoid functions. This paper uses the modified AlexNet architecture where the different stages of information processing in multiple hierarchical structures are implemented to improve the accuracy of classification. Another important advantage of using AlexNet is that it is used in overcoming the over fitting problem [21].

This paper uses a modified AlexNet with five convolution layers followed by pooling layer. The convolution layers aid in detecting the local features throughout the input image. The local structures are detected by connecting each node to a subset of spatially connected neurons. The similar image pattern is searched in each input image channel by enabling three connection weights shared between the nodes in the convolution layer called as kernels. The number of kernels depends on the number of parameters to be detected from the input layer. The hierarchical set of image features is attained by adding pooling layers in subsequent to the convolution layers. The max pooling layer helps in the reduced size by selecting the features in overlapping and non-overlapping neighborhood and eliminating the maximum responses. This also results in improved translation invariance. This is followed by the regression or softmax layer that generates the expected output. The BPN algorithm is used in training the CNN that effectively minimizes the cost function.

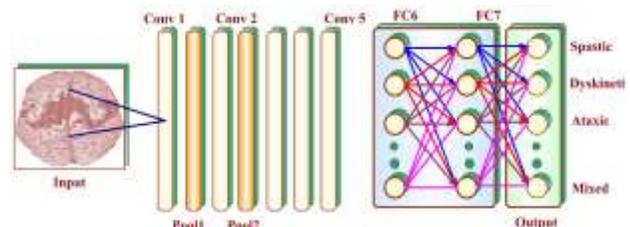


Fig. 3. Architecture of the Proposed Method.

The proposed method consists of five convolution layers followed by two fully connected layers. The kernel size, of the first convolution layer is 12 so that each unit of the feature map is mapped to 12 X 12 neighborhoods and this layer is to normalize the local response by convolving after every 4 pixels. This layer leads to 96 feature maps, followed by the pooling layer with a kernel size, of 6 and stride rate of 2. This layer is again followed by the convolution layer 2 with a kernel size, of 6 and stride rate of 2. Thus the pooled feature maps in each layer are convolved subsequently in the convolution layer and fed into the two fully connected layers for the rectified linear operation. This modified AlexNet results with 4096 feature maps for each image as tabulated in Table I.

TABLE I. SPECIFICATIONS OF PROPOSED CNN

Parameters	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5
Number of Filters	96	96	384	256	256
Kernel Size	12 X 12	6 X 6	6 X 6	3 X 3	3X 3
Stride	4	2	2	2	2
Learning Rate	0.02				
Weight Decay	0.0016				
Training Epochs	40-60				
No. of units in fully connected Layer					4096

Deep learning is a discipline of machine learning that is recently used in object recognition among a large volume of data. This is implemented effectively by rising the number of artificial neural network layers and each layer is designed to extract an exact feature that enhances the image classification[13, 14]. After preprocessing, the images are split into subclasses for calculating the gradient of the images in each data set, thereby reducing the voluminous data and parallel processing occurs to reduce the computational time. [15, 16].

Convolution neural networks (CNN) are widely used deep feed forward networks for image classification. CNN is more or less similar to feed forward neural networks, but the only difference between them is the connection pattern of the adjacent layers. CNN involves the connection of all nodes between the adjacent layers, whereas feed forward networks few nodes may be eliminated because of the complexity riveted in including too many parameters like over fitting, slow speed etc. This major challenge in feed forward networks is overcome by the CNN that includes kernel layers: convolution and pooling layers. The former layer uses only a portion of the previous layer as input in the size of preferably 3 X 3 or 5 X 5. But it deeply analyzes the limited input to gain maximum abstraction of the required features. The latter layer involves reducing the matrix size from the previous layers and hence minimizes the number of parameters in the entire network [17],[18]. This results in increased speed of computation and also avoids over fitting problems as in the case of feed forward networks.

