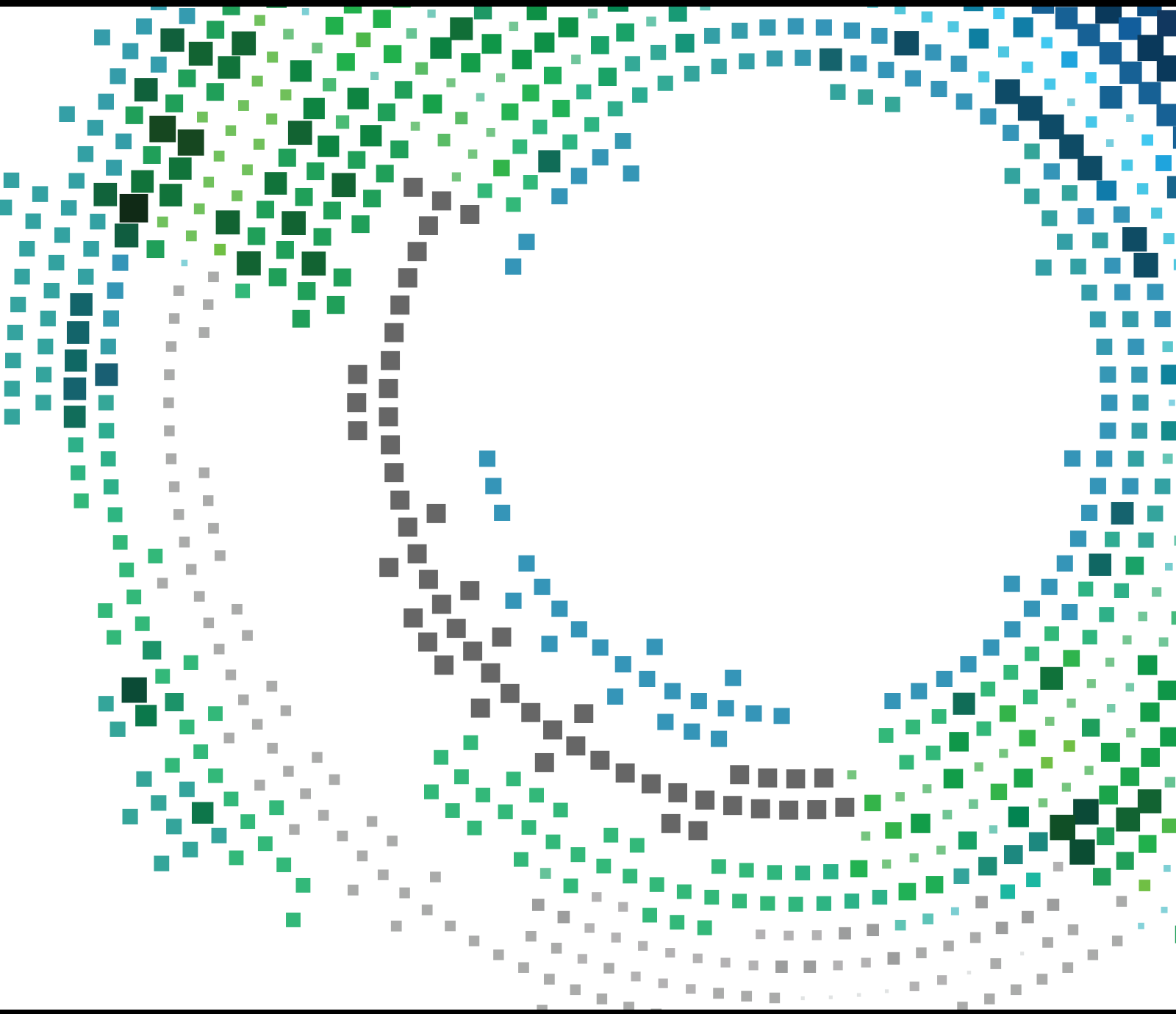
Mobile Information Systems

Federated Intelligence in Edge and IoT Networks

Lead Guest Editor: Junaid Shuja
Guest Editors: Syed Bilal Hussain Shah and Aman Singh



Federated Intelligence in Edge and IoT Networks

Mobile Information Systems

Federated Intelligence in Edge and IoT Networks

Lead Guest Editor: Junaid Shuja
Guest Editors: Syed Bilal Hussain Shah and Aman Singh

Chief Editor

Academic Editors

Contents

Hindawi
Mobile Information Systems
Volume 2023, Article ID 1060135, 17 pages
https://doi.org/10.1155/2023/1060135

Review Article

A Computer Vision-Based System for Recognition and Classification of Urdu Sign Language Dataset for Differently Abled People Using Artificial Intelligence

Hira Zahid,[1] **Sidra Abid Syed**,[2] **Munaf Rashid**,[3] **Samreen Hussain**,[4] **Asif Umer**,[5] **Abdul Waheed**,[6,7] **Shahzad Nasim**,[8] **Mahdi Zareei**,[9] **and Nafees Mansoor**[10]

[1]*Biomedical Engineering Department and Electrical Engineering Department, Ziauddin University, Karachi 74600, Pakistan*
[2]*Biomedical Engineering Department, Sir Syed University of Engineering and Technology, Karachi 75300, Pakistan*
[3]*Software Engineering Department, Sir Syed University of Engineering and Technology, Karachi 74600, Pakistan*
[4]*Electronic Engineering Department, Dawood University of Engineering & Technology, Karachi 74800, Pakistan*
[5]*Department of Computer Science & IT, Hazara University, Mansehra 23100, Pakistan*
[6]*Department of Computer Science, Women University Swabi, Swabi 23430, Pakistan*
[7]*School of Electrical and Computer Engineering, Seoul National University, Seoul 08826, Republic of Korea*
[8]*Begum Nusrat Bhutto Women University, Faculty of Management Information Science and Technology, Sukkur, Pakistan*
[9]*Tecnologico de Monterrey, School of Engineering and Sciences, Monterrey 64849, Mexico*
[10]*Department of Computer Science and Engineering, University of Liberal Arts Bangladesh (ULAB), Dhaka, Bangladesh*

Correspondence should be addressed to Abdul Waheed; abdul@netlab.snu.ac.kr and Nafees Mansoor; nafees@nafees.info

Received 18 September 2022; Revised 21 February 2023; Accepted 13 April 2023; Published 26 June 2023

Academic Editor: Junaid Shuja

Communication between normal people and deaf people is the most difficult part of daily life worldwide. It is difficult for a normal person to understand a word from the deaf one in their daily routine. So, to communicate with deaf people, different countries developed different sign languages to make communication easy. In Pakistan, for deaf people, the government developed Urdu Sign Language to communicate with deaf people. Physical trainers and experts are difficult to provide everywhere in society, so we need such a computer/mobile-based system to convert the deaf sign symbol into voice and written alphabet that the normal person can easily get the intentions of the deaf one. In this paper, we provided an image processing and deep learning-based model for Urdu Sign Language. The proposed model is implemented in Python 3 and uses different image processing and machine techniques to capture the video and transform the symbols into voice and Urdu writing. First, we get a video from the deaf person, and then the model crops the frames into pictures. Then, the individual picture is recognized for the sign symbol such as if the deaf showed a symbol for one, then the model recognizes it and shows the letter which he/she wants to tell. Image processing techniques such as OpenCV are used for image recognition and classification while TensorFlow and linear regression are used for training the model to behave intelligently in the future. The results show that the proposed model increased accuracy from 80% to 97% and 100% accordingly. The accuracy of the previously available work was 80% when we implemented the algorithms, while with the proposed algorithm, when we used linear regression, we achieved the highest accuracy. Similarly, when we used the TensorFlow deep learning algorithm, we achieved 97% accuracy which was less than that of the linear regression model.

1. Introduction

Because many people are born with impairments, none of us are flawless. We cannot ignore them in society due to a variety of issues. Even the government has a quota set aside for disabled people. Researchers are attempting to develop digital solutions to overcome limitations associated with special personas and enable them to participate in functioning societies [1]. Everything in our world is flawed, and idealism has no place in it, as many scientific data and

statistics demonstrate. Similarly, man is neither perfect nor ideal, and some people are born differently than others. Since then, they have been dubbed "handicapped." They are diverse, yet they each have their own set of needs. Deafness affects an estimated 72 million individuals globally [2], including roughly 10 million people in Pakistan. There are different communication styles of deaf people all around the world. Visual communication was used to convey information since the dawn of time. In general, several new sorts of trademarks, languages, and sign language are being adopted all over the world. Without the need for paper or pencil, the deaf community and the community at large may communicate efficiently using a variety of sign languages. Different nations, such as the United States, have their own sign languages, such as American Sign Language, British Sign Language, Spanish Sign Language, and probably sign languages across the world. There are still more sign languages than winks, and numerous varieties of American Sign Language (ASL) are exploited in communication. There are around 60 sign languages that are acknowledged and practiced [3]. ASL is a comprehensive and complicated language, according to the National Institute on Deafness and Other Communication Disorders (NIDCD). Hand gestures, as well as face expressions and muscular movements, are all examples of this. This is not simply a hand gesture translation in English; it can also handle grammar and pronunciation rules, as well as different races and dialects. Furthermore, there are several reports in various languages, including Chinese, American, and Indian, showing that a significant amount of work has been put into the worldwide sign language identification system. Local and regional languages and cultures play an essential role in the evolution of sign language, as they do in the evolution of any spoken language, regardless of origin. Many experts, on the other hand, have questioned why there is no common sign language for signatories [4]. It is identical to wondering why there is not a widely recognized language spoken across the world. Pakistani Sign Language has been used by deaf people in Pakistan to communicate among each other (PSL). It follows linguistic norms, just like all other sign languages, and it contains syntax, letters and words, gestures, and complicated sentences, just like spoken Urdu. It also has its own set of symbols and a constantly changing grammar, much like every other sign language system on the planet [5]. Due to its growth throughout time, PSL has evolved into a comprehensive language. Urdu is the official language of Pakistan and is spoken by many people across South Asia. In Urdu, the most widely used writing systems are Nastaliq and Naskh. Nastaliq style is commonly utilized in ancient Urdu literature and journalism. Persian, Pashto, Punjabi, Balochi, and Seraiki are among the ethnic languages that employ the Nastaliq writing style. Urdu belongs to the Indo-European language family. Since its inception, the Indo-European Urdu language has had its origins in India. In the Indian subcontinent, it is now one of the most frequently spoken languages. Urdu is one of India's 23 official languages and one of Pakistan's two languages [6]. In addition, Dubai boasts a sizable Urdu-speaking community. It is spoken by the majority of the world's inhabitants. This is a written version of Urdu that is based on the Arabic script and is developed from the Persian script. Urdu is written from right to left, much like Arabic. Sign languages have formed the backbone of distinct deaf cultures as a practical way of communication for deaf people all over the world. Other symptoms are used by listeners who are unable to communicate vocally owing to a disability or impairment, such as augmented and alternative communication, or whose family members are deaf, such as children of deaf adults. Through picture-to-speech technology, those who are deaf or hard of hearing, as well as blind people, can benefit from this effort. For the blind, having a computer recognize a character in an image and translate it to a sound can be lifesaving. Urdu, unlike Arabic and Persian, has a larger number of separate letters. Urdu's script is more complicated than Arabic or Persian. The Sind Welfare Association of the Deaf presented the fundamental structure of the Urdu alphabet for deaf people as shown in Figure 1. Similarly, in Figure 2, the Sindh Welfare Association of the Deaf provided the basic structure of number system for deaf people and implemented it in most of the schools. In Figure 3, the association provided structure for the deaf people about English alphabets using two hands while in Figure 4, the association presented English alphabets of sign language using single hand. In this case, gesture recognition has shown to be useful, helping deaf patients to interact with us more effectively and efficiently. Identification of the sign has taken a long time and effort all over the world. In the case of Urdu Sign Language, however, no such work has been undertaken. Around 0.2 million Pakistanis who are deaf or hard of hearing lack access to assistive and rehabilitative technologies. Gestures can be divided into two categories. Static gestures are those in which the hand, body, and face do not move. Signals that do not alter are known as static signals [7].

The perceivable gesture happens within a set duration that the performer physically orchestrates during static motions. The finger and hand positions are recognized and examined one after the other [8]. Other sign languages, such as British Sign Language (BSL), American Sign Language (ASL), Arabic Sign Language (ArSL), and Spanish Sign Language (SSL), are used in different regions of the globe [9]. Each of these sign languages evolves on its own. In general, gestures in sign language consist of theoretical fictional hand motions, such as the thumb, which is frequently employed for the word "OK," or the principles of the specific sign language. Spell each word one at a time.

To recognize gestures or hand movements, two basic methods are employed [10]. There are two methods: one is based on computer vision, which uses an image evaluation technique to translate images of the singer into text, and the other is based on machine learning.

Wearing sensor-equipped gloves [11] is the third approach. The present status of sign language recognition (SLR) is over 30 years behind the voice recognition technology due to a variety of causes. The capture and detection of two-dimensional video data is far more complicated than the analysis of linear audio signals, which is one of the key reasons for this. Sindh Welfare Association of the Deaf

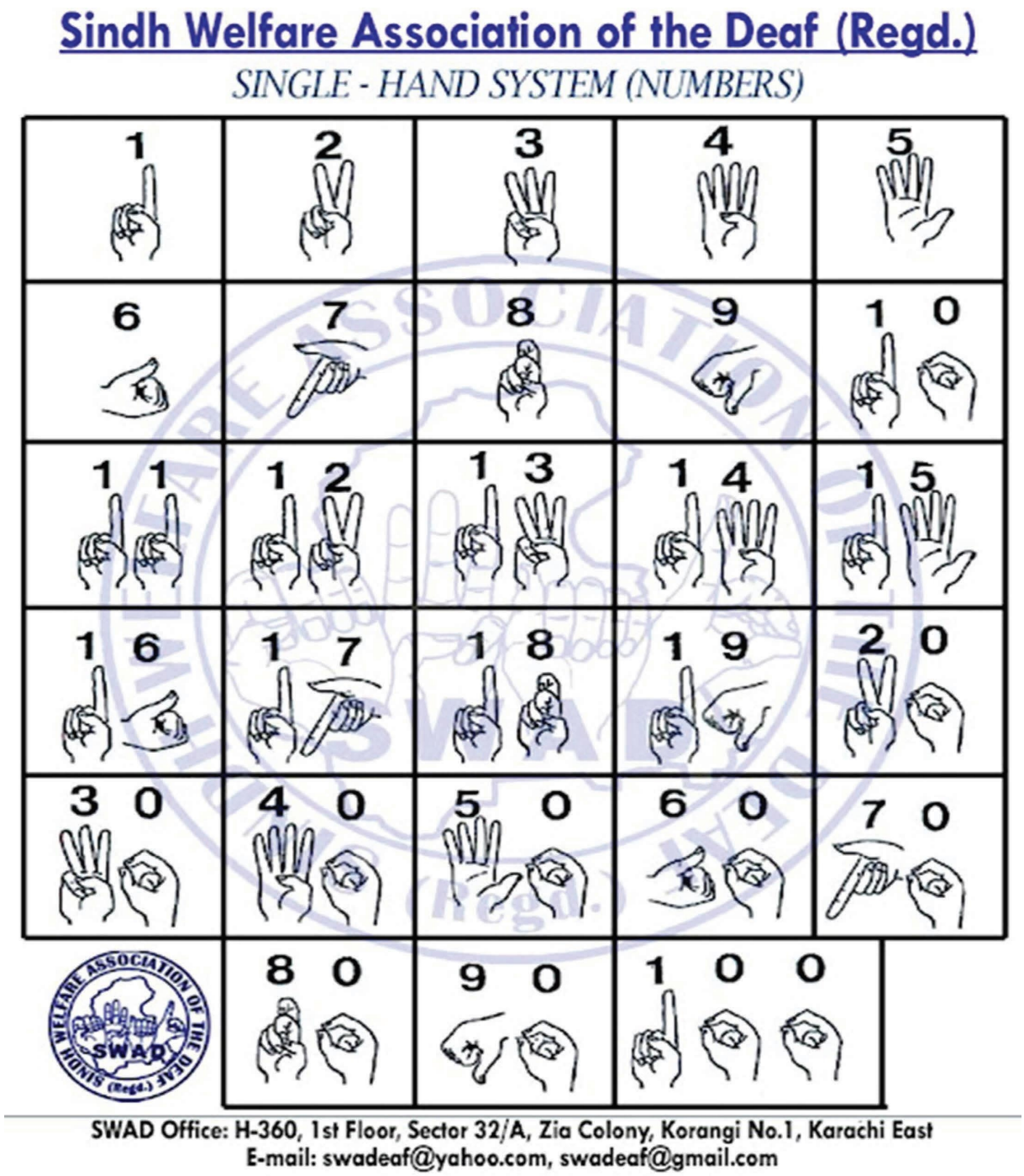


Figure 1: Urdu alphabets for deaf persons (Sindh Welfare Association of the Deaf).

provided standard alphabets for disabled people, which will be followed as a standard for Urdu speakers. In Figure 3, the association used the two-hand system for deaf people to communicate with other people without any misguidance or hesitation. They provided advance sign language for communication of English words such as if deaf want to speak "MAN," then he will provide the sign of M then sign for A and then sign for N. So, in this way, the deaf person can share his thoughts with healthy people. All such sign languages need computer-based systems to recognize such signs and then abbreviate/speak the correct words on behalf of the deaf ones. In Figure 4, the welfare association provided standard single hand English alphabets for deaf people. Instead of using double hand English alphabets, if any deaf person does not have one hand and he wants to communicate on single hand, then there is standard system for such disabled person to communicate with other healthy persons. Furthermore, oral communication's lexical and grammatical features are yet to be completely investigated, and no ordinary terms are accessible. Furthermore, there is no standard definition for

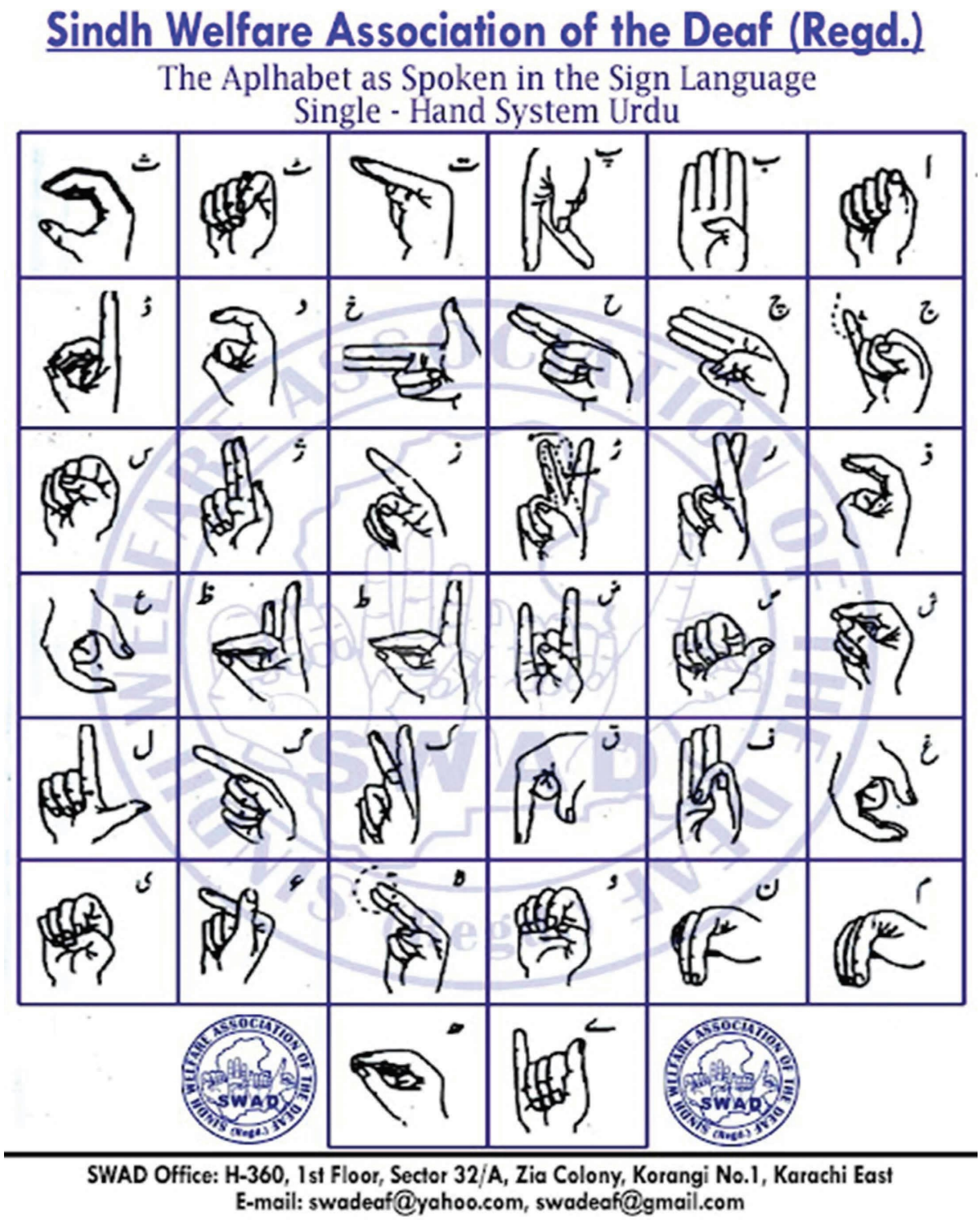


Figure 2: Number system for deaf persons (Sindh Welfare Association of the Deaf).