1) *Convolution layer:* The features that are identified to represent the input images are extracted in this convolution layer which consists of neurons oriented to form the feature maps. These feature maps are interconnected with the neighboring neurons in the preceding layer through predetermined weights [19], [14]. These are known weights are used in framing the new featured maps by convolving with the input, which results in a non-linear activation function. Even though the weights of all the neurons in a feature map tend to be equal, the feature extraction is effective in extracting different features at each level because different feature maps have variable weights. The  $n^{\text{th}}$  feature map output is denoted by  $Y_n$ . This is computed as follows,

$$Y_n = f(W_n * x) \tag{2}$$

Where  $x$  is the input and  $W_n$  is the convolution window for the  $n^{\text{th}}$  feature map,  $f(\cdot)$  denotes the non-linear activation function that is featured to extract the non-linear features in the given input image.

2) *Pooling layer:* This layer reduces the spatial resolution of each feature map besides increasing the spatial invariance that occurs due to the distortion input. The average value of all the input neurons can be propagated to the next layer with an average pooling function when a relatively small window of the neighborhood image is considered. But the maximum value of the input is propagated to the next layer through the maximum pooling aggregate function by selecting the largest element of the receptive field as follows,

$$Y_{nij} = \max_{(p,q) \in R_{ij}} X_{npq} \tag{3}$$

Where the feature map output of  $n^{\text{th}}$  element is denoted by  $Y_{nij}$  and  $x_{npq}$  is the element in  $(p,q)$  in the pooling region with a receptive field around the location  $(i,j)$ .

3) *Stacked layers:* When more features are required to be extracted for the classification of images, then the number of pooling layers along with convolution is stacked over one another. Softmax operator is used as it is widely used for classification problem using the Back Propagation Training (BPT) algorithm. The output from the final stack is a vector function  $f(x)$  that mainly depends on the confidence in classifying the input  $x$  in a given class of feature maps and it is obtained by the summation of the class scores of each layer. The class scores will not be an integer and it is a floating point value that is generally unbounded but the final output of the softmax output is a multidimensional vector and it is bounded that ranges from 0 to 1. This function has an exclusive property of breaking down the maximum value to get a maximum part of the distribution and other elements are assigned to a part of the distribution. This property makes this method more suitable in interpreting images in classification problems.

#### IV. RESULTS AND DISCUSSION

The fMRI of infants are collected from the open neuro, neuroimaging data, starplus fMRI data, CRCNS and oasis brain database and analyzed by synthesizing the images. The drift component, seasonal component, noise is removed by subjecting the images to fuzzy adaptive mean filtering.

##### A. Testing and Training

The data set obtained from the online sources is used in the training phase. Even though specific classification is not required in machine learning, since this research aims at the classification of medical images, the dataset is categorized specifically [20-24]. They are categorized based on the type of palsy and age of the infants. The sample images of infants with various types of palsy are shown in Fig. 4.

##### B. Pre-training

The experiments were carried out using tensorflow, an open source framework available for building and training multilayer neural networks. Here, the weights of the convolution layer were trained on the dataset available on the website and screen shot is shown in Fig. 5. Tensorflow is used to build the coding for the deep learning algorithm.

Four hundred fMRI images were trained and one hundred and fifty images were tested. The output nodes of the CNN are converted into class probabilities by the softmax function. The error between the predicted class and the actual output class is the loss function. The major challenge in training CNN for medical images is the limitations in the availability of the labelled data set. Very few datasets of fMRI is available for research, namely, neuroimaging data, starplus fMRI data, CRCNS data, etc.

But the final output layers were trained with real-time fMRI images obtained from the cerebral palsy society and indicated in Table II.



Fig. 4. fMRI Sample Dataset.

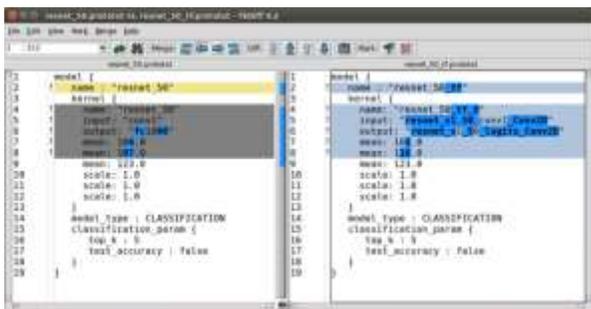


Fig. 5. Screen Shot of Tensorflow.