such indicators. In the early 1990s, research on the categorization and identification of sign language achieved a pinnacle. Techniques for collecting data are critical for identifying key aspects of various SLR studies [12]. Much research has looked towards data gloves or cyber gloves to extract the features of mechanical and nonmechanical components of signals due to the heavy dependence on sensor-based SLR systems. Unfortunately, using such sensors is inconvenient and restricted to the signer. Furthermore, because of the high cost of sensors, sensor-based SLR systems are not viable to deploy. The weight and capacity to manage variations under changing illumination and barriers

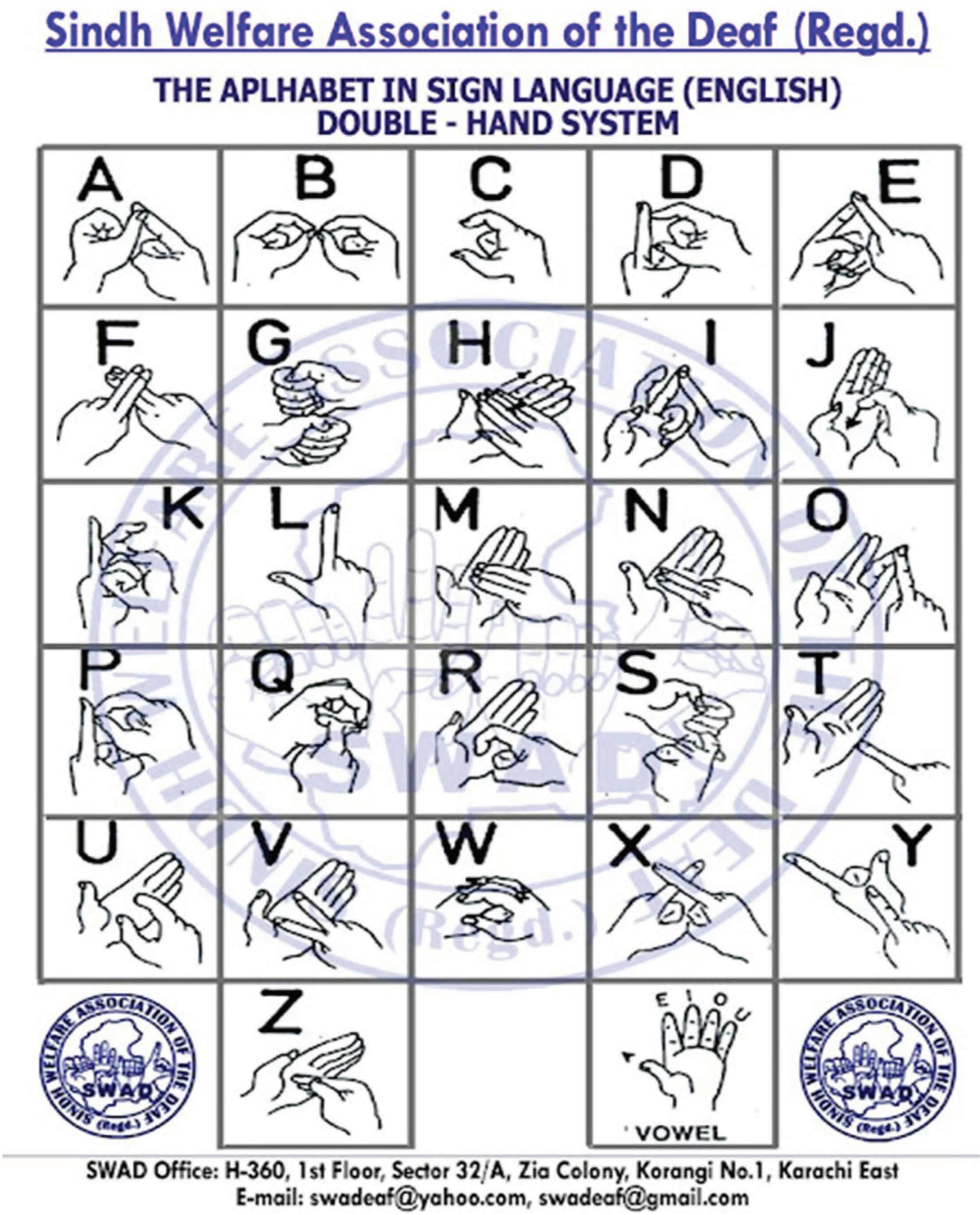


Figure 3: English alphabets for deaf persons (Sindh Welfare Association of the Deaf).

in the crowd, dynamic anomalies, and feature extraction phase of vision-based SLR systems, on the other hand, has tremendously affected researchers. To categorize the main characteristics of the various SLR jobs, population sampling approaches are critical. Many studies have employed electronic gloves or cyber gloves to collect data on the mechanical and nonmechanical components of symptoms due to the substantial dependence on sensor-based SLR systems. The usage of these sensors, on the other hand, is cumbersome and severely limiting for the signatory [13]. Furthermore, practical implementations of sensor-based SLR systems are problematic because of the high cost of sensors. On the other hand, because of their weight and throng, dynamic heterogeneous environment, and capacity to

Figure 4: Single-hand English alphabets for deaf persons (Sindh Welfare Association of the Deaf).

control changes in distribution phase under varying illumination and limitations, visionary SLR systems have wowed researchers [14]. The SLR solution's standard feature automatically enables signer-dependent actions, which means that all signers are educated before working with the patient. Signer independence, also known as cross-signer verification, entails the normalizing of features to eliminate confirmer interactivity. The line between certain signatures and the camera is rarely evident, as is the currency of signature and magnification [15]. SLR's early phases were likened to speech recognition in that they concentrated on symptoms. Although several SLR approaches for identifying continuous phrases have been established, the recognition accuracy for short dictionaries employing epithelial movement between the symbols is barely 90%. Researchers are now

working on developing an image-based system that can receive live stream photos and tell or write the sign language alphabets used by the deaf.

1.1. Contributions

(i) In this paper, we proposed an image-based sign language classification and recognition model to capture the image of the sign of the deaf person and recognize it and then tell the number in written and voice as well.

(ii) The proposed model is loaded into the system, and then the configuration is loaded or set with parameters like max number of hands and confidence level. The file with an index of names is loaded to show the human understandable output on screen. Open Computer Vision comes now and gets images from files or cameras (live feed). Then, the frame is prepared for detection and recognition.

(iii) We used Python 3 language for programming, Open Computer Vision, TensorFlow, and Keras for detection of images, and Open Computer Vision, TensorFlow, Keras, Pandas, and sklearn for module training.

(iv) The proposed model accurately detects and recognizes the sing language Urdu alphabets.

The following is a breakdown of the paper's structure. Section 2 is devoted to a review of the literature. The problem is outlined in Section 3. The proposed solution is shown in Section 4. The simulation and methodology are provided in Section 5, and results are covered in Section 6. The paper's discussion and conclusion are included in Section 7.

2. Literature Review

The disabled persons or special persons such as deaf people cannot communicate with normal person efficiently. Therefore, sign language can help people with disabilities to communicate. In sign language, several sorts of motions with various shapes are utilized [16]. Similarly, sign languages vary by geography, and there are currently 138 recognized sign languages. The British-American Sign Language is based on English, while Chinese and Indian Sign Languages are also growing in popularity. Because sign language is focused on forms and concepts while spoken and written languages are based on words and grammar, sign language grammar is mostly based on written and spoken language grammar. As a result, the two languages have different grammatical structures. Information technology has had a significant impact on human life. To assist humanity in solving various challenges, many technologies, techniques, and instruments have been invented [17]. Information technology has been utilized to overcome the communication gap between deaf and hearing people. The idea behind these IT-based technologies is to help deaf individuals interact more effectively with persons who have impairments and vice versa. IT-based technologies like these might be useful in overcoming this communication divide. Many developed countires solved the issue of miscommunication of deaf with normal people by using information technology (IT). By using IT, most of the issues of miscommunication are solved efficiently in this modern era [18]. In Pakistan, there is no such software or other IT technologies to solve the Urdu communication among deaf and normal people. As a result, we require such a computer-based system to communicate with deaf people and to decrease human involvement during the deaf people's understanding of everyday life activities. Using popular literature, reduce and recommend communication gaps for Pakistan's deaf population and find essential processes for building an architectural framework based on information technology programmed that can also help bridge the gap between the deaf and the country's public [19]. Mobile phone computing, gesture-based environments, and cloud technologies are all part of modern technology. Artifical Intelligence technologies such as Leap Motion Kinect, Google Glass, and Leap Motion Controller are using to capture the gesture of hands and other disabled parts of human body [20]. As previously said, technological advancements may be leveraged to help deaf individuals. Communication is a huge issue for deaf children since they are unable to interact with society because they are unable to speak normally. The learning environment for deaf students at educational institutions is not necessarily the same as for hearing students. As a result, sign language is one of the most effective ways for deaf individuals to communicate. Signature conversations cannot be understood by an expert or colleagues using a gesture-based interface, which causes communication challenges between the deaf and the public [21]. Communication among deaf and normal people is the ultimate goal of the modern research. Sensors, gadgets, and image-based methods are all utilized. HCI, robotics, game-based learning, and login software recognition system have all received more attention in recent research. Programs and systems for language recognition are employed. The PC vision community uses a variety of procedures and algorithms [22]. Efforts are already been made by the researchers in the field of communication among deaf and normal people. So, most of the best algorithms/software are the results of such research studies in the field of gesture recognition and communication for disabled people [19]. The game encourages users to engage with a virtual environment, allowing them to learn sign language in a novel and enjoyable way. It is regarded as a language of Portuguese Sign Language [23] to use sign language signals to consolidate similar aims and purposes. ISL translation system and Indian Sign Language (ISL) translation device for learning sign language pictures or continuous video images (of the public) are captured using a microphone or USB camera and can be interpreted by an application. It is envisaged that the obtained expressions will be translated, scaled, and disseminated. Image capture, identification of the binary type of hand, and finding shape and function are variables in the approach and interpretation processes. The message is displayed and sent to the recipient in the built-in form by the GUI program. It compels normal individuals to converse freely with deaf people [24]. With the use of image-based

approaches, the spoken prefixes are transformed to sign languages utilizing a computer-based system. With different degrees of success, this translation project has an exceptional employment offer. In [25], the authors presented sign languages of different countries such United States, Greece, South Africa, Arabic countries, Spain, Italy, Japan, Netherland, and United Kingdom. When it comes to people who cannot hear properly, sign language (LS) is a valuable resource. East Optical motion bidding is another name for the approach. This strategy is used by those who do not comprehend adequately. Language serves as the primary means of communication. Every country has its own set of signs. China, the United States, India, and Pakistan, for example, all have their own sign languages. Indian Sign Language and Pakistani Sign Language are two different sign languages. Many developing countries hold seminars on the subject. To close the gap, they organize a variety of project activities, including information technology. For those who are deaf and people who are not deaf, several surveys have been undertaken throughout Central and South Asia. Nonetheless, this approach is being investigated in Pakistan because there is no systematic information on it. In [18], the authors proposed grammar, content, and delivery tools used in Pakistan for disabled people communication as the main communication of deaf take place on the basis of language structure. However, the primary point has been made thus far. The goal of this study is to talk about the difficulties that need to be addressed to close the gap between the general and deaf communities. They provide several suggestions for constructing a bridge. Sign language follows a distinct set of norms than spoken and written languages. Sign language is a kind of communication that is used to communicate. It is built on forms, and written language is built on certain fundamental word construction and grammatical rules [26]. Information technology has a significant influence on our lives; individuals create many of the items we use. In India, exceptional labor has been done to pave the path for extraordinary individuals. The most significant challenge they encounter is their inability to communicate with others. People have taken up the role of virtual or effective language [27]. Pakistani academics are also focused on developing different assistive technologies for persons with impairments, such as a sensory glove and transliteration of American Sign Language [19]. The above automated device, dubbed "talking hand," was built to promote communication between the public and those who were impacted. The author employed artificial neural networks to receive sensory information utilizing gloves in the suggested method. The technique was utilized for 24 letters of the English alphabet and two punctuation marks by the author. As a result, deaf people who use the software can use it to communicate [28]. The authors did a similar study on the connection between deaf and handicapped individuals in [29], with the gloves equipped with sensors that detect spoken messages via finger movement. This is a handy program that converts the alphabet to text and speech [30]. The authors employed a two-based jump motion device technique to create letters in Pakistani Sign Language. The "communication module" is a module that trains one system for translation while the other gathers information using a jump motion device. The authors of [31] developed a gadget that translates physical signals to digital data and issues the necessary instructions for deaf people. The gadget uses symbols to transmit data to the computer alliance. This is a visual art that has been utilized in Pakistan before, such as a glove for deaf people. In Pakistan, there is a lot of effort being done for deaf persons who desire to communicate with regular people. The authors of [32] created a tool called an Ambiguous Classifier. Gloves are used to identify fingers, and this instrument indicates the deaf person's symptoms or the color of the operation. This approach has a 95% accuracy rate. Many academics are attempting to bridge the gap between deaf and hearing persons, and the authors of [18] developed a machine learning-based model that might serve as a foundation for comprehending signal-based communication. As a result, the authors presented a model for deaf individuals in Pakistan that assists them in translating English or Urdu texts or speaking in Pakistani Sign Language [18]. The authors proposed a study in [10] with the goal of producing a tool to assist persons with impairments as well as building a program to allow deaf people to conduct normal discussions with other deaf people. Enter sign language as text and make sure the other person can comprehend it. The authors of [33] used the GoogLeNet pretrained architecture on the ILSVRC dataset, which is based on convolutional neural networks and uses ASL datasets from Macy's Store. The University of Surrey employed transfer learning for this purpose. They created a solid model that identifies the letters and works well with newcomers. Fully generalizable translators may be created for any ASL publications. Deep sensor technology is fast gaining popularity, as are other instruments used in this process, which have shown to be successful, such as colorful advertisements like custom-designed gloves. Its purpose is to make the identifying process easier and more efficient. According to [34], certain signal units are simple to classify and identify. To date, automatic gesture language recognition systems have not been able to make use of today's deep detection technologies. Previously, only single camera technology was employed. There are simply pixels in basic picture datasets with no depth or contour information, although classifying images of ASL letter movements using CNN have had some success [33] but utilizing GoogLeNet architects who are already trained [35], a repeated deep structure has been suggested. Continuous sign language recognition uses a convolutional neural network. We have devised a step-by-step solution. How to educate our deep neural network's structure is the focus. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have made significant progress in signaling [36] and sign recognition [37]. In sign recognition, dynamic mundane dependency learning yielded significant results [38].

The authors used image processing and machine learning techniques to produce a detailed literature evaluation on Urdu Sign Language in [39]. Based on [40, 41] and the preceding literature assessment, the following difficulties in the field of Urdu Sign Language remain to be addressed:

(i) Image processing and deep learning-based computerized system is required for deaf people to communicate with the normal people in the society.

(ii) We have a shortage of people who are expert in Urdu Sign Language and who can take part as the middle entity between deaf and normal persons.

(iii) To remove the physical expert and perform that work by computer or any other electronic device, we need an efficient intelligent system to understand and communicate with deaf people for the betterment of the human society.

3. Problem Formulation and Gap Analysis

As in the literature review such as [39], the authors presented that there is no such computer-based system for Urdu sign langauge that could make possible the communication between deaf and normal person. So, in this research, we intend to work on such computer-based system that could help the deaf ones' communication normal ones. In Pakistan, the Urdu sign langauge is used by deaf people, but the normal people did not understand their communication, as sign langauge is not studied by everyone. So, we intend to propose such system that pick the sign of the deaf one and sound the word in voice by the computer to understand by the normal one.

4. Proposed Solution

In front of the camera, the deaf person shows the symbol he/she wants to communicate, and then the camera captures the picture of the symbol and sends it to another machine where image processing technique is used to classify and recognize the image. After recognition, the deep learning technique is used to train the model for future correspondence and send it to the main CPU for preprocessing.

In this section of the paper, we provide a detailed explanation of the proposed model with the help of flowcharts and diagrams.

In Figure 5, the proposed model is provided. As shown in the figure, the proposed model is based on Python 3, image processing model "Open Computer Vision," and deep learning models such as "linear regression" and "TensorFlow" using convolutional neural network. After preprocessing, the image is shown with the desired value that the deaf person wants to communicate. The following entities are used in developing the proposed model as shown in Figure 5.

4.1. Convolutional Neural Network (CNN). We used convolutional neural network in the proposed model. A convolutional neural network is a feed-forward neural network that processes input in a grid-like structure and is commonly used to evaluate visual pictures. ConvNet is another name for it. To recognize and categorize items in a picture, a convolutional neural network is employed. Multiple layers of artificial neurons make up convolutional neural networks. Artificial neurons are mathematical functions that calculate the weighted sum of various inputs and output an activation value, like their biological counterparts. Each layer of a ConvNet creates numerous activation maps when you input a picture into it. The important aspects of the picture are highlighted using activation maps. Each neuron takes a patch of pixels as input, multiplies their color values by their weights, adds them all together, and then runs them through the activation function. Basic characteristics such as horizontal, vertical, and diagonal edges are often detected by the CNN's first (or bottom) layer.

The first layer's output is sent into the second layer, which extracts more complicated characteristics like corners and edge combinations. Each neuron's action is determined by its weight. When given pixel data, CNN's artificial neurons pick out numerous visual features. Basic characteristics such as horizontal, vertical, and diagonal edges are generally detected by the CNN's first (or bottom) layer. The first layer's output is sent into the next layer, which extracts more complicated characteristics like corners and edge combinations. The layers recognize higher-level characteristics such as objects, faces, and more as you progress further into the convolutional neural network. The CNN model is shown in Figure 6. The following hidden layers are used by the CNN architecture to classify and recognize the images or text.

4.1.1. Convolution Layer. This is the initial stage in obtaining useful information from a photograph. The convolution action is performed by many filters in a convolution layer. Every image is seen as a pixel value matrix. Also, we get the image we wanted as a result.

4.1.2. ReLU Layer. The rectified linear unit is abbreviated as ReLU. After the feature maps have been extracted, they must be moved to a ReLU layer. ReLU conducts an element-by-element procedure, setting all negative pixels to zero. It causes the network to become nonlinear, and the result is a corrected feature map.

4.1.3. Pooling Layer. Pooling is a downsampling process that decreases the feature map's dimensionality. To create a pooled feature map, the corrected feature map is now sent via a pooling layer. The pooling layer employs a variety of filters to recognize various aspects of the picture, including edges, corners, the body, feathers, eyes, and the beak.

4.1.4. Fully Connected Layer. Feed-forward neural networks are what the fully connected layer is all about. Fully connected levels are the network's final layers. The output from the final pooling or convolutional layer, which is flattened and then fed into the fully connected layer, is the input to the fully connected layer. We used ResNet model of the CNN methodology.

4.2. ResNet. Residual neural network (ResNet) by Kaiming et al. introduced a novel architecture with "skip connections" and features heavy batch normalization. Such skip connections are also known as gated units or gated recurrent units and have a strong similarity to recent successful

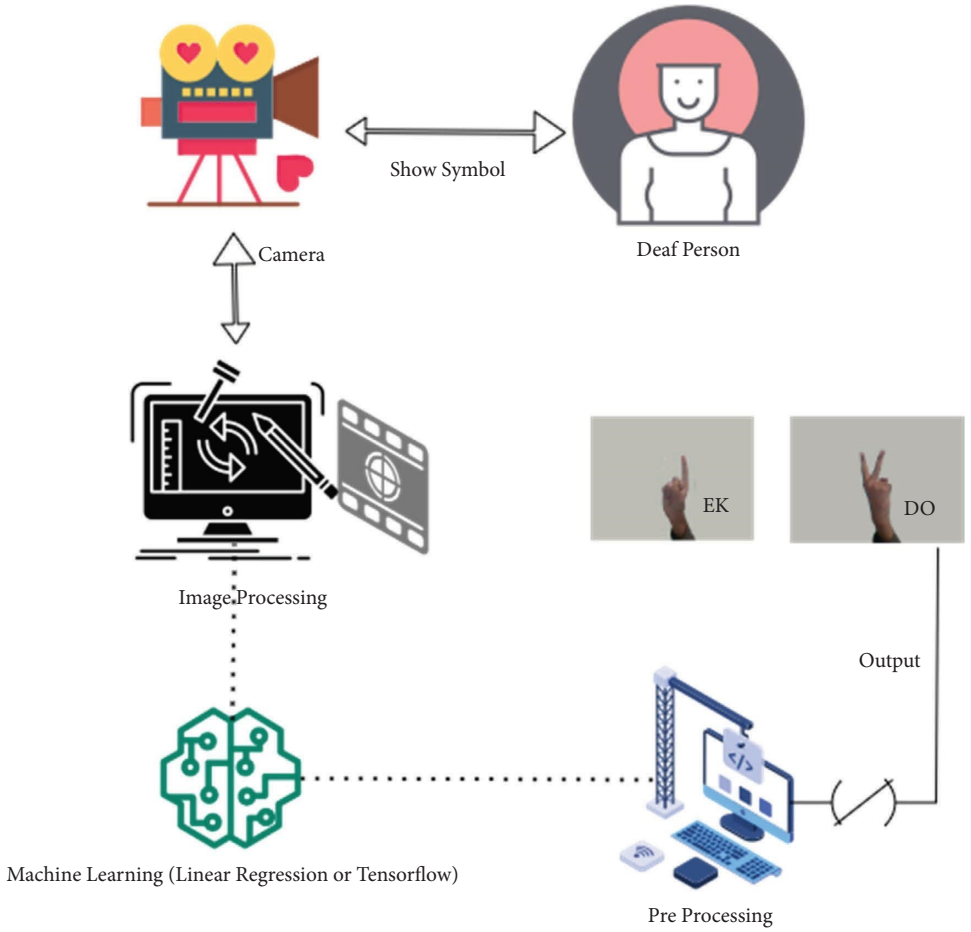


Figure 5: Proposed image processing-based solution.

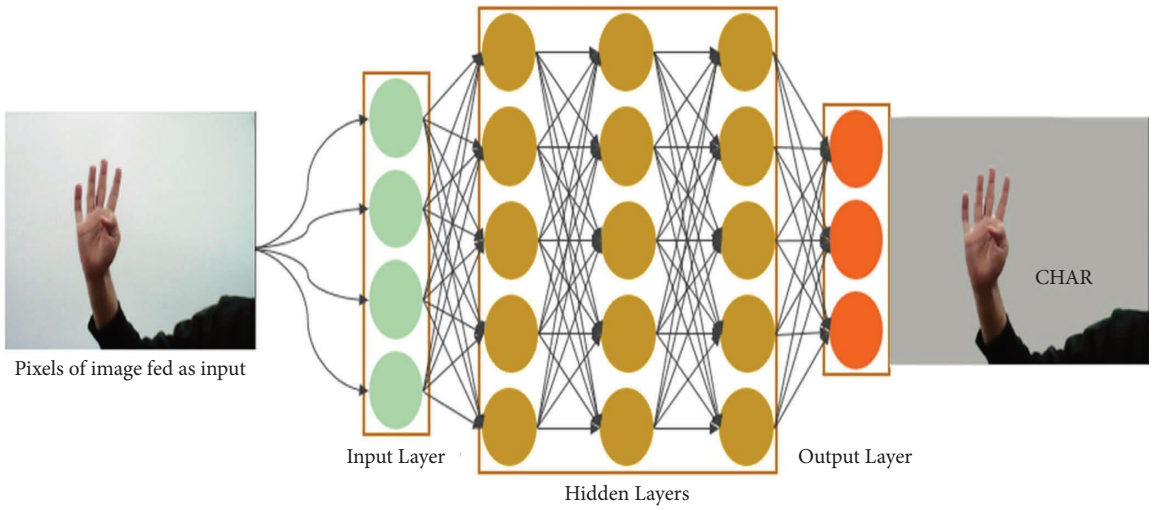


Figure 6: CNN architecture for the proposed model.

elements applied in RNNs. Thanks to this technique, they were able to train a NN with 152 layers while still having lower complexity than VGGNet. It achieves a top-5 error rate of 3.57% which beats human-level performance on this dataset. AlexNet has two parallel CNN lines trained on two GPUs with cross-connections, GoogLeNet has inception modules, and ResNet has residual connections. The library of CCN which is called ResNet is used to train the sign language model to acquire better results. Figure 7 shows the ResNet architecture for the image extraction and classification.

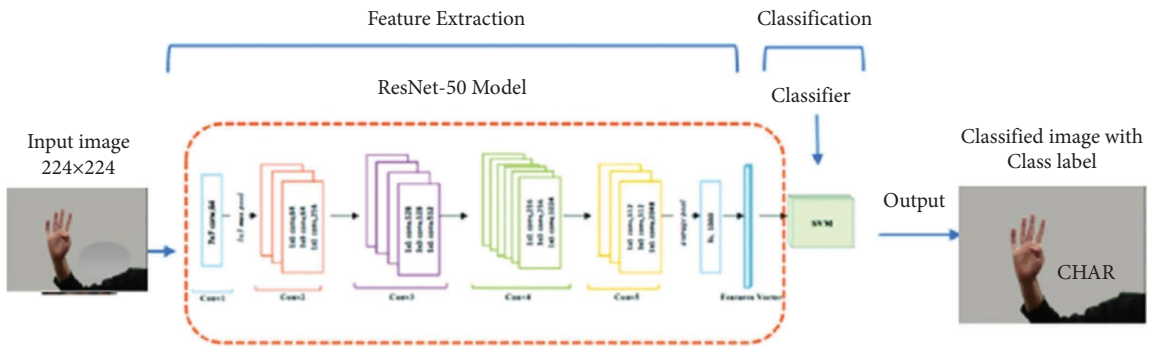


Figure 7: ResNet architecture.

4.3. Camera. A camera is a visual instrument for capturing images. The camera comprises a sealed box (camera body) with a tiny hole (aperture) that allows light to be captured onto a light-sensitive surface at its most basic level (usually photographic film or a digital sensor). To regulate how light falls on a light-sensitive surface, cameras use a variety of methods. The camera's lenses concentrate the light that enters it. The aperture can be made smaller or larger. The length of time a light-sensitive surface is exposed to light is determined by a shutter mechanism. In the art of photography, the steel image camera is an essential tool. Photographic, digital imaging, and photo printing images can be recreated afterwards. Film, videography, and cinematography are among the creative genres covered by the motion picture camera.

4.4. Programming Language. Python was the programming language that we utilized. Python is a popular general-purpose programming language with a lot of flexibility. Python is an object-oriented programming language, making it ideal for quick application development. Python's basic syntactic value is easy to comprehend, which reduces the cost of software security. Modules and packages are supported by Python, which fosters program modularity and code reuse. Python language and large standard library for all main platforms are accessible in free source code or binary format.

4.5. Open Computer Vision. As an image processing-based model, we employed Open Computer Vision. Open Computer Vision is a collection of programming functions for computer vision that is primarily intended for real-time use. In a word, it is an image processing library. It is primarily utilized to perform all image-related operations. More than 2500 complex algorithms are included in the library, including a comprehensive range of both traditional and contemporary machine learning and computer vision techniques.

4.6. TensorFlow. The TensorFlow deep learning model was employed. TensorFlow is a framework for graphing and analyzing complicated complexities. Multiple rows known as model tensors are needed to do this. It is a tool for TensorFlow training. Deep learning-based PSL dataset is utilized for both research and development at the same time.

Table 1 shows the abbreviations used in the research.

5. Simulation and Methodology

To implement the concept of Urdu Sign Language symbols by computer, we used Core i5 laptop with Windows 10. We used 8 GB RAM and 256 GB SSD card. Urdu Sign Langue's different symbols were provided as input to the dataset for training the model. The authors used Python-based programming environment and embedded the image processing and deep learning techniques such as OpenCV and TensorFlow. The NumPy IDE is used for the programming setup. NumPy stands for "Numerical Python" and is a Python module. It was used to calculate numerical values. Two datasets are used as number system symbols provided by Sindh welfare association and alphabet symbols used for deaf people. It has many logarithmic processing operations, including differentiation and integration. Multidimensional array is used to store the information sign langauge in the computer memory. The model is imported into the system, followed by the setup, which includes parameters such as the maximum number of hands and the confidence level. To display the human-readable output on the screen, a file with a name index is loaded. Open Computer Vision comes now and gets images from files or cameras (live feed). Then, the frame is prepared for detection and recognition. The model detects and draws the landmarks on that frame. The prediction model takes these landmarks as input and outputs the prediction as class id which is then later matched with the index of name file. Table 2 is used for simulation setup of the proposed model, and the parameters are referenced from [38–40].

Table 2 is used for simulation setup for the evaluation and implementation of the proposed system. Programming language is defined and provided; if anyone wants to work further in the research area, then he/she can know about the programming language used in the research. Other libraries of Python which are used in the proposed research are provided in Table 2. After completion of the proposed system, we feed live video to the model, and images shown in Figure 6 were drawn. As

Table 1: Abbreviation table.

Abbreviation	Full form
PSL	Pakistan Sign Language
ReLU	Rectified linear unit
CNN	Convolutional neural network
ASL	American Sign Language
NIDCD	National Institute on Deafness and Other Communication Disorders
BSL	British Sign Language
ArSL	Arabic Sign Language
SSL	Spanish Sign Language
SLR	Sign language recognition
IT	Information technology
ISL	Indian Sign Language
HCI	Human-computer interaction
PSL	Portuguese Sign Language
PC	Personal computer

Table 2: Simulation setup components.

S. No.	Field	Component
1	Programming language	Python 3
2	Modules for detection	Open Computer Vision, TensorFlow, Keras
3	Modules for training	Open Computer Vision, TensorFlow, Keras, Pandas, sklearn

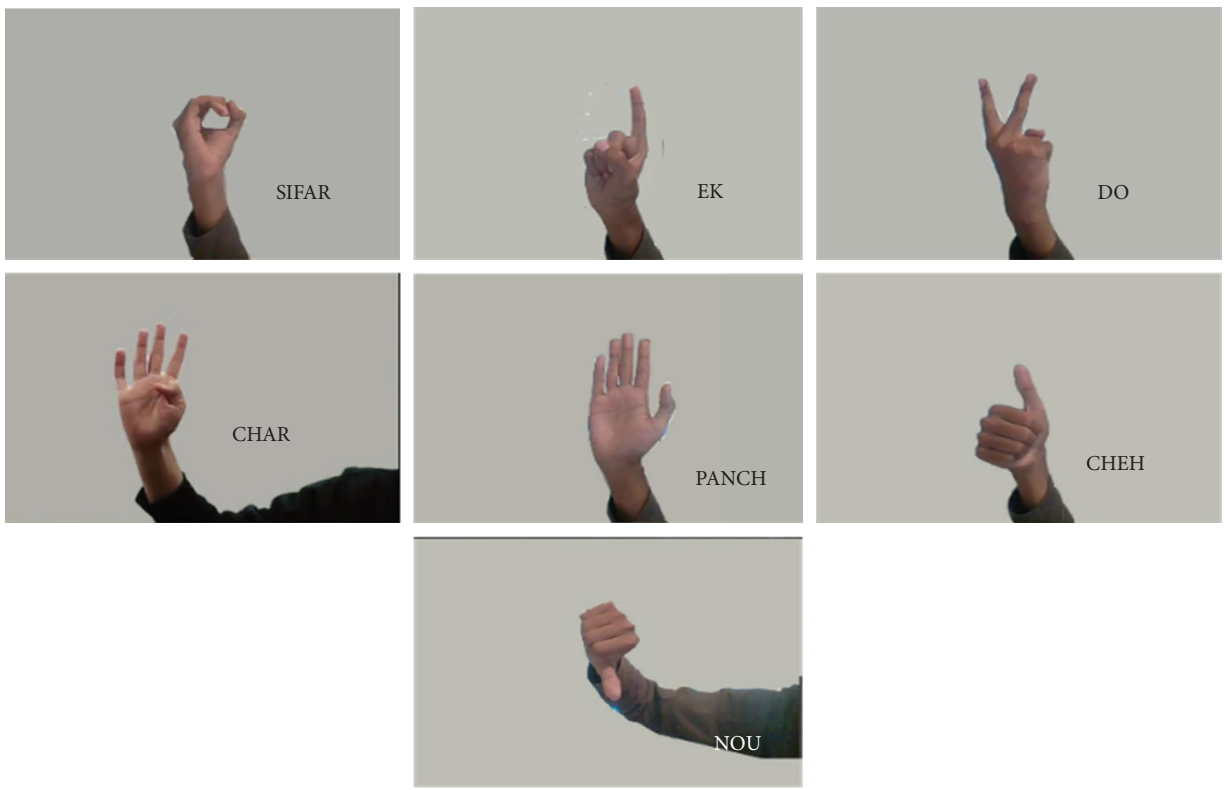


Figure 8: Live video feed results from the proposed model.

shown in Figure 8, the proposed model is evaluated based on live feed video, and when we showed the Urdu Sign Language symbols one by one, the proposed model recognized the symbols and provided them in written form on real-time basis.

6. Results

Furthermore, we trained the model in different simulations runs, and the following results were obtained as shown in Figures 9–12.

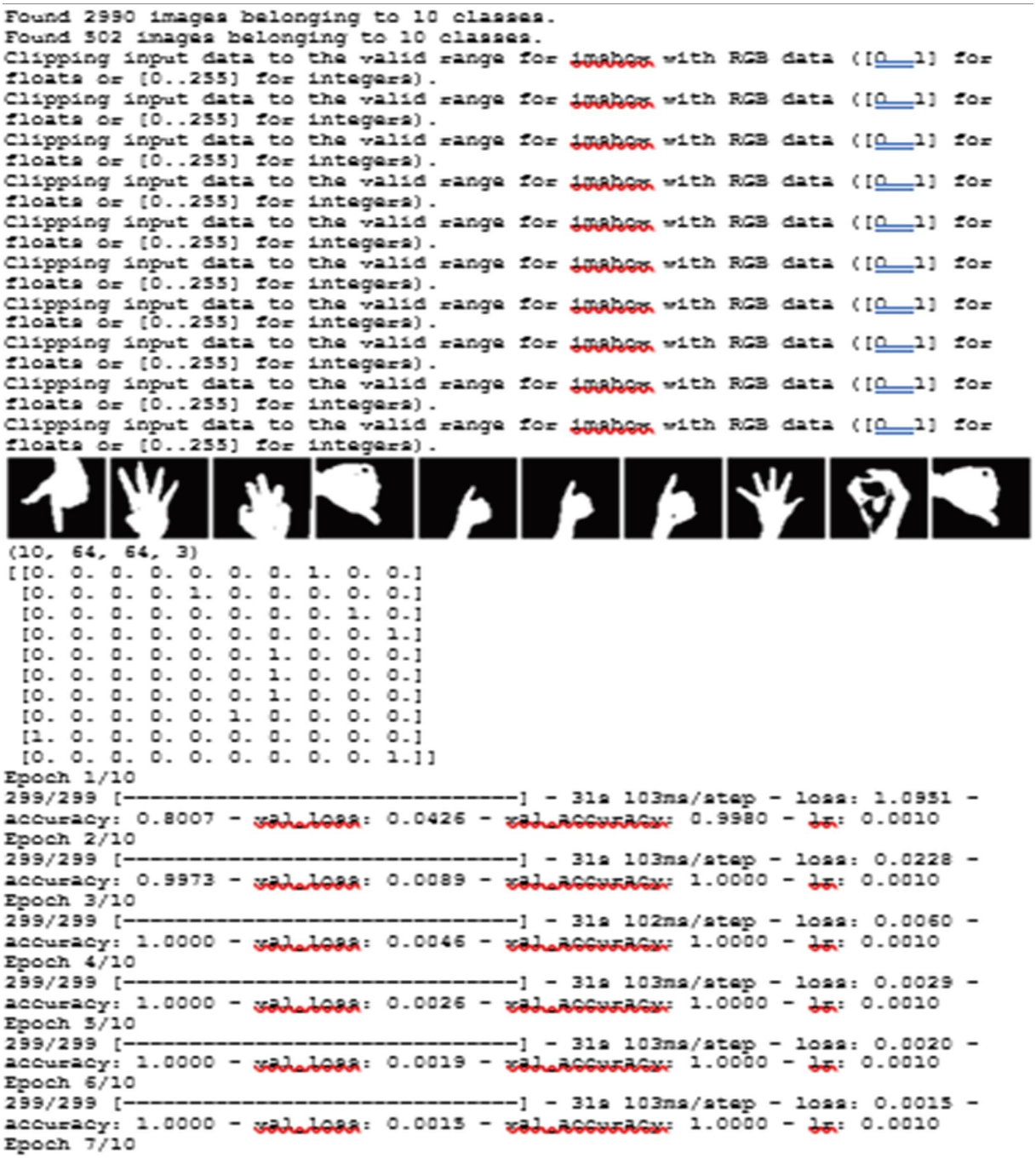


Figure 9: Result of the proposed model 1.

As shown in Figures 7–10, the proposed model accurately recognized the Urdu Sign Language symbols form the live video, and hence it can be told that the proposed model is an efficient model for deaf people to communicate with normal people. Furthermore, the accuracy of the proposed is evaluated and provided in the following figures.

As shown in Figure 13, the proposed model's accuracy with linear regression was 100% while using TensorFlow, the accuracy was 97% as some of the pictures were not recognized correctly.

As compared with the latest work, our proposed model performs very well as the previous work provided the accuracy up to 80% and we improved the accuracy up to 100%, and the proposed model can easily convert the Urdu Sign Language symbols into voice and alphabets. In Figure 14, RMSE of the proposed model is provided. When the model initially started its training, the root mean square error was

```
299/299 [==============================] - 31s 104ms/step - loss: 0.0012 -
accuracy: 1.0000 - val_loss: 0.0011 - val_accuracy: 1.0000 - lr: 0.0010
Epoch 8/10
299/299 [==============================] - 31s 103ms/step - loss: 9.7756e-04
- accuracy: 1.0000 - val_loss: 9.6149e-04 - val_accuracy: 1.0000 - lr: 0.0010
Epoch 9/10
299/299 [==============================] - 31s 105ms/step - loss: 8.1869e-04
- accuracy: 1.0000 - val_loss: 8.1612e-04 - val_accuracy: 1.0000 - lr: 0.0010
Epoch 10/10
299/299 [==============================] - 32s 106ms/step - loss: 7.1409e-04
- accuracy: 1.0000 - val_loss: 7.2608e-04 - val_accuracy: 1.0000 - lr: 0.0010
loss of 0.0002975249080918729 3; accuracy of 100.0%
{'loss': [1.0950770378112793, 0.022833531054854393, 0.005968990270048 38,
0.002935325726866722, 0.001999481115490198, 0.0015140236355364323,
0.0011748004471883178, 0.0009775563376024365, 0.0008186884806491435,
0.0007140882662497461], 'accuracy': [0.8006688952445984, 0.9973244071006775,
1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0], 'val_loss': [0.04260633513331413,
0.008947278372943401, 0.004601104184985161, 0.00264947721734643,
0.0018566565122455359, 0.0014645023038610816, 0.0011406627018004656,
0.0009614907903596759, 0.0008161191944964 23, 0.0007260802667587996],
'val_accuracy': [0.9980079531669617, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 1.0,
1.0], 'lr': [0.001, 0.001, 0.001, 0.001, 0.001, 0.001, 0.001, 0.001, 0.001,
0.001]}
loss of 0.0012862437870353 46; accuracy of 100.0%
Model: "sequential_7"
_________________________________________________________________
 Layer (type)                 Output Shape              Param #
=================================================================
 conv2d_21 (Conv2D)           (None, 62, 62, 32)        896

 max_pooling2d_21 (MaxPoolin  (None, 31, 31, 32)        0
 g2D)

 conv2d_22 (Conv2D)           (None, 31, 31, 64)        18496

 max_pooling2d_22 (MaxPoolin  (None, 15, 15, 64)        0
 g2D)

 conv2d_23 (Conv2D)           (None, 13, 13, 128)       73856

 max_pooling2d_23 (MaxPoolin  (None, 6, 6, 128)         0
 g2D)

 flatten_7 (Flatten)          (None, 4608)              0

 dense_28 (Dense)             (None, 64)                294976

 dense_29 (Dense)             (None, 128)               8320

 dense_30 (Dense)             (None, 128)               16512

 dense_31 (Dense)             (None, 10)                1290

=================================================================
Total params: 414,346
Trainable params: 414,346
Non-trainable params: 0
```

Figure 10: Result of the proposed model 2.

```
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
predictions on a small set of test data--

Three   Six   Four   One   Eight   Seven   Nine   Three   Seven   One
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
Clipping input data to the valid range for imshow with RGB data ([0..1] for
floats or [0..255] for integers).
```

```
Actual labels
Three   Six   Four   One   Eight   Seven   Nine   Three   Seven   One   (10,
64, 64, 3)
{'accuracy': [0.8006688952445984,
  0.9973244071006775,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0],
 'loss': [1.0950770378112793,
  0.02283531054854393,
  0.00596899027004838,
  0.002935325726866722,
  0.001999481115490198,
  0.0015140236355364323,
  0.0011748004471883178,
  0.0009775563376024365,
  0.0008186884806491435,
  0.0007140882662497461],
 'lr': [0.001, 0.001, 0.001, 0.001, 0.001, 0.001, 0.001, 0.001, 0.001,
0.001],
 'val_accuracy': [0.9980079531669617,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0,
  1.0],
 'val_loss': [0.04260633513331413,
  0.008947278372943401,
  0.004601104184985161,
  0.002649477721734643,
  0.0018566565122455359,
  0.0014645023038610816,
  0.0011406627018004656,
  0.0009614907903596759,
  0.0008161191944964233,
  0.0007260802667587996]}
```

Figure 11: Result of the proposed model 3.

Figure 12: Result of the proposed model 4.