TABLE II. TESTING AND TRAINING DATASET

Image Category	Training	Test	Total
Spastic	89	44	133
Dyskinetic	54	25	79
Ataxic	26	17	43
Mixed	48	34	82
TOTAL	217	120	337

The training of the framed network was repeated for the available dataset until the loss function is minimized by adjusting the assumed weights[23] ,[25]. The training progress is continuously measured by mapping the training loss with the iterations. The number of images in each iteration is assumed to be twenty. The accuracy of each data set is also examined and plotted beside the loss function as indicated in Fig. 6.

This challenge is overcome by the concept of transfer learning. Here the weights used in training a smaller dataset is derived from any large dataset with an assumption that the required image features are shared among the two data sets.

##### C. Comparative Result Analysis

The research experiment included training and testing phase with each set running 150 epochs. The accuracy tends to increase in each training set and losses were lowered consequently. Classification of fMRI is absolutely different from training MR images with increased complexity due to three dimensional time series nature. The training session is focused with high accuracy level and eliminating the false data with the best chosen hyper parameters. Thus the CNN with three layer model and twice the length size have converged with highest accuracy of 66.8%

The performance of this algorithm can be analyzed by the confusion matrix shown in Table III. The image data set is categorized into five image groups comprising of twenty images in a group. The confusion matrix is useful in identifying the number of images classified properly as the type of cerebral palsy.

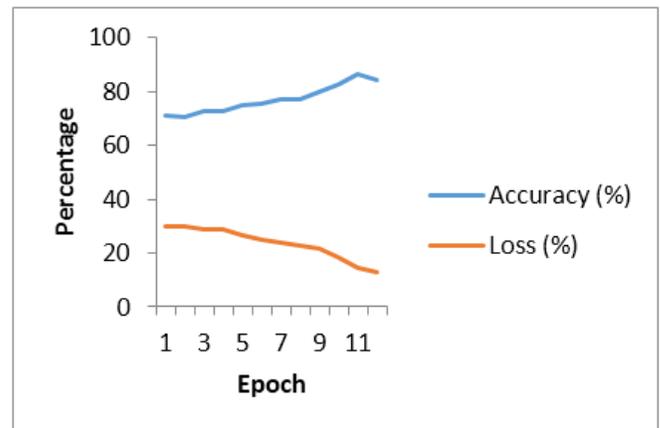


Fig. 6. Training and Validation Results.

TABLE III. CONFUSION MATRIX

Details	1	2	3
TP	12	16	11
FP	2	1	2
TN	3	2	3
FN	3	2	4
Accuracy	0.75	0.86	0.7

TP- True Positive, FP- False Positive, TN- true Negative, FN- False Negative

A true positive value ( $t_p$ ) is the total images which is affected with CP and correctly identified as an affected image by the algorithm. A true negative (TN) is the quantity of affected images which is not recognized by the algorithm. Similarly, false negative ( $f_n$ ) is the number of images which is not affected by the CP and identified by the algorithm correctly. False positive (fp) is the quantity of CP affected fMRI identified as not affected with CP by the algorithm. The performance of the algorithm for fMR images is measured using various parameters like precision, recall and accuracy. The precision value is calculated based on the ratio of the true positive (tp) to the addition of the true positive (tp) and false positive (fp) rates. Recall value is estimated based on the ratio of the true positive (tp) value to the addition of the true positive (tp) with the rates of false negative (fn). Accuracy is defined as the ratio of the addition of tn and tp to the addition of tn, tp, fn and fp.

$$Precision = t_p / (t_p + f_p) \quad (4)$$

$$Recall = t_p / (t_p + f_n) \quad (5)$$

$$Accuracy = (t_p + t_n) / (t_p + t_n + f_p + f_n) \quad (6)$$

The trained tensorflow network resulted in a final accuracy of 66.8% of the collected test data set. When the same test data set is classified by the radiologists the accuracy level was 62.4%.

The analysis of the fMRI of the cerebral palsy [25]affected infant is done using the deep learning algorithm and a sample is depicted in Fig. 7.

The experimental results were compared with GoogleNet, AlexNet and LeNet. The performance parameters like runtime, training loss, test accuracy and validation accuracy is recorded in Table IV.