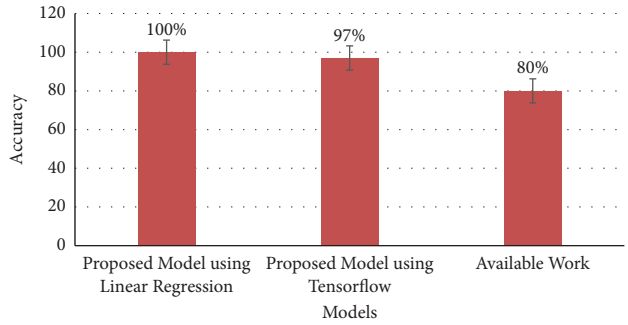


Figure 13: Accuracy of the proposed model.

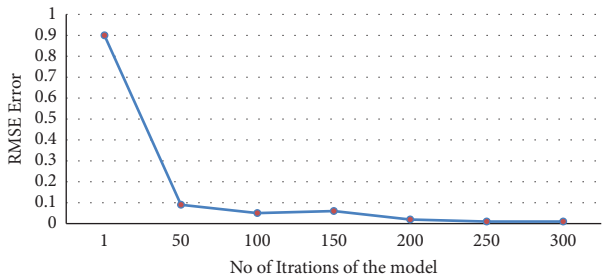


Figure 14: Root mean square error.

high, while after some iterations, the error decreased as shown in Figure 14.

7. Conclusion

In this paper, we provided an image processing and deep learning-based model for Urdu Sign Language. The proposed model is implemented in Python 3 and used different image processing and machine techniques to capture the video and transform the symbols into voice and Urdu writing. First, we get a video from the deaf person, and then the model crops the frames in pictures. Then, the individual picture is recognized for the sign symbol such as if the deaf showed a symbol for one, then the model recognizes it and shows the letter which he/she wants to tell. Image processing technique such as OpenCV is used for image recognition and classification while TensorFlow and linear regression are used for training the model to behave intelligently in the future. The results show that the proposed model increased accuracy from 80% to 97% and 100% accordingly. The accuracy of the previously available work was 80% when we implemented the algorithms, while with the proposed algorithm, when we used linear regression, we achieved the highest accuracy. Similarly, when we used the TensorFlow deep learning algorithm, we achieved 97% accuracy which was less than that of the linear regression model. In future work, we need to implement and develop a mobile-based model to help the deaf people in normal societies.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was sponsored by the Department of Computer Science and Engineering, University of Liberal Arts Bangladesh (ULAB), Dhaka, Bangladesh

References

[1] E. Emerson and C. Hatton, *Health Inequalities and People with Intellectual Disabilities*, Cambridge University Press, Cambridge, UK, 2014.

[2] A. Kuenburg, P. Fellinger, and J. Fellinger, "Health care access among deaf people: table 1," *Journal of Deaf Studies and Deaf Education*, vol. 21, no. 1, pp. 1–10, 2016.

[3] A. Kumar, S. Kumar, S. Singh, and V. Jha, "Sign Language recognition using convolutional neural network," in *ICT Analysis and Applications*, , pp. 915–922, Springer, 2022.

[4] S. Vachmanus, A. A. Ravankar, T. Emaru, and Y. Kobayashi, "Multi-modal sensor fusion-based semantic segmentation for snow driving scenarios," *IEEE Sensors Journal*, vol. 21, no. 15, pp. 16839–16851, 2021.

[5] R. Elakkiya, "Retracted article: machine learning based sign language recognition: a review and its research Frontier," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 7, pp. 7205–7224, 2021.

[6] S. Sharma and S. Singh, "Vision-based hand gesture recognition using deep learning for the interpretation of sign language," *Expert Systems with Applications*, vol. 182, Article ID 115657, 2021.

[7] A. Khelalef, F. Ababsa, and N. Benoudjit, "An efficient human activity recognition technique based on deep learning," *Pattern Recognition and Image Analysis*, vol. 29, no. 4, pp. 702–715, 2019.

[8] R. Mishra and R. Subban, "Face detection for video summary using enhancement based fusion strategy," *International Journal of Renewable Energy Technology*, vol. 3, no. 15, pp. 69–74, 2014.

[9] A. Middleton, S. D. Emery, and G. H. Turner, "Views, knowledge, and beliefs about genetics and genetic counseling among deaf people," *Sign Language Studies*, vol. 10, no. 2, pp. 170–196, 2010.

[10] A. Wadhawan and P. Kumar, "Sign language recognition systems: a decade systematic literature review," *Archives of Computational Methods in Engineering*, vol. 28, no. 3, pp. 785–813, 2021.

[11] M. Oudah, A. Al-Naji, and J. Chahl, "Elderly care based on hand gestures using kinect sensor," *Computers*, vol. 10, no. 1, p. 5, 2020.

[12] L. Meng and R. Li, "An attention-enhanced multi-scale and dual sign language recognition network based on a graph convolution network," *Sensors*, vol. 21, no. 4, p. 1120, 2021.

[13] L. Quesada, G. López, and L. Guerrero, "Automatic recognition of the American sign language fingerspelling alphabet to assist people living with speech or hearing impairments," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 4, pp. 625–635, 2017.

[14] N. Mohamed, M. B. Mustafa, and N. Jomhari, "A review of the hand gesture recognition system: current progress and future directions," *IEEE Access*, vol. 9, pp. 157422–157436, 2021.

[15] R. Elakkiya and K. Selvamani, "Subunit sign modeling framework for continuous sign language recognition," *Computers and Electrical Engineering*, vol. 74, pp. 379–390, 2019.

[16] D. K. L. Lee and P. Borah, "Self-presentation on Instagram and friendship development among young adults: a moderated mediation model of media richness, perceived functionality, and openness," *Computers in Human Behavior*, vol. 103, pp. 57–66, 2020.

[17] S. Kafle and M. Huenerfauth, "Predicting the understandability of imperfect English captions for people who are deaf or hard of hearing," *ACM Transactions on Accessible Computing (TACCESS)*, vol. 12, no. 2, pp. 1–32, 2019.

[18] N. S. Khan, A. Abid, and K. Abid, "A novel natural language processing (NLP)–based machine translation model for English to Pakistan sign language translation," *Cognitive Computation*, vol. 12, no. 4, pp. 748–765, 2020.

[19] A. Abbas and S. Sarfraz, "Developing a prototype to translate text and speech to Pakistan Sign Language with bilingual subtitles: a framework," *Journal of Educational Technology Systems*, vol. 47, no. 2, pp. 248–266, 2018.

[20] M. J. Cheok, Z. Omar, and M. H. Jaward, "A review of hand gesture and sign language recognition techniques," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 1, pp. 131–153, 2019.

[21] A. Mindess, *Reading between the Signs: Intercultural Communication for Sign Language Interpreters*, Nicholas Brealey, London, UK, 2014.

[22] A. Rashid and O. Hasan, "Wearable technologies for hand joints monitoring for rehabilitation: a survey," *Microelectronics Journal*, vol. 88, pp. 173–183, 2019.

[23] S. Hermawati and K. Pieri, "Assistive technologies for severe and profound hearing loss: beyond hearing aids and implants," *Assistive Technology*, vol. 32, 2019.

[24] M. Mahesh, A. Jayaprakash, and M. Geetha, "Sign language translator for mobile platforms," in *Proceedings of the 2017 International Conference on Advances in Computing, Communications, and Informatics (ICACCI)*, pp. 1176–1181, IEEE, Mangalore, India, September, 2017.

[25] B. L. Ludlow, "Virtual reality: emerging applications and future directions," *Rural Special Education Quarterly*, vol. 34, no. 3, pp. 3–10, 2015.

[26] S. Žilič Fišer, I. Kožuh, and I. Kožuh, "The impact of cultural events on community reputation and pride in Maribor, the European Capital of Culture 2012," *Social Indicators Research*, vol. 142, no. 3, pp. 1055–1073, 2019.

[27] S. Sankar Kumar, J. Jenitha, I. Narmadha, and A. Suganya, "An embedded module as "Virtual Tongue" for voiceless," *International Journal of Information Sciences and Techniques*, vol. 4, no. 3, pp. 155–163, 2014.

[28] M. Naseem, S. Sarfraz, A. Ali, and H. Ali, "Developing a prototype to translate Pakistan Sign Language into text and speech while using convolutional neural networking," *Journal of Education and Practice*, vol. 10, 2019.

[29] K. Kim, J. Choi, and S.-M. Lee, "Why does bundled product in telecommunication service market matter: evidence from South Korea," *International Journal of u-and e-Service, Science and Technology*, vol. 9, no. 3, pp. 209–226, 2016.

[30] N. Raziq and S. Latif, "Pakistan sign language recognition and translation system using leap motion device," in *Proceedings of the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pp. 895–902, Springer, Asan-si, Korea, November, 2016.

[31] A. Fatima and K. Huma, *Image Based Pakistan Sign Language Recognition System*, 2011.

[32] S. Kausar, M. Y. Javed, and S. Sohail, "Recognition of gestures in Pakistani sign language using fuzzy classifier," in *Proceedings of the 8th Conference on Signal Processing, Computational Geometry and Artificial Vision*, pp. 101–105, World Scientific and Engineering Academy and Society (WSEAS), Rhodes, Greece, August, 2008.

[33] B. Garcia and S. A. Viesca, "Real-time American sign language recognition with convolutional neural networks," *Convolutional Neural Networks for Visual Recognition*, vol. 2, pp. 225–232, 2016.

[34] D. S. Quentin, H. Wannous, and J. P. Vandeborre, "Skeleton-based dynamic hand gesture recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 1–9, Las Vegas, NV, USA, June, 2016.

[35] O. Koller, N. C. Camgoz, H. Ney, and R. Bowden, "Weakly supervised learning with multi-stream CNN-LSTM-HMMs to discover sequential parallelism in sign language videos," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 42, no. 9, pp. 2306–2320, 2020.

[36] J. Lien, N. Gillian, M. E. Karagozler et al., "Soli: ubiquitous gesture sensing with millimeter wave radar," *ACM Transactions on Graphics*, vol. 35, no. 4, pp. 1–19, 2016.

[37] L. Zou, J. Zheng, C. Miao, M. J. Mckeown, and Z. J. Wang, "3D CNN based automatic diagnosis of attention deficit hyperactivity disorder using functional and structural MRI," *IEEE Access*, vol. 5, pp. 23626–23636, 2017.

[38] F. J. Ordóñez and D. Roggen, "Deep convolutional and lstm recurrent neural networks for multimodal wearable activity recognition," *Sensors*, vol. 16, no. 115, 2016.

[39] H. Zahid, M. Rashid, S. Hussain, F. Azim, S. A. Syed, and A. Saad, "Recognition of Urdu sign language: a systematic review of the machine learning classification," *PeerJ Computer Science*, vol. 8, p. e883, 2022.

[40] M. P. Kane, S. Fernandes, R. Fonseca, S. Desai, A. Shetye, and A. Sharma, "Sign Language apprehension using convolution neural networks," in *Proceedings of the 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–7, IEEE, Kharagpur, India, October, 2022.

[41] E. Fatima, W. Naeem, and I. Abbas, "The influence of gender on the discourse markers in pakistani sign language," *Pakistan Journal of Scientific Research*, vol. 4, no. 2, pp. 1201–1207, 2022.

Hindawi
Mobile Information Systems
Volume 2023, Article ID 5828671, 9 pages
https://doi.org/10.1155/2023/5828671

Research Article

Multihop Uplink Communication Approach Based on Layer Clustering in LoRa Networks for Emerging IoT Applications

Alain Bertrand Bomgni,[1,2] **Hafiz Munsub Ali**,[3] **Mohammed Shuaib**,[4,5] **and Yann Mtopi Chebu**[2]

[1]*University of South Dakota, Vermillion, SD, USA*
[2]*University of Dschang, Dschang, Cameroon*
[3]*Binghamton University, Vestal, NY, USA*
[4]*College of Computer Science and IT, Jazan University, Jazan, Saudi Arabia*
[5]*University Center for Research & Development (UCRD), Department of Computer Science and Engineering, Chandigarh University, Gharuan, Mohali 140413, Punjab, India*

Correspondence should be addressed to Alain Bertrand Bomgni; alain.bomgni@usd.edu

Received 2 November 2022; Revised 20 November 2022; Accepted 25 April 2023; Published 20 May 2023

Academic Editor: Junaid Shuja

LoRa technology is widely used in the Internet of things network applications. It enables low-volume data transmission via small wireless devices. The principle of LoRa networks (an LPWAN technology: Low Power Wide Area Network) is to transmit data by air from sensors with a short transmission range, about over ten kilometers. These sensors should not be powered by electricity, and batteries power them. Hospital visits are inevitable, but current advances in communication could reduce the burden on hospitals with remote (from home) treatments using these wireless sensors. Thus, using the LoRaWAN protocol could greatly facilitate patient diagnosis by transmitting data between doctors and patients in real time and with minimal energy consumption. The objective of this work is to set up a multihop IoT network containing a large number of sensors based on LoRa for uplink communication. This work evaluates the energy consumption and the packet delivery rate in the multihop IoT network. The simulation result shows that the proposed approach reduces power consumption by 50% and improves the packet delivery rate by 2% compared to the existing state of the art.

1. Introduction

The Internet of things (IoT) is experiencing considerable scientific expansion in several areas, facilitating the exchange of information between objects, hardware, and software resources [1–5]. Technological advancements in the field of IoT have enabled the development of a wide variety of applications such as precision agriculture (PA), smart city, asset tracking, health care, and many more [6, 7]. Most of these applications require long-range communications with characteristics such as low data rate, low deployment cost, low power consumption, and security management [8–11]. Thus, short range radio technologies are not very suitable for wide coverage applications. A wide range of data acquisition objects already participate in a broad spectrum of applications that significantly consider long-range communication with low power consumption to extend network life without human intervention [11]. Thus, these growing needs have led to the emergence of Low Power Wide Area Networks (LPWANs). LPWAN is a type of wireless communication that is positioned as a connectivity facilitator for IoT applications or for cellular networks. Indeed, cellular solutions have the advantage of offering long connectivity but are energy intensive [11, 12]. LPWAN technology has experienced considerable growth because it has a set of interesting features among which we can mention scalable deployment, high energy efficiency, low management, and operating costs. Indeed, LPWAN technology makes it possible to build networks made up of thousands of objects with a long range (several kilometers) [13]. Figure 1 [11]

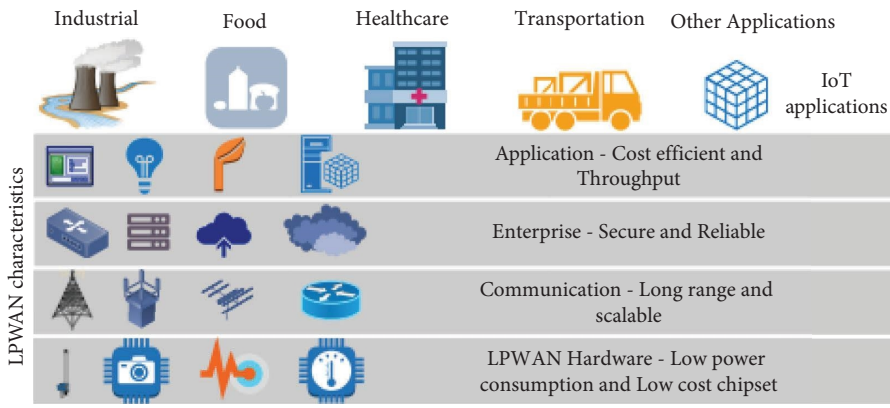


Figure 1: LPWAN characteristics make it an excellent choice for the IoT applications [11].

presents an architecture of LPWAN technology that facilitates the increase in the number of IoT applications. You can see a panoramic view of the functionalities at different layers as an added value for many applications. In the literature, there are several licensed and unlicensed LPWAN technologies, and among them, the most used solutions are LoRaWAN, Sigfox, and NB-IoT [11, 14].

LoRaWAN is an LPWAN-based communication solution that was designed to take advantage of a long-range, low-cost, and low-power hub-and-spoke network [15]. A LoRaWAN network consists of three essential components as follows: the terminals, the gateway, and then a link to the server, as shown in Figure 2. In addition, security (end-to-end encryption in the various communications) is an important element taken into account in LoRaWAN solutions. Such a LoRaWAN network consists of objects equipped with sensors or actuators that use the LoRa physical layer to exchange messages with the [16] gateway.

Remote health care and remote patient monitoring are concepts that have captured the attention of researchers in recent years [7]. Indeed, a smart home equipped with several objects capable of remotely monitoring one or more patients appears to be an interesting solution nowadays. Specifically, such technology can be an alternative for monitoring disabled people, quarantined people, and people with chronic illnesses. IoT provides an environment of objects connected to cloud-based applications and services, with different cooperation mechanisms, appropriate standardization, and advanced sensors with low-cost and low-power microprocessors [17, 18]. According to Figure 3, LoRaWAN is considered as one of the best IoT solutions based on the healthcare monitoring system due to its wide communication range and perfect interoperability between IoT sensors.

In this work, we have explained a multihop communication protocol over a large-scale area with LoRa devices while ensuring a deterministic and intelligent choice of the gateway which must redirect the information submitted by a device to guarantee, for example, a real-time information treatment by the server while minimizing the amount of energy.

This protocol takes place in two phases. A first phase consists of subdividing the networks into different layers and a second phase during which each device chooses the relay gateway for uplink communications.

We proposed a layered multihop clustering method for structuring large-scale networks. For this purpose, we supposed that the communications between two-end devices are reliable. The proposed algorithm tries to minimize the energy consumption spent during the formation of the layers. We obtained an acceptable packet delivery rate, and the number of messages sent is very low. Moreover, the proposed protocol is energy efficient extending by the way of IoT device battery life time, and it has a linear time complexity which is an asset for real-time IoT applications.

The rest of this paper is organized as follows: Section 2 presents a state of the art on some LoRa protocols, a mathematical formulation of the problem is presented in Section 3, our approach is presented in Section 4, the results of the experiments are presented in Section 5, and finally, the conclusion and some future works are presented in Section 6.

2. Review of the Literature

2.1. LoRa and LoRaWAN. Long Range (LoRa) is Semtech's spread spectrum modulation technique, a proprietary communication standard that enables long range, single-hop communications. With LoRa technology, it is possible to decode transmissions of up to 19.5 dB on a noise floor [21–23]. This technique allows the reception of a multiple number of messages on channels, an orthogonal separation between the signals. This offers an advantage in the management of the flow.

A characteristic of LoRa is that it offers an improvement of criteria such as SF (spreading factor), TP (transmission power), CR (coding rate), and BW (bandwidth) with a relation given by equation (1) [23–25].

$$R_b = \mathrm{SF} \times \frac{\mathrm{BW}}{2^{SF}} \times \mathrm{CR}. \quad (1)$$

This technology is based on the ISM (industrial, scientific, and medical) bands, whose distribution of frequencies and regulations vary according to the region of the world. The two frequencies mainly used are 868 MHz in Europe and 915 MHz in North America. This physical layer relies on an alternative Spread Spectrum Modulation (SSM) called Chirp Spread Spectrum (CSS) which spreads the base signal over

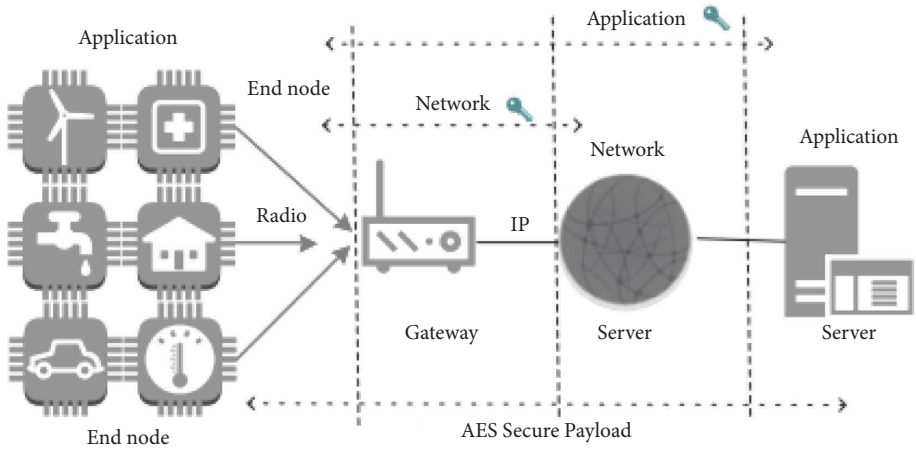


Figure 2: LoRaWAN network architecture [11].

Network topologies	Topology	Radio frequency	Range	Data rate	Energy Consomption
BLE	Ad hoc	2.4 GHz	10 m	1-2 Mb/s	Very Low
ZibBee	Mesh	868.3 MHz, 2.4 GHz	100 m	0.02-0.25 Mb/s	low
WIFI	Star	2.4 GHz	Less than 1 km	11 Mb/s - 10 Gb/s	High
SigFox	Star	Between 862 and 928 MHz	10 Km	100-600 b/s	Medium
LoraWan	Star or peer to peer	Between 860 and 1020 MHz	Less than 30 Km	Up to 50 Kb/s	Very Low

Figure 3: Comparison between different specifications of network technology [13, 19, 20].

a given frequency domain and increases mean bandwidth with the aim of increasing resistance to interference, reducing energy consumption, and integrating an error-correcting code. This type of modulation, widely used for radar applications in the past, is now necessary for low-speed communications. During a transmission, the spreading factor is adjustable and imposes a preliminary search to optimize the value according to various criteria. Indeed, starting from a fixed pass-band, a high SF directly implies an increase in the range and in the transmission delay T_s of a symbol expressed in seconds. The latter can be calculated using Formula (2). On the other hand, still in the case of a high SF, the communicating system sees its bit rate decreasing but has better reception sensitivity. Formula (1) presents the relationship between the final flow rate and the spreading factor [26].

$$T_s = \frac{2^{SF}}{\mathrm{BW}}. \tag{2}$$

In LoRa, there are several types of equipment among which we can mention the following: terminals, gateways, servers, application servers, and Join Server; a layout of a LoRa architecture is given by Figure 4.

LoRaWAN is a robust solution competing with other LPWANs by taking up the strengths of LoRa technology while having a strong influence on battery life, network load capacity, quality of service, and security. The LoRaWAN

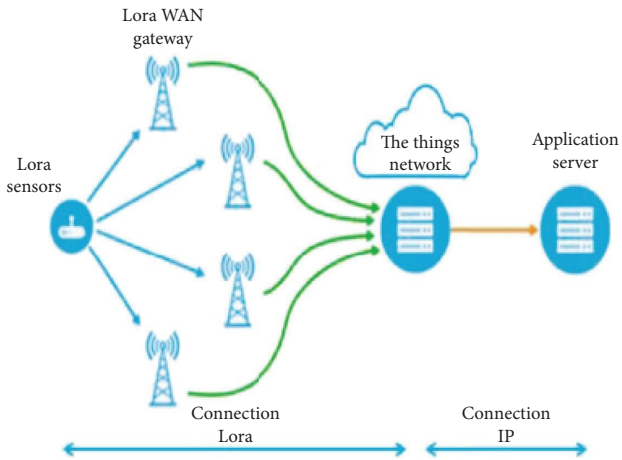


Figure 4: LoRaWAN technology [27].

network is organized according to a star of stars topology. The communication proposed in this network is bi-directional while clearly favoring uplink transmissions towards the concentrators [15]. This organization, illustrated in Figure 4, is in fact composed of a multitude of concentrators which relay the information received from the nodes to a central server using a GSM or Ethernet protocol most of the time. The central server makes it possible to eliminate duplicates received by the various concentrators and manages the flow rates of the nodes in order to optimize the

capacity of the network and to extend the autonomy of the wireless devices.

2.2. Multihop Communications in LoRa Networks. In [22], the authors propose an algorithm which addresses three main criteria which are load balance in the network, reduction of the number of hops between the root, and a terminal and connectivity problem, using a faster throughput (higher SF) for connections for insertion of each node away from the root with the Topdown Breadth First-Search (TBFS) algorithm. This protocol uses long range communications for subtree formations, which requires a higher spreading factor and therefore additional energy consumption.

In [24], the author proposes new multihop clustering algorithm LoRaWAN networks. This approach is divided into two steps. The first one allows to form the layers, and the second one allows to choose the gateway for the communications to the root. For the layer formation, the protocol modifies the initial structure by adding elements of layer identifications by the gateways. The process is managed by the root which sends a broadcast with a hop count of 0 for the identification of the first layer. The answers of the elements of this layer allow him to make another diffusion for the identification of the following layer by passing by layer 0. Layer 1 sends an answer, and the process proceeds thus until obtaining all the layers. The selection is made from the RSSI of each gateway except for this one at a layer lower than a node. It has been compared to the method proposed in [28]. It also proposes an approach of multihop communication in LoRa and has LoRaWAN. This method thus allows a good communication between terminals over a long distance. However, the layer formation mechanism is very tedious when the number of layers is very high and would consume a lot of time and energy.

In [29], a protocol that maintains connectivity and coverage with the network using multihop communications is proposed. Evaluations are made on parameters such as the spreading factor and the packet reception rate. This protocol shows how in a smart city, the use of LoRa technology with multihop communications can save energy, ensure network coverage, and good connectivity. However, the use of the spread spectrum factor is still very high. This increases the energy consumption of the nodes.

In [30], it is proposed to use a simple relay device to increase the LoRaWAN coverage area for rural areas. The authors suggested deploying relay nodes by knowing the locations that are not covered by the gateway. The authors proposed a simple message forwarder and a synchronization mechanism. They showed that the energy consumption decreases with the addition of the relay node to deliver the packets. This method saves energy by minimizing retransmissions and increases the network connectivity rate. However, this protocol is only valid for a maximum of 2 hops. This does not allow for scalability.

In [31], the authors propose a transmission protocol (concurrent transmission) which proceeds by flooding the network for the design of multihop communications. The transmission of packets is done by transmitting identical packets in a synchronous manner, which increases the efficiency of the network by solving the problem of packet collisions. Although this protocol improves the efficiency of the multihop network and is robust against collisions, it results in a huge energy consumption due to the numerous identical messages broadcasted through the network.

3. Problem Formulation

We consider $\{gw_1, gw_2, \ldots, gw_g\}$ the set of gateways in the network, $\mathrm{DV} = \{dv_1, dv_2, \ldots, dv_d\}$ the set of LoRa terminals in the network that need to be dispersed in layers, and $C = \{c_1, c_2, \ldots, c_c\}$ the set of formed layers in the network. We seek to improve the operation of large-scale LPWANs by considering the multiobjective problem (energy-efficient formation of layers and intelligent selection of the best gateway). The selection of the best gateway is given by

$$dv_i = \left\{ g_j \in E_i | j = \arg\min_k \left(f\left(g_k, dv_i\right)\right)\right\}, \tag{3}$$

où.

(1) dv_i is the set of gateways determined as follows:

$$dv_i \| E_i \| = \sum_{i=1}^{i=g} Li,$$
$$L = \begin{cases} 1, & si\ d\left(dv_i\ g_k\right) \leq R\ \forall k \in \{1, 2, \ldots, g\}, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

(2) f is the objective function of each terminal in relation to a gateway.

This problem is formulated subject to the constraints as follows:

(1) Let $\mathrm{alpha}_{i,j}$ be a binary value which indicates the admission of the device dv_i to the gateway g_j.

(2) $\sum_{k \in dv} \alpha_{k,j} = 1$.

(3) $\forall i, j \in GW,\ g_i \cap g_j = \varnothing$.

4. Multihop Uplink Communication Approach

In this section, we present an efficient approach to multiobjective routing in a LoRa network based on layer clustering. This approach is divided into two steps. The first one is to form layers, and the second one is to select the best gateway for routing data to the root.

4.1. Assumptions

(1) The nodes are randomly deployed on a square surface

(2) The transmission radio is the same for each equipment

(3) The gateways are deployed in a deterministic way to ensure the coverage of the deployment area

```
layer_id = ∞;
if id = = 0 then
   CREATE_DIS_MESSAGE (1, 0, 0, 0);
   BROADCAST (DIS);
end if
if DIS message then
   if DIS. L_ID ¡ layer_idthen
      gtwlayer_id = DIS.L_ID
      CREATE_DIA_MESSAGE (M_ID + 1, gtwlayer_id + 1, H_CNT + 1, ID);
      UNICAST (DIA);
      CREATE_DIS_MESSAGE (M_ID, gtwlayer_id, ID);
      BROADCAST (DIS);
      EXPIRER (timer);
      WAIT_UNTIL (timer);
      if EXPIRER (timer) then
         if Not DIA reception then
            CREATE_DIN_MESSAGE (id, layer_id, g);
            UNICAST (DIN)
         end if
      end if
   end if
end if
if DIN message then
   CREATE_DIN_MESSAGE (ID, gtwlayer_id, layer_id);
   UNICAST (DIN);
end if
```

Algorithm 1: Formation of the network layers.

4.2. Layer Formation. Each gateway has the following parameters for layer formation:

(1) id represents the identifier of the gateway

(2) layer_id is the layer number to which the gateway belongs

(3) *gwt* contains the id of its gateway to reach the root gateway

We define three types of messages for layer formation. A DIL (Discover Information Layer) and DIA (Discover Information Acceptance) which contain the fields L_{ID} for the layer number, H_{NT} is the number of hops from the root gateway, T_{NID} is the identifier of the node transmitting a DIA or DIL message, and finally, a gatewaylayer_id contains the identifier of the relaying gateway towards the root. A DIN (Direct Information Notification) message contains the fields ID for the identifier of the transmitting gateway, gatewaylayer_id contains the identifier of the relay gateway to the root, and layer contains the number of layers of the formed network.

The root gateway initiates the broadcast of a DIA message with the LID field set to 0 to indicate the start of the layering process. As soon as a DIS message is received, each gateway initiates a DIA message to indicate that the message has been received and initiates a DIS message again, this time with the LID number incremented by 1 and the hop number set to 1. It then sets a timer t and waits until the end of this time. If it has received another DIL message, it generates a DIL message and transmits it to its relay gateway.

Otherwise, it generates a DIL message and forwards it to its relay gateway and thus considers itself as the leaf node of the layered tree. The process repeats itself until layer $n-1$ receives DILs from layer n, transmits DILs to layer $n-2$, and so on until the DILs are distributed to the root. This will allow the root gateway to know the number of layers formed in the network. Algorithm 1 is executed by all the gateways for the formation of the network layers.

An illustration of this approach is presented in Figure 5. The root gateway in the center of the figure (purple color) illustrates the formation of the layers. The other gateways in green, red, and blue colors are Layer 1, Layer 2, and Layer 3 gateways, respectively.

4.3. Gateway Selection. This step consists of intelligently choosing a gateway in its layer to be able to route information to the root gateway. Once the layer formation is complete, each gateway will issue a broadcast message to tell each device which gateways in its layer, the upper and/or perhaps lower layer, where it can access. Each node will calculate its objective function to determine which gateway should be chosen to minimize energy consumption costs. Algorithm 2 is executed by all the end devices for the selected gateway.

$$f = w_1 \times \text{RSSI} + w_2 \times SF + w_3 \times \text{Layer\_id}, \tag{5}$$

where RSSI (Received Signal Strength Indication) is the received signal strength, SF (spreading factor) and Layer_id is the layer number of the gateway, and $w_1 + w_2 + w_3 = 1$.

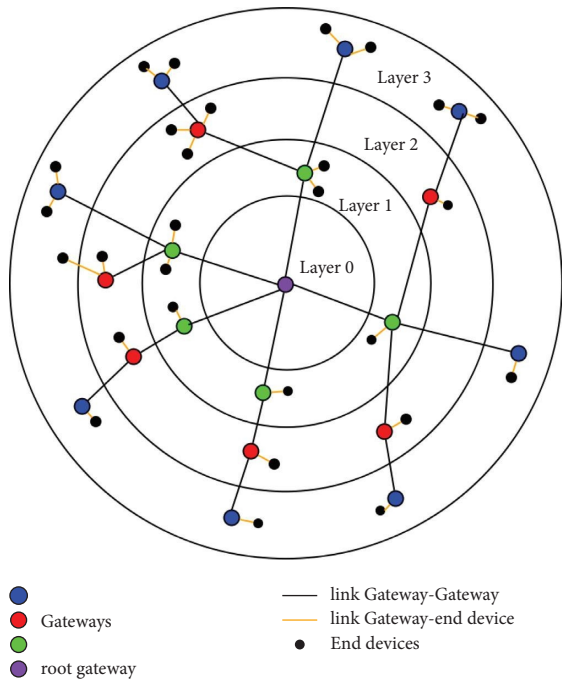


Figure 5: Example of layer formation.

∀ node n in network;
  ∀ receive g_i Broadcast;
    Compute f_i for Gateway g_i with formula $w_1 \times \text{RSSI} + w_2 \times SF + w_3 \times \text{Layer\_id}$;
  Select max (f_i) and send it unicast_message;

Algorithm 2: Selection of gateway.

For each gateway message received, the device evaluates the objective function f. It will therefore choose among the gateways in its layer, the gateway with the largest value of f.

5. Results

The simulation is conducted on an i5 series processor with 4 GB of RAM using LoRaSim. LoRaSim is a discrete-event simulator based on SimPy for simulating collisions in LoRa networks and to analyse scalability. Their simulator and the model energy are described in [32].

The simulation parameters are listed in Figure 6.

Figure 7 shows a comparison of the energy consumed by the RPL, Farooq, and LoRaWan protocols. We can observe that our protocol outperforms those of the others by consuming 50%, 70%, and 80% less than the Farooq protocols [24, 28] and LoRaWan.

We also bring an improvement in the packet delivery rate of 2% compared to [24] in Figure 8.

Figure 9 shows the number of messages sent for the layer formation process in the network. We see that compared to the Farooq protocol, the number of messages sent remains constant regardless of the number of layers formed in the network. This proves that the root gateway sends the same number of messages for the formation of the layers whatever the size of the network. So, it also proves that this protocol is suitable for large-scale networks.

Parameters	Value
Frequency	500 KHz
Initial Energy	5j
Bandwidth	125 KHz
Data Rate	250 bps
Spreading Factor	7
Coding Rate	4/5
Number of LoRaWAN Nodes	30-120
Number of Gateway	20-40
Number of Layers	1-20

Figure 6: Simulation parameters.

Figure 10 shows the number of messages sent for the layer formation process in the network. We see that compared to the Farooq protocol, the number of messages sent remains constant regardless of the number of layers formed in the network. This proves that the intermediate gateways send the same number of messages for the formation of the layers whatever the size of the network. Therefore, the

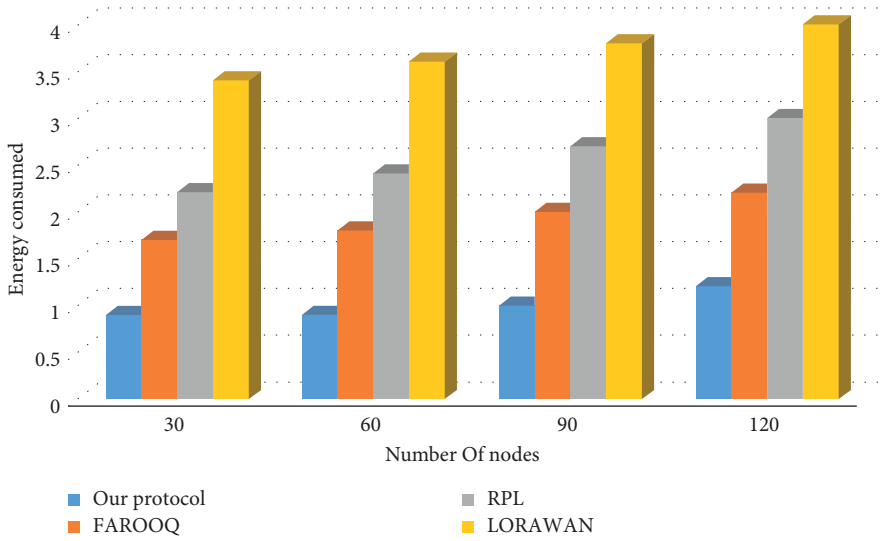


Figure 7: The comparison of energy consumption.

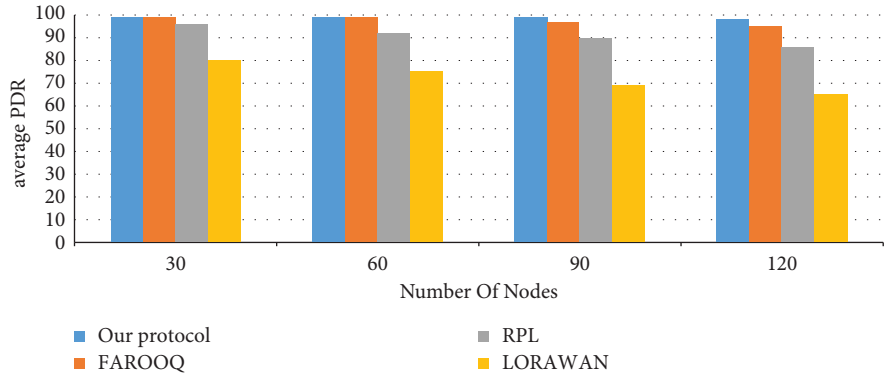


Figure 8: Mean packet delivery ratio (PDR).

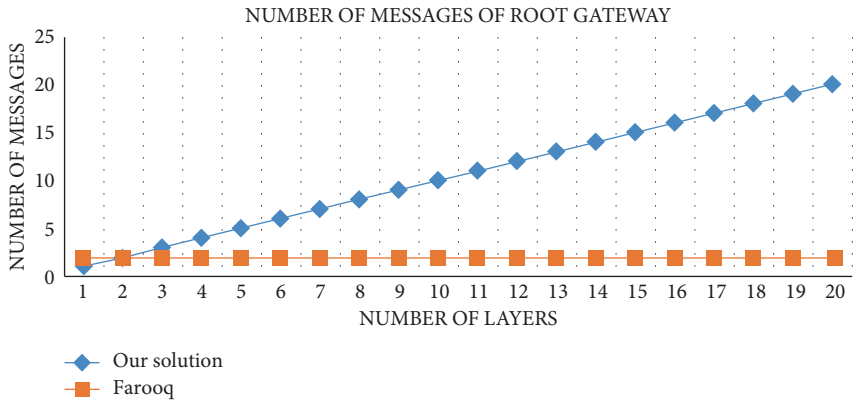


Figure 9: Number of messages sent by the root gateway.

scalability of the network has no impact on the messages sent by the intermediate gateways.

The protocol in the literature review sends too many messages in the case of the root gateway as well as in the case of the intermediate gateways, which indicates without a doubt that the energy consumption of this protocol is extremely high for the formation of layers in the network.

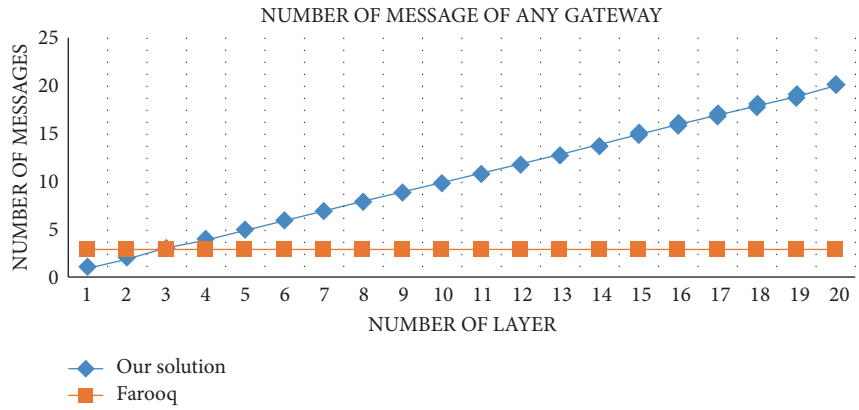


Figure 10: Number of messages sent by intermediate gateways.

6. Conclusion

In this article, we have proposed a low power system with LoRa technology. This system can be used to monitor the physiological parameters of a patient to determine his medical situation, in order to anticipate the aggravation of pathologies for patients and to reduce the time of hospitalization and cost, especially with the spread of the Covid pandemic. Our results showed very good efficiency in terms of system life, with autonomy gains multiplied by 2. Work is underway to improve the study surface.

Data Availability

No underlying data was collected or produced in this study.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent

Informed consent was obtained from all individual participants included in the study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. B. Bomgni, M. L. F. Sindjoung, D. K. Tchibonsou, M. Velempini, and J. F. Myoupo, "Neseprin: a new scheme for energy-efficient permutation routing in iot networks," *Computer Networks*, vol. 214, Article ID 109162, 2022.

[2] R. Zi, J. Liu, L. Gu, and X. Ge, "Enabling security and high energy efficiency in the internet of things with massive mimo hybrid precoding," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8615–8625, 2019.

[3] X. Ge, Y. Sun, H. Gharavi, and J. Thompson, "Joint optimization of computation and communication power in multi-user massive mimo systems," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 4051–4063, 06 2018.

[4] X. Ge, B. Yang, J. Ye, G. Mao, C.-X. Wang, and T. Han, "Spatial spectrum and energy efficiency of random cellular networks," *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 1019–1030, March 2015.

[5] J. Yang, X. Ge, J. Thompson, and H. G. Gharavi, "Power-consumption outage in beyond fifth generation mobile communication systems," *IEEE Transactions on Wireless Communications*, vol. 20, no. 2, pp. 897–910, Feb 2021.

[6] 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.

[7] H. M. Ali, J. Liu, S. A. C. Bukhari, and H. T. Rauf, "Planning a secure and reliable iot-enabled fog-assisted computing infrastructure for healthcare," *Cluster Computing*, vol. 25, pp. 2143–2161, 2022.

[8] Hafiz Munsub Ali, W. Ejaz, D. C. Lee, and I. Khater, "Optimising the power using firework-based evolutionary algorithms for emerging iot applications," *IET Nteworks*, vol. 15, 2019.

[9] A. Bomgni, B. Garrik, M. Jagho, M. A. Hafiz, G. Z. David, and G. Z. Etienne, "Espina: efficient and secured protocol for emerging iot network applications," *Cluster Computing*, vol. 24, 2022.