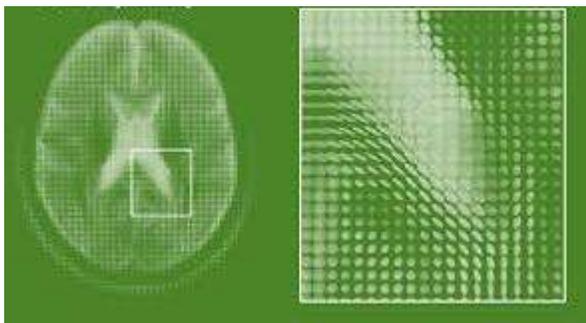


Fig. 7. Analysis of fMRI.

TABLE IV. COMPARATIVE ANALYSIS OF PERFORMANCE PARAMETERS WITH OTHER TECHNIQUES

Method	Runtime (sec)	Training Loss	Validation Accuracy %	Test Accuracy %
GoogleNet	1655	1.6	65	63
AlexNet	33466	1.4	74	70
LeNet	52470	1.51	53	55
Modified AlexNet (Proposed)	16728	0.82	80.4	78.6

It is evident from the experimental results that the classification algorithm for medical imaging analysis cannot be similar to the architecture used in natural image classification. Better accuracy in the classification of cerebral palsy is achieved by the modified AlexNet in terms of the number of convolution layers, normalization function for the local response, kernel size and stride rate.

## V. CONCLUSION

In this paper, we recommended a novel architecture of CNN based on AlexNet that incorporates five layers of convolution and layers of pooling stacked together for higher level of accuracy in the classification of the fMRI brain images of the cerebral palsy infants. The experimental results have vividly shown that deep learning network proposed in this paper presents with a higher level of precision and accuracy compared to other existing methods besides overcoming the high level of complexity due to the challenges in acquiring the fMRI of infants. However, the medical image data set was very limited due to privacy and other security reasons that increased the hunger of deep learning architecture. Even though the samples were limited the features considered were numerous that aided inappropriate classification of the cerebral palsy. This research shall be further extended in developing a network to classify the types further by considering the fMRI along with the oculomotor responses to improve the accuracy level still better.

## ACKNOWLEDGMENT

The authors like to express their genuine gratitude to the VGM scan and Diagnostic laboratories, Coimbatore and Jain University, Bangalore for providing chances to do the project in this area. Finally, the authors acknowledge.

## REFERENCES

- [1] K. Dhara, S. Mukhopadhyay, A. Dutta, M. Garg, and N. Khandelwal, "A combination of shape and texture features for classification of pulmonary nodules in lung CT images," *Journal of digital imaging*, vol. 29, pp. 466-475, 2016.
- [2] M. Ahmadi, M. O'Neil, M. Fragala-Pinkham, N. Lennon, and S. Trost, "Machine learning algorithms for activity recognition in ambulant children and adolescents with cerebral palsy," *Journal of neuroengineering and rehabilitation*, vol. 15, pp. 1-9, 2018.
- [3] C. M. Bertonecelli, P. Altamura, E. R. Vieira, S. S. Iyengar, F. Solla, and D. Bertonecelli, "PredictMed: A logistic regression-based model to predict health conditions in cerebral palsy," *Health informatics journal*, vol. 26, pp. 2105-2118, 2020.
- [4] R. O. Bahado-Singh, S. Vishweswaraiah, B. Aydas, N. K. Mishra, C. Guda, and U. Radhakrishna, "Deep learning/artificial intelligence and blood-based DNA epigenomic prediction of cerebral palsy," *International journal of molecular sciences*, vol. 20, p. 2075, 2019.