[10] Y. Brice Chebu Mtopi, A. Bertrand Bomgni, H. Munsub Ali, D. R. G. Zanfack, W. Ejaz, and E. Zohim, "Multihop optimal time complexity clustering for emerging iot applications," *Cluster Computing*, vol. 26, 2022.

[11] R. K. Singh, P. P. Puluckul, R. Berkvens, and M. Weyn, "Energy consumption analysis of lpwan technologies and lifetime estimation for iot application," *Sensors*, vol. 20, no. 17, p. 4794, 2020.

[12] W. Wang and G. Shen, "Energy efficiency of heterogeneous cellular network," in *Proceedings of the 2010 IEEE 72nd Vehicular Technology Conference - Fall*, Ottawa, Canada, September 2010.

[13] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of lpwan technologies for large-scale iot deployment," *ICT express*, vol. 5, no. 1, pp. 1–7, 2019.

[14] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2019.

[15] LoRaWAN, "Lora alliance," 2022, https://lora-alliance.org/about-lorawan/.

[16] LoRaWAN Specification, "Lora alliance," 2022, https://lora-alliance.org/resource-hub/lorawanr-specification-v11.

[17] N. Misran, M. S. Islam, G. K. Beng, N. Amin, and M. T. Islam, "Iot based health monitoring system with lora communication technology," in *Proceedings of the 2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, pp. 514–517, Bandung, Indonesia, July 2019.

[18] F. A. Muhammad, N. K. Abdul, J. Shuja, A. K. Iftikhar, G. K. Fiaz, and R. K. Atta, "A lightweight and compromise-resilient authentication scheme for iots," *Transactions on emerging telecommunications technologies*, vol. 33, 2019.

[19] A. Lavric and V. Popa, "Performance evaluation of lorawan communication scalability in large-scale wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6730719, 9 pages, 2018.

[20] D. Ismail, M. Rahman, and A. Saifullah, "Low-power wide-area networks: opportunities, challenges, and directions," in *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking*, Varnasi, India, January 2018.

[21] M. C. Bor, R. Utz, T. Voigt, and J. M. Alonso, "Do lora low-power wide-area networks scale?" in *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, New York City, NY, USA, November 2016.

[22] G. Zhu, C.-H. Liao, T. Sakdejayont, I.-W. Lai, Y. Narusue, and H. Morikawa, "Improving the capacity of a mesh lora network by spreading-factor-based network clustering," *IEEE Access*, vol. 7, pp. 21584–21596, 2019.

[23] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on lpwa technology: lora and nb-iot," *Ict Express*, vol. 3, no. 1, pp. 14–21, 2017.

[24] M. O. Farooq, "Clustering-based layering approach for uplink multi-hop communication in lora networks," *IEEE Networking Letters*, vol. 2, no. 3, pp. 132–135, 2020.

[25] M. Usmonov and F. Gregoretti, "Design and implementation of a lora based wireless control for drip irrigation systems," in *Proceedings of the 2017 2nd International Conference on Robotics and Automation Engineering (ICRAE)*, pp. 248–253, Shanghai, China, December 2017.

[26] X. Wang, M. Fei, and X. Li, "Performance of chirp spread spectrum in wireless communication systems," in *Proceedings of the 2008 11th IEEE Singapore International Conference on Communication Systems*, pp. 466–469, Guangzhou, China, November 2008.

[27] LoRaWAN, Oct 2020,https://lora-developers.semtech.com/library/tech-papers-and-guides/lora-and-lorawan/.

[28] B. Sartori, S. Thielemans, M. Bezunartea, B. An, and K. Steenhaut, "Enabling rpl multihop communications based on lora," in *Proceedings of the 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*,Rome, Italy, October 2017.

[29] M. S. Aslam, A. Khan, A. Atif et al., "Exploring multi-hop lora for green smart cities," *IEEE Network*, vol. 34, no. 2, pp. 225–231, 2020.

[30] Diop Mamour and C. Pham, "Increased flexibility in long-range iot deployments with transparent and light-weight 2-hop lora approach," *Wireless Days (WD)*, vol. 6, 2019.

[31] C.-H. Liao, G. Zhu, D. Kuwabara, M. Suzuki, and H. Morikawa, "Multi-hop lora networks enabled by concurrent transmission," *IEEE Access*, vol. 5, pp. 21430–21446, 2017.

[32] M. Bor, R. Utz, T. Voigt, and Juan Alonso, "Do lora low-power wide-area networks scale?" in *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pp. 59–67, New York city, NY, USA, November 2016.

Hindawi
Mobile Information Systems
Volume 2023, Article ID 7690322, 11 pages
https://doi.org/10.1155/2023/7690322

Research Article

Cognitive Lightweight Logistic Regression-Based IDS for IoT-Enabled FANET to Detect Cyberattacks

Khaista Rahman,[1] **Muhammad Adnan Aziz**,[2] **Nighat Usman**,[3] **Tayybah Kiren**,[4] **Tanweer Ahmad Cheema**,[1] **Hina Shoukat**,[5] **Tarandeep Kaur Bhatia**,[6] **Asrin Abdollahi**,[7] **and Ahthasham Sajid**[8]

[1]*Department of Electronic Engineering, School of Engineering and Applied Sciences, Isra University, Islamabad, Pakistan*
[2]*FoIT & CS, University of Central Punjab, Lahore, Pakistan*
[3]*Department of Computer Sciences, Bahria University Islamabad Campus, Islamabad, Pakistan*
[4]*Department of Computer Science (RCET), University of Engineering and Technology, Lahore, Pakistan*
[5]*Department of Computer Science, COMSATS University Islamabad, Attock Campus, Islamabad, Pakistan*
[6]*School of Computer Science, University of Petroleum & Energy Studies (UPES), Dehradun, Uttarakhand, India*
[7]*Department of Electrical Engineering, University of Kurdistan, Sanandaj, Iran*
[8]*Department of Computer Science, FICT, BUITEMS, Quetta, Pakistan*

Correspondence should be addressed to Asrin Abdollahi; a.abdollahi@eng.uok.ac.ir

Received 12 October 2022; Revised 22 October 2022; Accepted 25 November 2022; Published 29 April 2023

Academic Editor: Junaid Shuja

In recent few years, flying ad hoc networks are utilized more for interconnectivity. In the topological scenario of FANETs, IoT nodes are available on ground where UAVs collect information. Due to high mobility patterns of UAVs cause disruption where intruders easily deploy cyberattacks like DoS/DDoS. Flying ad hoc networks use to have UAVs, satellite, and base station in the physical structure. IoT-based UAV networks are having many applications which include agriculture, rescue operations, tracking, and surveillance. However, DoS/DDoS attacks disturb the behaviour of entire FANET which lead to unbalance energy, end-to-end delay, and packet loss. This research study is focused about the detail study of machine learning-based IDS. Also, cognitive lightweight-LR approach is modeled using UNSW-NB 15 dataset. IoT-based UAV network is introduced using machine learning to detect possible security attacks. The queuing and data traffic model is utilized to implement DT, RF, XGBoost, AdaBoost, Bagging and logistic regression in the environment of IoT-based UAV network. Logistic regression is the proposed approach which is used to estimate statistical possibility. Overall, experimentation is based on binomial distribution. There exists linear association approach in logistic regression. In comparison with other techniques, logistic regression behaviour is lightweight and low cost. The simulation results presents logistic regression better results in contrast with other techniques. Also, high accuracy is balanced well in optimal way.

1. Introduction

Integration of 5G wireless networks with FANETs is a new concept which uses to improve coverage and reduce delay [1–3]. Mobile ad hoc network is considered the primary idea where VANET and FANET are emerged. UAV swarms or group collectively make FANETs [4]. There can be either signal or multi-UAVs system. Initially, UAVs are only utilized to collect data from ground IoT nodes [5]. But, nowadays, aerial vehicles have changed the dynamics of every human which include smart farming using UAVs, rescue operations, border surveillance, and many more.

In comparison with other traditional fields, FANETs are very much cost low and can be deployed everywhere. The high mobility patterns of UAVs limit energy level in entire network. Due to wireless connectivity in FANETs, internet

of things plays an important role. Although, there exist two ways of communication which consist of a2a (air-to-air) and a2g (air-to-ground) [6]. Recently, Zigbee (IEEE 802.15.4) is introduced in FANETs for secure and long-range communication. Mobile UAV pattern effects quality of service (QoS) in the field of IoT-based FANETs. In the conventional UAV network, there exist satellite, ground base station, and UAVs [7].

FANET network needs to be secured from cyberattacks which reduce connectivity in between nodes and interrupt communication. False data attack is one of the dangerous threats during remote patient surgery or operation [8]. However, DoS/DDoS security attacks can be easily detected with the help of the intrusion detection system. Various research studies formulate that identification of cyberattacks in FANETs is considered a major problem [9]. Intruder/attacker UAVs can be used to steal data and jam potential links [10, 11]. Therefore, a proposed system model will consists of detecting ongoing cyberattacks like DoS/DDoS and ping of death which is referred to as dynamic-IDS. This research study will only expand to simulate detection of attacks in FANETs. Furthermore, topological arrangements of FANETs are shown in Figure 1. The main points of the research paper are as follows:

(i) Machine learning algorithms such as DT, RF, XGBoost, AdaBoost, Bagging and logistic regression are utilized

(ii) UNSW-NB 15 dataset is used for training and testing data

(iii) Cognitive lightweight-LR approach is proposed to detect attacks

(iv) Detailed comparative analysis is formulated using machine learning techniques

Major contribution points of this study elaborate the concept of machine learning algorithms which use to detect possible cyberattacks. Comprehensive study is evaluated to understand previous ideas and compare them with the proposed solution. UNSW-NB15 dataset is utilized for experimentation and performance analysis of machine learning classifiers.

Figure 1 illustrates the concept of UAV network using the concept of intruders. When unmanned aerial vehicles tries to collect data from IoT ground nodes at the same time attackers use to deploy fake data packets which leads miss information. Also, FANET network is presented which use to have base station, satellite, and UAVs.

Apart from that machine learning techniques are used in IoT, ad hoc networks, software define networks, and many other fields. Therefore, in machine learning data set is utilized which use to have detailed data for the specific area. Classifiers or algorithms are trained properly to evaluate the performance.

The rest of the article is structured with Section 1 which consists of the study introduction where Section 2 is composed of brief literature having past data about the problem. Similarly, machine learning algorithms in Section 3 and Section 4 represent the proposed model. Section 5 demonstrates simulation results. The theoretical analysis and future direction is discussed in Section 6, which is explained in the conclusion section.

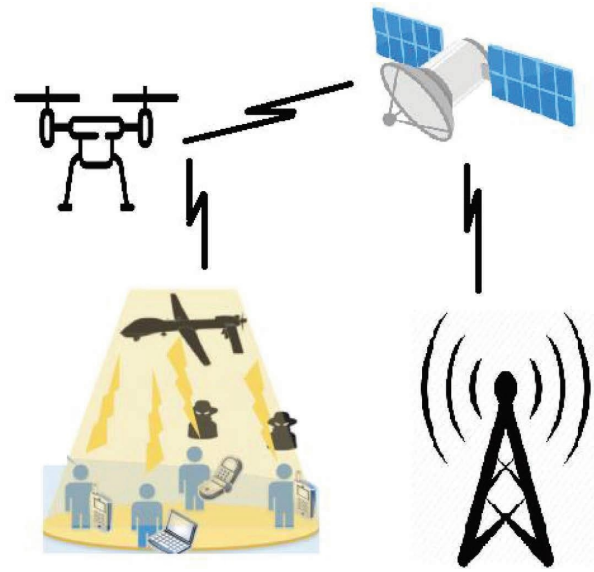


Figure 1: Physical arrangement of UAV network.

2. Related Survey

In the literature section, limitations regarding traditional IDS in other fields are discussed as follows.

Initially, IDS was designed for MANET, VANET, WSN, and IoT networks which use to be vulnerable to cyberthreats such as sinkhole, DoS/DDoS, and PoD. Sometimes, inside the network, attack is initiated which is commonly called sinkhole. While, due to DoS/DDoS security attacks the other neighbor nodes become unavailable for legitimate user. Abdollahi and Fathi implemented a novel IDS for internet of things to identify abnormal data packets. Furthermore, false alarm and missed detection should be reduced which cause issues in network [12].

Real-time IDS can capture abnormal live data packets in contrast with offline. KDD cup 99 data set is commonly utilized in machine learning algorithms to detect damaged caused because of cyberattack [13]. Therefore, real-time IDS are needed for recently emerged technology FANETs.

Identification of attacker through IDS is widely used approach. Therefore, network-IDS usually collect data from network through monitoring traffic. While, different signs of intrusion and alert messages need detection otherwise IoT network level becomes slow down. Deep learning algorithms using KDD cup 99 is simulated through normal, DoS, Probe, R2L, and U2R where high accuracy is examined. FANET is low cost but intrusion can be happen quite easily due to high mobility. Moreover, this study elaborates intelligent intrusion detection framework for UAVs. Authors proposed signature-based IDS for FANETs [14].

Flooding attacks slow down entire process of FANET networks. UAV-IDS-2020 is utilized which use to have unidirectional and bidirectional flow in the data traffic

management [15]. Table 1 presents various IDS in UAV networks. In addition, information in Table 1 is mostly about signature-based intrusion detection system. Various areas of studies are conducted to identify cyberattacks. Also, advance datasets are utilized for experimentation of different machine learning techniques.

3. Machine Learning Classifiers/Algorithms

Machine Learning is a term used in the computer science branch that considerably desires to allow computers to "understand" without being instantly programmed [21, 22]. Computers "understand" in machine learning by enhancing their implementation at assignments through "background." In general, "background" usually implies suiting to information; therefore, there is not an exact border among machine learning and statistical techniques [23]. Machine learning techniques have demonstrated significant assurance in furnishing answers to complicated issues [24]. A few of the applications we employ every day from exploring the Internet to recognizing the speech are the instances of enormous strides created in recognizing the assurance of machine learning [25]. Machine learning have two categories: first is supervised learning and second is unsupervised learning. These two categories will wrap all the combination of classification, and techniques of clustering [26]. Supervised learning strategies enclosed combination of various base classifiers; whereas, unsupervised learning strategies enclosed anticipation maximization algorithms as well clustering techniques. In addition, machine learning techniques are used in different field of studies to improve overall performance.

3.1. Decision Tree. Machine learning is the method of learning or dragging unique designs from extensive data sets by applying techniques from artificial intelligence. Category and forecast are the strategies employed to make out essential data categories and indicate a probable trend [27]. The decision tree is an essential category approach in the machine learning classification. It is typically employed in commerce, management, and detection of fraud [28]. As the typical approach of the decision tree, ID3, C4.5, and C5.0 methods have the values of increased organizing rate, powerful learning capability, and straightforward structure. Yet, these methods are also insufficient in a functional application [29]. When utilizing it to categorize, there exists the issue of bending to select features that have more weight and managing features that have fewer weights. Decision trees are amazing techniques to enable anyone to determine the most suitable method of activity [30]. They develop a favorably beneficial arrangement in which one can set choices and investigate the potential consequences of those choices. A decision tree is employed to describe graphically the findings, the possibilities, and the results related to conclusions and occurrences [31].

3.2. Random Forest. Random forest is a unique approach in the field of machine learning that solves many complex issues [32]. Random forest is a mixture of a sequence of tree network classifiers. This approach has numerous useful features and has been significantly employed in the categorization, forecasting, and regression process [33]. Corresponding with the classic approaches random forest has numerous useful integrities; thus, the extent of the application of this unique approach is extremely comprehensive [34]. It is one of the most suitable learning approaches. Generally, this technique is a regression-tree approach that employs bootstrap collection and randomization of forecasters to acquire an increased extent of predictive accurateness [35]. The principal disadvantage of this unique approach is that an enormous number of trees can make the approach slow and inadequate for real-time forecasts**.** Generally, these approaches are quick to prepare, but a little slow to make forecasts once they are prepared [36].

3.3. Extreme Gradient Boosting. The XGBoost is a brief name for the extreme gradient boosting technique. It is a unique approach that is also known as a tree-based strategy that poses beneath the supervised component of the machine learning domain [37]. Although it can be employed for both categorization as well as regression issues, all of the instructions and illustrations in this technique guide the algorithm's service for categorization only [38]. It is an important and scalable performance of gradient enabling framework. It sustains diverse accurate operations, involving deterioration, categorization, and ranking [39]. In comparison to the regular gradient boosting, XGBoost employs its strategy of creating trees where the score of the similarity and growth choose the most suitable node breaks [40].

3.4. AdaBoost. Boosting algorithm is a famous approach in the machine learning domain to solve the complex problems. AdaBoost is the standard approach in the family of Boosting [41]. This approach has the authority of resisting overfitting. Comprehending the secrets of this sensation is a charming fundamental academic issue. Multiple investigations are dedicated to describing it through statistical theory and margin approach [42]. AdaBoost approach was the preferably suitable boosting algorithm and stayed one of the most widely employed and examined, with applications in multiple domains. Also, this approach can be utilized to facilitate the execution of any algorithm used in machine learning [43]. These are approaches that accomplish precision just beyond random event on a categorization issue. The most appropriate and hence common method employed with AdaBoost are decision trees along with level one [44].

3.5. Bagging Classifier. Bagging is a widely known ensemble building strategy, where an individual classifier in the ensemble is prepared on a separate bootstrap replicate of the training group [45]. The current outcome has demonstrated that bagging can decrease the effect of outliers in training data, particularly if the distant

Table 1: Intrusion detection system for UAV networks.

Reference	Authors	Field of study	Type of IDS	Description
[16]	Bouhamed et al.	UAV network	Signature	Deep reinforcement learning IDS is formulated to detect possible security attacks
[17]	Shrestha et al.	UAV network	Signature	UAV-based IDS is designed using machine learning where decision tree approach given the optimal results in terms of accuracy
[18]	Amouri et al.	Mobile Internet of things (M-IoT)	Signature	Two different mobility models are used which include random way point and Gauss–Markov while designing IDS for mobile IoTs. DDoS and black hole attacks are easily detected with 98% high power velocity
[19]	Khan et al.	Internet of things	Signature	Deep learning-based IDS is implemented for IoT to detect MITM, DDoS, and DoS
[20]	Ghaleb et al.	Vehicular ad hoc networks (VANETs)	Signature	Machine learning algorithms are used to propose IDS for VANETs using NSL-KDD data set

observations are resampled with a more inferior possibility [46]. It is also known as Bootstrap aggregating, which involves having individual models in the ensemble voice with similar significance. To facilitate sample variance, bagging trains every model in the ensemble employing a randomly marked subset of the training group [47]. As an instance, the random forest approach incorporates random decision trees along with bagging to acquire extremely elevated classification precision. Bagging attempts to execute parallel trainees on undersized sample inhabitants and then carries a norm of all the forecasts [48]. Bagging operates by integrating forecasts by voting, every model obtains equivalent significance "Idealized" interpretation: Model several training groups of size n and then create a classifier for each training group and connect the classifiers' forecasts [49].

4. Cognitive Lightweight Logistic Regression Approach

Logistic regression approach is employed to estimate the statistical importance of individual separate variable with reference to possibility [50]. It is a strong form of modelling binomial effect. For instance: if the individual is stirring to suffer from cancer or not by carrying weights 0 as well as 1. Decision trees, as well as logistic regression, are extremely famous approaches in the machine learning domain to solve complex issues [51]. Instead of having so many advantages, decision trees tend to have issues handling linear associations among variables as well as logistic regression has problems with relations effects among variables [52, 53]. Therefore, logistic regression is lightweight and cognitive in nature. Due to lightweight behaviour, LR is easy to deploy on the UAV network. Figure 2 presents the flow chart of cognitive lightweight-LR approach. Equations (1) and (2) present the logic explanation of linear logistic regression [54].

$$Y = \beta 0 + \beta 1X1 + \beta 2X2 + \beta 3X3 + \cdots, \tag{1}$$

$$\text{logit}(p) = \ln\left(\frac{p}{1-p}\right) = \beta 0 + \beta 1X1 + \beta 2X2 + \beta 3X3 + \cdots. \tag{2}$$

Figure 2 is the detailed flow chart regarding logistic regression. Initially, training data are used to formulate and train each function. Cost function is used to be calculated for logistic regression to test overall data. While, testing binary classification is utilized either "0" and "1" means "presence of attack" or "absence of attack" is identified easily.

5. Simulation Results

The simulation environment is designed for IoT-based UAV networks in anaconda python. UNSW-NB 15 dataset is used which consists of various cyberattacks such as DoS/DDoS, backdoors, fuzzers, exploits shellcode, and worms. The mentioned dataset consists of more than two million records. UNSW-NB 15 is a hybrid dataset where advanced data network traffic is incorporated. Three major problems can be easily tackled using UNSW-NB 15 dataset like low footprint, data traffic scenarios, and training/testing methods. However, for light weight algorithms the mentioned dataset are giving better results. Binary classification is utilized while simulating machine learning techniques which include decision tree, random forest, XGBoost, AdaBoost, bagging, and logistic regression [55–64]. Furthermore, the data are divided in training and testing modules which are as follows.

5.1. Data Training. Figure 3 provides detail information about training dataset. During training almost 56.06% data illustrates security attacks, while around 44.94% there is "no attack." Moreover, training dataset is quite balanced due to that false alarm is reduced.

5.2. Data Testing. Figure 4 shows data regarding testing dataset where 31.94% portion is for "no attack" scenario. However, 68.06% data are giving information regarding attacks.

Figure 5 depicts the detail information about training and testing datasets. The metric of high accuracy is maintained in optimal way using UNSW-NB 15 dataset. In high accuracy, there are two scenarios which include attack or no attack. Furthermore, if there will be attack but in reality no attack will be detected which will be false positive. Similarly, true negative will be having no attack where no attack can be identified.

The overall results of machine learning classifiers are presented in Figure 6. Logistic regression performs well in comparison with other algorithms. LR detects security attacks for about 82.54%, while, random forest 71.59%, XG Boost 49.54%, DT 49.17%, Bagging 44.70%, and AdaBoost around 28.39%. Also, Figure 6 provides information about the results of various machine learning classifiers in the area of IoT enabled FANETs. Figure 7 shows the similar results of Figure 6.

5.3. Comparative Discussion of ML-Based IDS. Table 2 elaborates the detailed comparison regarding ML-based intrusion detection system. The approach of network-based intrusion detection system is widely utilized. Also, anomaly-based IDS is quite popular approach to detect cyberattacks. In anomaly-IDS technique, a novel threshold is needed to be designed for identification of security attacks. While, signature-based IDS must have the concept of some possible attacks features stored in database. Although hybrid-IDS is the combination of anomaly and signature but the use is quite less. Therefore, the proposed solution is providing better possibilities to detect cyberattacks. In addition, Table 2 shows the studies which use to have information about different types of intrusion detection system. Also, machine learning-based IDS are widely utilized in the previous study.

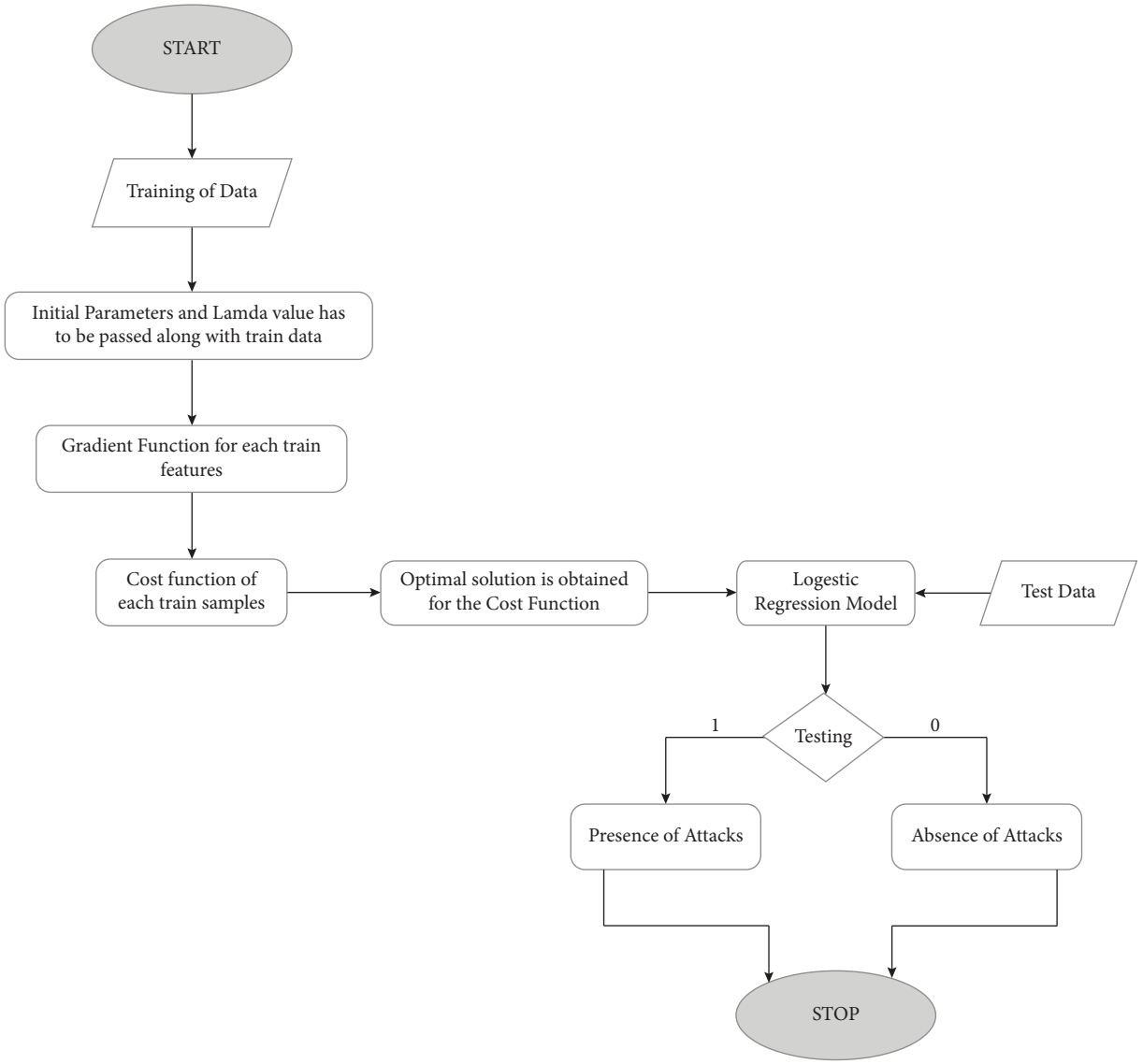


Figure 2: Flowchart of cognitive lightweight-LR technique.

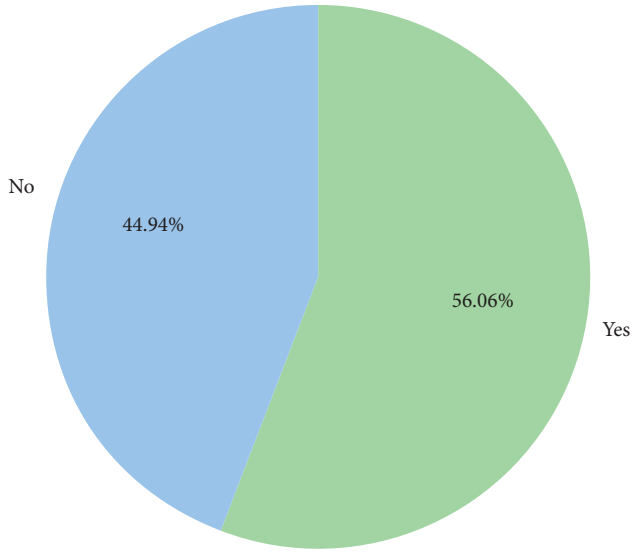


Figure 3: Training data for IoT-based UAV network.

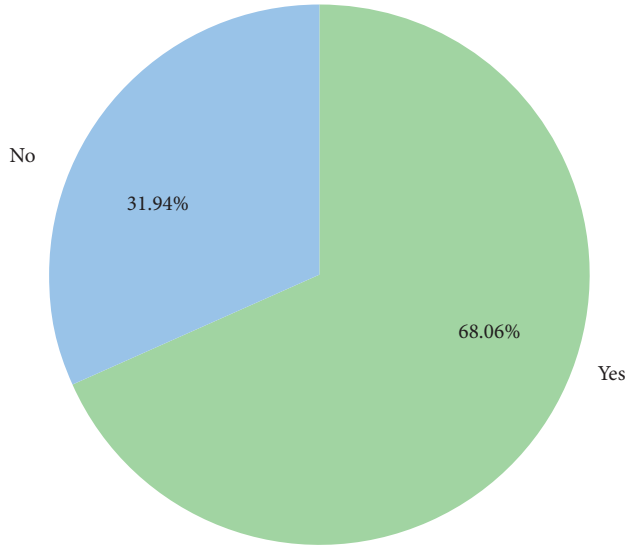


Figure 4: Testing data for IoT-based UAV network.

Figure 5: Comparison of training and testing datasets.

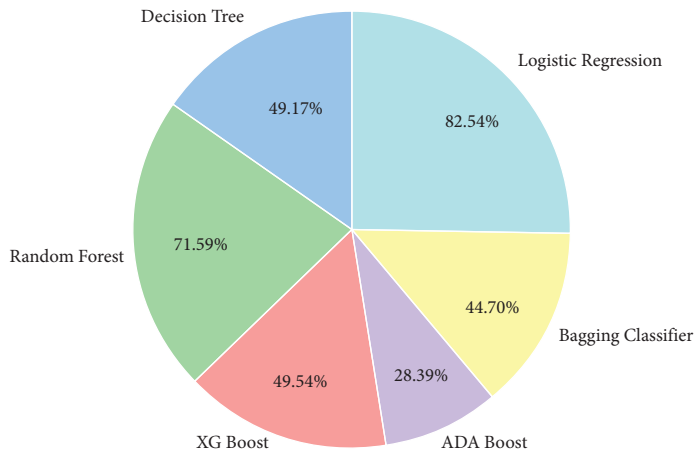


Figure 6: Performance analysis of machine learning classifiers (DT, RF, XGBoost, AdaBoost, Bagging and logistic regression).

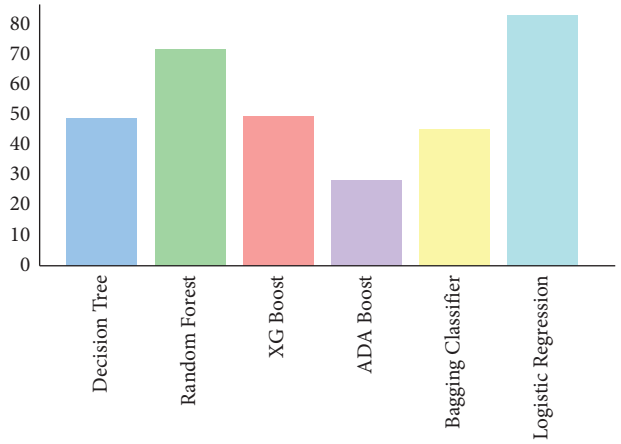


Figure 7: Comparative results of machine learning classifiers.

Table 2: Detailed comparative study of ML-based IDS.

Reference	Network-based IDS	Host-based IDS	Anomaly-based IDS	Signature-based IDS	Hybrid-based IDS	Machine learning-based IDS	Future scope
[65]	✓	X	✓	✓	X	✓	X
[66]	✓	X	✓	✓	X	✓	✓
[67]	✓	X	✓	✓	X	✓	✓
[68]	✓	X	✓	✓	X	✓	✓
[69]	✓	X	✓	✓	X	✓	X
[70]	✓	X	✓	✓	X	✓	✓
[71]	✓	X	✓	✓	X	✓	✓
[72]	✓	X	✓	✓	X	✓	X
[73]	✓	X	✓	✓	X	✓	✓
[74]	**X**	X	**X**	**X**	X	**X**	✓
[75]	✓	X	✓	✓	X	✓	X
[76]	✓	X	✓	✓	✓	✓	✓
Proposed work	✓	X	✓	✓	X	✓	✓

6. Conclusion

Machine learning-based techniques are deployed in IoT-based UAV networks. The main aim of this research study is to propose a novel concept of detecting abnormal behaviour using machine learning. Flying ad hoc networks is the combinations of group of UAVs formulate a network. FANET structure consists of UAVs, satellites, and ground-based stations. While, IoT sensor nodes are deployed on ground and UAVs use to collection information. However, cognitive lightweight-LR approach has reduced false alarm and balanced high accuracy in IoT-based UAV network. UNSW-NB 15 dataset is utilized to check the performance. Nowadays, security is one of the major concerns in almost every field of study. FANET-based IDS is the approach utilized to detect possible cyberattacks. The proposed approach has mimicked the overhead, and false data packets are detected easily. The simulation results shows that logistic regression performed better in comparison with other techniques. The concept of IoT-based UAV networks can be merged with smart cities in near future. In addition, optimization techniques and graph theory will give new directions to this study. Data traffic models and new datasets are the need of futuristic cities.

6.1. Future Direction. In near future, UAV network will be widely utilized for flying taxis in the concept of smart cities. Therefore, artificial intelligence, machine learning, deep learning, reinforcement-based learning, and federated learning can be utilized for intelligent IDS to detect cyberattacks. While in smart cities internet of everything will be used to advance communication. Routing protocols and communication standards need to be further investigated. Also, novel datasets need to be designed which will be helpful for researchers and scientists for further experimentations [77–79].

Data Availability

All the data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks," in *Proceedings of the 35th Annu. Hawaii Int. Conf. Syst. Sci*, pp. 3866–3875, Big Island, HI, USA, January 2002.

[2] I. U. Khan, I. M. Qureshi, M. A. Aziz, T. A. Cheema, and S. B. H. Shah, "Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET)," *IEEE Access*, vol. 8, pp. 56371–56378, 2020.

[3] I. U. Khan, A. Abdollahi, and A. Jamil, "Bisma baig, muhammad adnan aziz, and fazal subhan. "A novel design of FANET routing protocol aided 5G communication using IoT," *Journal of Mobile Multimedia*, vol. 27, pp. 1333–1354, 2022.

[4] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET routing on city roads using real-time vehicular traffic information," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3609–3626, 2009.

[5] I. U. Khan, N. Z. Syeda Zillay, A. Abdollahi et al., "Reinforce based optimization in wireless communication technologies and routing techniques using internet of flying vehicles," in *Proceedings of the 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*, pp. 1–6, St.Petersburg, Russian Federation, May 2020.

[6] J. Sun, F. Khan, J. Li, M. D. Alshehri, A. Ryan, and M. Wedyan, "Mutual authentication scheme for ensuring a secure device-to-server communication in the internet of medical things," *IEEE Internet of Things Journal*, vol. 2021, Article ID 3078702, 11 pages, 2021.

[7] I. U. Khan, A. Ryan, H. J. Alyamani et al., "RSSI-controlled long-range communication in secured IoT-enabled unmanned aerial vehicles," *Mobile Information Systems*, vol. 2021, Article ID 5523553, 11 pages, 2021.

[8] M. Ahmed and A. K. Pathan, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling*, vol. 8, no. 1, p. 4, 2020.

[9] I. U. Khan, A. Abdollahi, A. Ryan et al., "Intelligent detection system enabled attack probability using Markov chain in aerial networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 1542657, 9 pages, 2021.

[10] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, 2019.

[11] H. Tran and C. So, "Enhanced intrusion detection system for an EH IoT architecture using a cooperative UAV relay and friendly UAV jammer," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 11, pp. 1786–1799, 2021.

[12] A. Abdollahi and M. Fathi, "An intrusion detection system on ping of death attacks in IoT networks," *Wireless Personal Communications*, vol. 112, no. 4, pp. 2057–2070, 2020.

[13] A. Pharate, H. Bhat, V. Shilimkar, and N. Mhetre, "Classification of intrusion detection system," *International Journal of Computer Application*, vol. 118, p. 7, 2015.

[14] R. A. Ramadan, A.-H. Emara, M. Al-Sarem, and M. Elhamahmy, "Internet of drones intrusion detection using deep learning," *Electronics*, vol. 10, no. 21, p. 2633, 2021.

[15] Q. Abu Al-Haija and A. Badawi, "High-performance intrusion detection system for networked UAVs via deep learning," *Neural Computing & Applications*, pp. 1–16, 2022.

[16] O. Bouhamed, O. Bouachir, M. Aloqaily, and I. Ridhawi, "Lightweight IDS for UAV networks: a periodic deep reinforcement learning-based approach," in *Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 1032–1037, IEEE, Bordeaux, France, May 2021.

[17] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, "Machine-learning-enabled intrusion detection system for cellular connected UAV networks," *Electronics*, vol. 10, no. 13, p. 1549, 2021.

[18] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "A machine learning based intrusion detection system for mobile Internet of Things," *Sensors*, vol. 20, no. 2, p. 461, 2020.

[19] M. A. Khan, M. A. Khan, S. Ullah Jan et al., "A deep learning-based intrusion detection system for MQTT enabled IoT," *Sensors*, vol. 21, pp. 7016–21, 2021.

[20] A. Ghaleb, F. Saeed, M. Al-Sarem et al., "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET," *Electronics*, vol. 9, no. 9, p. 1411, 2020.

[21] G. Carleo, I. Cirac, K. Cranmer et al., "Machine learning and the physical sciences," *Reviews of Modern Physics*, vol. 91, no. 4, Article ID 045002, 2019.

[22] A. E. Hassanien, A. Darwish, and S. Abdelghafar, "Machine learning in telemetry data mining of space mission: basics, challenging and future directions," *Artificial Intelligence Review*, vol. 53, no. 5, pp. 3201–3230, 2020.

[23] T. Leiner, D. Rueckert, A. Suinesiaputra et al., "Machine learning in cardiovascular magnetic resonance: basic concepts and applications," *Journal of Cardiovascular Magnetic Resonance*, vol. 21, no. 1, pp. 1–14, 2019.

[24] A. Mahmood and J.-L. Wang, "Machine learning for high performance organic solar cells: current scenario and future prospects," *Energy & Environmental Science*, vol. 14, no. 1, pp. 90–105, 2021.

[25] D. Soriano-Valdez, I. Pelaez-Ballestas, A. Manrique de Lara, and A. Gastelum-Strozzi, "The basics of data, big data, and machine learning in clinical practice," *Clinical Rheumatology*, vol. 40, no. 1, pp. 11–23, 2021.

[26] S. Lee, S. H. Lam, T. A. Hernandes Rocha et al., "Machine learning and precision medicine in emergency medicine: the basics," *Cureus*, vol. 13, p. 9, 2021.

[27] B. Charbuty and A. Abdulazeez, "Classification based on decision tree algorithm for machine learning," *Journal of Applied Science and Technology Trends*, vol. 2, no. 01, pp. 20–28, 2021.

[28] M. Pandey and V. K. Sharma, "A decision tree algorithm pertaining to the student performance analysis and prediction," *International Journal of Computer Application*, vol. 61, p. 13, 2013.

[29] B. Chandra and P. Paul Varghese, "Fuzzy SLIQ decision tree algorithm," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 38, no. 5, pp. 1294–1301, 2008.

[30] N. Bhargava, G. Sharma, R. Bhargava, and M. Mathuria, "Decision tree analysis on j48 algorithm for data mining," *Proceedings of international journal of advanced research in computer science and software engineering*, vol. 3, p. 6, 2013.

[31] M. Kumar, M. Hanumanthappa, and T. V. Suresh Kumar, "Intrusion Detection System using decision tree algorithm," in *Proceedings of the 2012 IEEE 14th international conference*

on communication technology, pp. 629–634, IEEE, Chengdu, China, November 2012.

[32] G. Biau and E. Scornet, "A random forest guided tour," *Test*, vol. 25, no. 2, pp. 197–227, 2016.

[33] M. Schonlau and R. Y. Zou, "The random forest algorithm for statistical learning," *STATA Journal*, vol. 20, no. 1, pp. 3–29, 2020.

[34] Y. Liu, Y. Wang, and J. Zhang, "New machine learning algorithm: random forest," in *International Conference on Information Computing and Applications*, pp. 246–252, Springer, Berlin, Germany, 2012.

[35] S. J. Rigatti, "Random forest," *Journal of Insurance Medicine*, vol. 47, no. 1, pp. 31–39, 2017.

[36] L. Zhu, D. Qiu, D. Ergu, Y. Cai, and K. Liu, "A study on predicting loan default based on the random forest algorithm," *Procedia Computer Science*, vol. 162, pp. 503–513, 2019.

[37] R. P. Sheridan, W. M. Wang, A. Liaw, J. Ma, M. Eric, and Gifford, "Extreme gradient boosting as a method for quantitative structure–activity relationships," *Journal of Chemical Information and Modeling*, vol. 56, no. 12, pp. 2353–2360, 2016.

[38] P. Carmona, F. Climent, and A. Momparler, "Predicting failure in the US banking sector: an extreme gradient boosting approach," *International Review of Economics & Finance*, vol. 61, pp. 304–323, 2019.

[39] Y.-C. Chang, K.-H. Chang, and G.-J. Wu, "Application of eXtreme gradient boosting trees in the construction of credit risk assessment models for financial institutions," *Applied Soft Computing*, vol. 73, pp. 914–920, 2018.

[40] R. Song, S. Chen, B. Deng, and L. Li, "eXtreme gradient boosting for identifying individual users across different digital devices," in *International Conference on Web-Age Information Management*, pp. 43–54, Springer, Berlin, Germany, 2016.

[41] T. Chengsheng, H. Liu, and B. Xu, "AdaBoost typical Algorithm and its application research," in *MATEC Web of Conferences*vol. 139, EDP Sciences, Article ID 00222, 2017.

[42] T.-K. An and M.-H. Kim, "A new diverse AdaBoost classifier," in *2010 International conference on artificial intelligence and computational intelligence*, vol. 1, pp. 359–363, IEEE, 2010.

[43] P. Wu and H. Zhao, "Some analysis and research of the AdaBoost algorithm," in *International Conference on Intelligent Computing and Information Science*, pp. 1–5, Springer, Berlin, Heidelberg, 2011.