- [5] R. Cunningham, M. B. Sánchez, P. B. Butler, M. J. Southgate, and I. D. Loram, "Fully automated image-based estimation of postural point-features in children with cerebral palsy using deep learning," *Royal Society open science*, vol. 6, p. 191011, 2019.
- [6] J. J. Lee-Park, H. Deshpande, J. Lisinski, S. LaConte, S. L. Ramey, and S. C. DeLuca, "Neuroimaging strategies addressing challenges in using fMRI for the children with cerebral palsy," 2018.
- [7] S. A. Rethlefsen, D. D. Ryan, and R. M. Kay, "Classification systems in cerebral palsy," *Orthopedic Clinics*, vol. 41, pp. 457-467, 2010.
- [8] J. W. Gorter, M. Ketelaar, P. Rosenbaum, P. J. Helders, and R. Palisano, "Use of the GMFCS in infants with CP: the need for reclassification at age 2 years or older," *Developmental Medicine & Child Neurology*, vol. 51, pp. 46-52, 2009.
- [9] A. Moreno-De-Luca, D. H. Ledbetter, and C. L. Martin, "Genetic insights into the causes and classification of the cerebral palsies," *The lancet neurology*, vol. 11, pp. 283-292, 2012.
- [10] S. Love, I. Novak, M. Kentish, K. Desloovere, F. Heinen, G. Molenaers, et al., "Botulinum toxin assessment, intervention and after - care for lower limb spasticity in children with cerebral palsy: international consensus statement," *European Journal of Neurology*, vol. 17, pp. 9-37, 2010.
- [11] A. Crichton, M. Ditchfield, S. Gwini, M. Wallen, M. Thorley, J. Bracken, et al., "Brain magnetic resonance imaging is a predictor of bimanual performance and executive function in children with unilateral cerebral palsy," *Developmental Medicine & Child Neurology*, vol. 62, pp. 615-624, 2020.
- [12] M. A. Lindquist, "The statistical analysis of fMRI data," *Statistical science*, vol. 23, pp. 439-464, 2008.
- [13] S. Khan and S.-P. Yong, "A deep learning architecture for classifying medical images of anatomy object," in *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 2017, pp. 1661-1668.
- [14] K. A. Garrison, C. Rogalsky, T. Sheng, B. Liu, H. Damasio, C. J. Winstein, et al., "Functional MRI preprocessing in lesioned brains: manual versus automated region of interest analysis," *Frontiers in neurology*, vol. 6, p. 196, 2015.
- [15] Q. Li, W. Cai, X. Wang, Y. Zhou, D. D. Feng, and M. Chen, "Medical image classification with convolutional neural network," in *2014 13th International Conference on Control Automation Robotics & Vision (ICARCV)*, 2014, pp. 844-848.
- [16] T. L. Sutcliffe, W. C. Gaetz, W. J. Logan, D. O. Cheyne, and D. L. Fehlings, "Cortical reorganization after modified constraint-induced movement therapy in pediatric hemiplegic cerebral palsy," *Journal of child neurology*, vol. 22, pp. 1281-1287, 2007.
- [17] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*: MIT press, 2016.
- [18] Y. Bleyenheuft, L. Dricot, N. Gilis, H.-C. Kuo, C. Grandin, C. Bleyenheuft, et al., "Capturing neuroplastic changes after bimanual intensive rehabilitation in children with unilateral spastic cerebral palsy: a combined DTI, TMS and fMRI pilot study," *Research in developmental disabilities*, vol. 43, pp. 136-149, 2015.
- [19] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, et al., "Going deeper with convolutions," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015, pp. 1-9.
- [20] A. Paulson and J. Vargus-Adams, "Overview of four functional classification systems commonly used in cerebral palsy," *Children*, vol. 4, p. 30, 2017.
- [21] X. Xi, E. Keogh, C. Shelton, L. Wei, and C. A. Ratanamahatana, "Fast time series classification using numerosity reduction," in *Proceedings of the 23rd international conference on Machine learning*, 2006, pp. 1033-1040.
- [22] R. Meszlényi, L. Peska, V. Gál, Z. Vidnyánszky, and K. Buza, "Classification of fMRI data using dynamic time warping based functional connectivity analysis," in *2016 24th European signal processing conference (EUSIPCO)*, 2016, pp. 245-249.
- [23] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Advances in neural information processing systems*, 2012, pp. 1097-1105.
- [24] L. Koman and B. Smith, "en Shilt, JS (2004) Cerebral palsy," *The Lancet*, vol. 363, pp. 1619-163.
- [25] D. Pantazis, A. Joshi, J. Jiang, D. W. Shattuck, L. E. Bernstein, H. Damasio, et al., "Comparison of landmark-based and automatic methods for cortical surface registration," *Neuroimage*, vol. 49, pp. 2479-2493, 2010.