[44] B. Sun, S. Chen, J. Wang, and H. Chen, "A robust multi-class AdaBoost algorithm for mislabeled noisy data," *Knowledge-Based Systems*, vol. 102, pp. 87–102, 2016.

[45] M. Zareapoor and P. Shamsolmoali, "Application of credit card fraud detection: based on bagging ensemble classifier," *Procedia Computer Science*, vol. 48, no. 2015, pp. 679–685, 2015.

[46] Sandag and A. Green, "A prediction model of company health using bagging classifier," *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, vol. 6, no. 1, pp. 41–46, 2020.

[47] E. Bauer and R. Kohavi, "An empirical comparison of voting classification algorithms: bagging, boosting, and variants," *Machine Learning*, vol. 36, no. 1, pp. 105–139, 1999.

[48] K. Machová, F. Barcak, and P. Bednár, "A bagging method using decision trees in the role of base classifiers," *Acta Polytechnica Hungarica*, vol. 3, no. 2, pp. 121–132, 2006.

[49] S. Kotsiantis and P. Pintelas, "Combining bagging and boosting," *International Journal of Computational Intelligence*, vol. 1, no. 4, pp. 324–333, 2004.

[50] D. Caigny, K. Arno, W. Koen, and D. Bock, "A new hybrid classification algorithm for customer churn prediction based on logistic regression and decision trees," *European Journal of Operational Research*, vol. 269, no. 2, pp. 760–772, 2018.

[51] A. Arabameri, B. Pradhan, K. Rezaei, M. Yamani, H. R. Pourghasemi, and L. Lombardo, "Spatial modelling of gully erosion using evidential belief function, logistic regression, and a new ensemble of evidential belief function–logistic regression algorithm," *Land Degradation & Development*, vol. 29, no. 11, pp. 4035–4049, 2018.

[52] D. Böhning, "Multinomial logistic regression algorithm," *Annals of the Institute of Statistical Mathematics*, vol. 44, no. 1, pp. 197–200, 1992.

[53] K. Chaudhuri and C. Monteleoni, "Privacy-preserving logistic regression," *Advances in Neural Information Processing Systems*, vol. 21, 2008.

[54] N. Srimaneekarn, H. Anthony, W. Liu, and C. Tantipoj, "Binary response analysis using logistic regression in dentistry," *International Journal of Dentistry*, vol. 2022, Article ID 5358602, 8 pages, 2022.

[55] N. Moustafa, G. Creech, and J. Slay, "Big data analytics for intrusion detection system: statistical decision-making using finite dirichlet mixture models," in *Data Analytics and Decision Support for Cybersecurity*, pp. 127–156, Springer, Cham, 2017.

[56] N. Moustafa, J. Slay, and G. Creech, "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks," *IEEE Transactions on Big Data*, vol. 5, no. 4, pp. 481–494, 2019.

[57] N. Moustafa and S. Jill, "The evaluation of Network Anomaly Detection Systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Information Security Journal: A Global Perspective*, vol. 25, no. 1-3, pp. 18–31, 2016.

[58] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, Canberra, ACT, Australia, November 2015.

[59] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "Netflow datasets for machine learning-based network intrusion detection systems," 2020, https://arxiv.org/abs/2011.09144.

[60] N. Moustafa, B. Turnbull, and K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4815–4830, 2019.

[61] N. Moustafa, G. Misra, and J. Slay, "Generalized outlier Gaussian mixture technique based on automated association features for simulating and detecting web application attacks," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 245–256, 2021.

[62] M. Keshk, N. Moustafa, E. Sitnikova, and G. Creech, "Privacy preservation intrusion detection technique for SCADA systems," in *Proceedings of the 2017 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, Canberra, ACT, Australia, November 2017.

[63] N. Moustafa, G. Creech, and J. Slay, "Anomaly detection system using beta mixture models and outlier detection," in *Progress in Computing, Analytics and Networking*, pp. 125–135, Springer, Singapore, 2018.

[64] N. Moustafa and J. Slay, "A network forensic scheme using correntropy-variation for attack detection," in *IFIP*

International Conference on Digital Forensics, pp. 225–239, Springer, Cham, 2018.

[65] A. Ugendhar, S. Babu Illuri, R. Vulapula et al., "A novel intelligent-based intrusion detection system approach using deep multilayer classification," *Mathematical Problems in Engineering*, vol. 2022, Article ID 8030510, 10 pages, 2022.

[66] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things," *Sensors*, vol. 19, no. 9, p. 1977, 2019.

[67] A. Dahou, M. A. Elaziz, S. A. Chelloug et al., "Intrusion detection system for IoT based on deep learning and modified reptile search algorithm," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 6473507, 15 pages, 2022.

[68] J. Ren, J. Guo, Q. Wang, Y. Huang, X. Hao, and J. Hu, "Building an effective intrusion detection system by using hybrid data optimization based on machine learning algorithms," *Security and Communication Networks*, vol. 2019, Article ID 7130868, 11 pages, 2019.

[69] S. Einy, C. Oz, and D. N. Yahya, "The anomaly-and signature-based IDS for network security using hybrid inference systems," *Mathematical Problems in Engineering*, vol. 2021, Article ID 6639714, 10 pages, 2021.

[70] K. Albulayhi, Q. Abu Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman, and F. T. Sheldon, "IoT intrusion detection using machine learning with a novel high performing feature selection method," *Applied Sciences*, vol. 12, no. 10, p. 5015, 2022.

[71] A. O. Alzahrani and J. F. A. Mohammed, "Designing a network intrusion detection system based on machine learning for software defined networks," *Future Internet*, vol. 13, no. 5, p. 111, 2021.

[72] P. Verma, D. Ankur, R. Singh et al., "A novel intrusion detection approach using machine learning ensemble for IoT environments," *Applied Sciences*, vol. 11, no. 21, Article ID 10268, 2021.

[73] H. Zainel and C. Koçak, "LAN intrusion detection using convolutional neural networks," *Applied Sciences*, vol. 12, no. 13, p. 6645, 2022.

[74] M. Althunayyan, N. Saxena, S. Li, and P. Gope, "Evaluation of black-box web application security scanners in detecting injection vulnerabilities," *Electronics*, vol. 11, no. 13, p. 2049, 2022.

[75] S. Ullah, J. Ahmad, M. A. Khan et al., "A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering," *Sensors*, vol. 22, no. 10, p. 3607, 2022.

[76] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine," *Electronics*, vol. 9, no. 1, p. 173, 2020.

[77] O. Friha, M. Amine Ferrag, L. Shu, L. Maglaras, K.-K. R. Choo, and M. Nafaa, "FELIDS: federated learning-based intrusion detection system for agricultural Internet of Things," *Journal of Parallel and Distributed Computing*, vol. 165, pp. 17–31, 2022.

[78] A. Duraisamy and M. Subramaniam, "Attack detection on IoT based smart cities using IDS based MANFIS classifier and secure data transmission using IRSA encryption," *Wireless Personal Communications*, vol. 119, no. 2, pp. 1913–1934, 2021.

[79] Loo, E. Chong, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, 2006.

Hindawi
Mobile Information Systems
Volume 2023, Article ID 3265310, 14 pages
https://doi.org/10.1155/2023/3265310

Review Article

A Hybrid Framework of Blockchain and IoT Technology in the Pharmaceutical Industry: A Comprehensive Study

Abidemi A. Emmanuel,[1] **Jinmisayo A. Awokola**,[1] **Shadab Alam**,[2] **Salil Bharany**,[3] **Praise Agboola**,[1] **Mohammed Shuaib**,[2,4] **and Rafeeq Ahmed**[5]

[1]*Department of Computer Sciences, Precious Cornerstone University, Ibadan 200251, Nigeria*
[2]*College of Computer Science and IT, Jazan University, Jazan, Saudi Arabia*
[3]*Department of Computer Engineering and Technology, Guru Nanak Dev University, Amritsar, Punjab, India*
[4]*Razak Faculty of Technology and Informatics (RFTI), Universiti Teknologi Malaysia (UTM), Kuala Lumpur 54100, Malaysia*
[5]*Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India*

Correspondence should be addressed to Salil Bharany; salilbharany@gmail.com and Mohammed Shuaib; shuaib@graduate.utm.my

Received 21 September 2022; Revised 15 October 2022; Accepted 6 April 2023; Published 20 April 2023

Academic Editor: Junaid Shuja

The pharmaceutical company is key to having a strong healthcare system, and excellent healthcare is essential for every society and economy. However, there are significant concerns with medication safety and security as a result of fake and inferior medical items, which constitute a significant hazard and harm to consumers' health. Globally, drug counterfeiting is a severe problem that endangers the public's health as well as the health of consumers. The global business of manufacturing fake medications generates enormous annual revenue. To have a quality healthcare system, the pharmaceutical industry is of great importance and plays a vital role in medicine and pharmaceutical supplies. With emerging computer technologies like blockchain and IoT cutting across several industries and sectors and revolutionizing the world, a systematic literature review of various articles chosen from different databases was carried out in this study to analyze and evaluate application areas of this technology in the pharmaceutical industry and existing frameworks that have been proposed to solve problems faced in the pharmaceutical industry. The outcome of this review showed that the application of the blockchain and IoT hybrid framework can assist in reducing the drug counterfeit problem and provide solutions to most of the problems faced in the pharmaceutical industry. This study also proposed a framework that addressed the drawbacks of existing frameworks in the pharmaceutical industry.

1. Introduction

Healthcare systems worldwide continue to face challenges, which frequently result in rising costs or poorer health outcomes (morbidity and mortality) [1]. This happens for various reasons, one of which is the pharmaceutical supplies or medicines provided by the pharmaceutical industry. One of the foundational components of the healthcare system is medicine supplies [2]. Because of the huge risk that counterfeit and substandard medications represent to clients' well-being in today's health-conscious culture, drug quality and regulatory compliance have received great international attention [3]. The popularity of prescription pharmaceuticals and their widespread use, according to an article in the American Journal of Law and Medicine, "have attracted unsavory individuals interested in abusing vulnerable patients and the markets for medicines" [4]. Pharmaceutical companies invest a lot of money in the research and development (R&D) of new medications that benefit society and are recognized as safe and effective in the United States by the Federal Drug Administration (FDA), but suppliers of fake medications avoid this step and provide these medications at little cost to them; profit margins are frequently as high as 3000 per cent [5].

According to an analyst, investing $1000 in fake prescription pharmaceuticals can yield a $30,000 earning, which is ten times the profitability of heroin trafficking [6]. According to one source, selling fake sildenafil, for instance, "may be as much as 2000 times more profitable" than selling cocaine. Additionally, because detection is far more challenging, the likelihood of being discovered is substantially smaller [7]. Medical professionals relate the issue of medications that yield subpar clinical effects to patient variance, making detection challenging. Patients typically have little reason to believe they are taking fake medications. It is challenging to test for bad pharmaceuticals because the packaging is frequently thrown away, especially since the poisons may become undetected in the bloodstream within a few days. The evidence is obliterated the moment it is consumed or injected, as suggested by one case [4]. Additionally, individuals might not want to admit that they obtained medications over the internet without a prescription. As a result, there is a very low chance that a counterfeiter will be discovered [8].

Less than 1% of medicines sold in affluent nations are thought to be fake, the World Health Organization (WHO) claims. However, this percentage is only about 10% worldwide; in some developing nations, this percentage may reach up to 30%. Approximately 10–30% of the pharmaceuticals supplied in developing countries are fraudulent, which is a significant problem for the pharmaceutical industry today. Medication fraud is a global issue as well. According to estimates from the World Health Organization (WHO), up to 30% of the medicines sold in some regions of Latin America, Africa, and Asia are fake [9]. In Nigeria, 64% of antimalarial medications were discovered to be fake in 2011. An estimated 10% of medicines sold worldwide are fake [10]. The market for fake medicines is estimated to be worth $200 billion yearly, but internet sales of counterfeit medicines account for $75 billion of that figure. The main problem with these fake medications is not that they are not the real thing but that they can behave extremely different from what was previously anticipated. Because these fake medications cannot address the ailment they were intended to, they can be dangerous for individuals who take them [11]. The effectiveness of supply chain management is significantly impacted by pharmaceutical businesses' performance as key actors in the pharmaceutical supply chain. Numerous supply chain dangers are internal risks brought on by improper management of a firm's processes, people, and functions. These risks could be easily controlled by effective mitigation techniques [12]. Numerous sectors today need to overcome financial obstacles to operate efficiently and make money as a result of the current economic situation. This is particularly true in the pharmaceutical industry, where technology is continuously being created to discover new ways to treat illnesses, store medications, and work as effectively as possible [13].

Blockchain-based applications have shown promise in the development of the healthcare industry, and they have continued to prove a reliable platform for information exchange and review. Regardless, healthcare systems must be cautiously optimistic about the potential of blockchain technology and do the careful commercial and technical due diligence motivated by specific use cases [14]. The blockchain network uses cryptography to ensure that only authorized users may access all of the data. Because the blockchain is a decentralized platform with no centralized entity controlling or storing the network's occurrences, a sender who wants to make a transaction needs a blockchain P2P network [15]. Blockchain technology has essential features: immutability, distributed, decentralized, security, consensus, and unanimous. The applications of blockchain technology cut across several industries and sectors; in the pharmaceuticals firm's tamper-proof and immutability, the blockchain enables distribution network transparency and traceability process and ensures drug provenance. Also, pharmaceutical records and other prior data are kept secure and cannot be breached.

The demand for Internet of Things (IoT) devices has been progressively growing in recent years as a consequence of the expanding demand on the world market for quicker and more efficient manufacturing processes, the necessity of improving military capabilities, and the conversion of everyday objects into intelligent ones like intelligent houses, enterprises, and cities. Internet of Things gadgets have many advantages, but they also have many drawbacks. For example, they produce a large amount of data and a large amount of energy and raise trust concerns because they are centralized and under the authority of a single administrator who may alter the fundamental infrastructure or even shut it down totally. The Internet of Things (IoT) technology enables objects to gather and later share data about themselves and their surroundings. These data are sent to a central server after being captured with a device [16, 17]. This is where the integration and incorporation of blockchain technology come in IoT devices.

The blockchain architecture is, by default, decentralized. It enables IoT devices to safely and dependably exchange acquired data among themselves and transfer it to a decentralized cloud server [18]. Data privacy, security, and integrity are one of the biggest problems faced with IoT devices and can be solved using blockchain technology [19]. Figure 1 shows the pictorial representation of the world of IoT and its domains.

The pharmaceutical industry plays a critical role in having a solid healthcare system; good healthcare is vital to every country and economy. Regardless of this fact, there are main issues with drug safety and security because of falsified and substandard medical products, which pose a great threat and harm to consumers' health [20]. The pharmaceutical supply chain (PSC) involves numerous partners and intermediaries from manufacturing to consumption, which cannot ascertain transparency in today's centralized systems. Some of the global challenges faced by the pharmaceutical industry are counterfeiting drugs, data manipulation, and poor monitoring of the supply chain. Other challenges related to the management approach include lack of standardization and regulatory compliance, nonavailability of a feedback system, and loss of confidence in the medications and healthcare providers. Therefore, this review examines the overview of the existing literature on blockchain and IoT

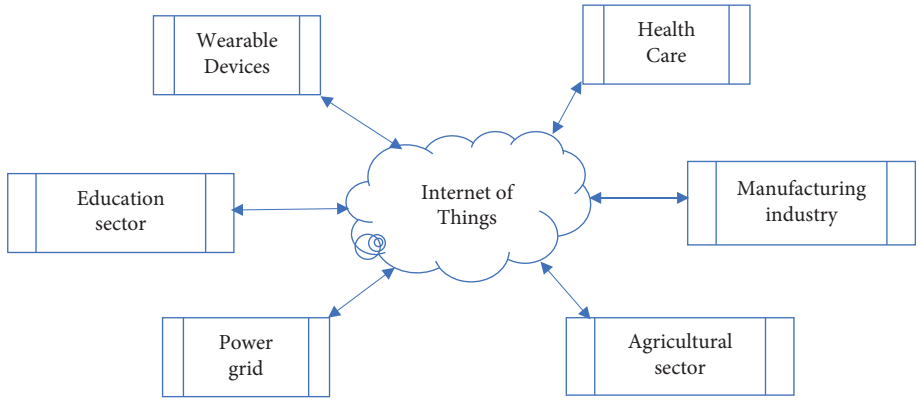


Figure 1: Internet of things technology.

in the pharmaceutical industry and proposes a novel framework with patient feedback to mitigate the problem in the existing framework as well as spur researchers to develop a more robust system for the pharmaceutical industry.

This study consists of five sections. The next section describes the literature reviews. The study reviews blockchain and IoT articles and provides a summary table for the literature showing their drawback. The methodology was described in Section 3. This section described the techniques and various databases visited and obtained articles for the systematic review. Section 4 presents the proposed framework for blockchain and IoT technologies in the pharmaceutical industry, while Section 5 concludes the study and gives a future research direction.

2. Related Reviews

This section entails a review of related works in the application of blockchain and IoT technology in the pharmaceutical industry.

Haq and Muselemu in the study [21] proposed the use of blockchain technology in the pharmaceutical business to combat counterfeit pharmaceuticals. The proposed model used blockchain technology as an immutable ledger and a unique identity of a hashed pharmaceutical product registered on the blockchain and labelled as a QR code to track the end user's supply chain history and provenance of pharmaceutical products. The study tends to prevent counterfeit drugs in the pharmaceutical industry but lacks the required client feedback to combat fake drug distribution. This study discussed how blockchain technology could be used to improve clinical research quality [22]. A similar model to Haq and Muselemu was proposed by Sahoo et al. [23]. The model uses blockchain technology but introduces the use of IoT to track the supply chain process from the manufacturer of a particular product to the consumer/end user. In their work, every manufacturer must be certified/licensed by a standard regulatory body and possess a unique ID to be labelled on the drug. The authors discussed healthcare and blockchain in a broad general sense [24]. However, the authors did not provide any details on blockchain in the drug production or pharmaceutical supply chain [25, 26].

Rayan and Zubair [27] proposed a medicine supply network centred on radio frequency identification (RFID) that supervises the system to safeguard the chain's security and the provision of high-quality health care. It offered a technological solution integrating blockchain, RFID, and IoT to improve the monitoring of pharmaceutical products as they travel through the pharmaceutical supply chain. The study lacks the feedback mechanism to validate the authenticity of the supply chain [28]. TrustChain is a three-layered structure for reputation administration proposed by Malik et al. [29] TrustChain was depicted as a blockchain-based supply chain application that is used to navigate trust challenges related to commodity quality.

Pandey and Dhanalakshmi [30] suggested a pharmaceutical distribution chain counterfeiting remedy. The study did an overview of different solutions and models that exist and proposed a model involving the use of smart contracts and how distributed ledger technology might assist participants in preventing counterfeit pharmaceuticals from entering the supplier base. A feasible blockchain-based anti-counterfeit pharmaceutical management system is proposed to reduce drug cloning and improve medicinal integrity. The proposed system is built on the Ethereum blockchain and the IPFS protocols to enable tamper-proof tracking [31].

Plotnikov and Kuznetsova [32] proposed using an IoT solution to provide real-time location tracking with a wireless sensor placed within the medicine packaging and blockchain as an immutable ledger for data storage. Another study offered a counterfeit prevention system that tracked medications from the manufacturer to the end user [33]. In the proposed model, manufacturers of the medication control and record all blockchain transactions. A comparison of the details of data previously stored on the blockchain with what is submitted reveals any attempted fraud, with inconsistencies revealing fake medications [34].

Subramanian et al. [35] designed and implemented a crypto pharmacy mobile application using hybrid blockchain technology to eliminate third-party presence (buy/sell) in a medicine purchase. Nem blockchain was integrated with the mobile application. Another study talked about Industry 4.0 and emerging technologies transforming the industry across every sector. The serialization process of tracking and tracing was analyzed, and it showed that it was still

susceptible to central failure, amongst several others. A better solution, NFT, was proposed that replaces all of the components of the serialization process and takes the form of distributed ledger technology through the use of blockchain [36]. A study by Gogos and Rochelle [37] evaluates the potential and drawbacks of blockchain in the pharmaceutical industry. The authors gave an overview of blockchain technology, smart contracts, and other major components of a blockchain [38].

Shashi [39] highlighted one of the most important but challenging aspects of the pharmaceutical industry temperature monitoring. Pharmaceutical items, such as medications, pharmaceuticals, vaccines, and specialty therapies, function normally when stored at a set temperature. Some of the exact and managed storage limits for different kinds of pharmaceutical items include below +25°C (controlled temperature), +2°C to +8°C (temperature-sensitive products), −20°C to −40°C (negative temperature), and −70°C (ultra-low temperature) [40]. The report also mentions that pharmaceutical goods that are not properly manufactured or delivered at the proper temperature might create difficulties when ingested. The author conducted research to identify the IoT-based digital enablers used by pharmaceutical supply chain managers to optimize the cold chain process. A model was proposed by Jammula et al. [41] using blockchain and IoT sensors to combat the problem of temperature monitoring as one of the biggest challenges faced by the pharmaceutical industry other than drug counterfeiting.

Kumari [42] identifies that fake medicines and drug counterfeiting seriously threaten the healthcare sector and society. Therefore, a blockchain-based architecture is presented to combat the danger of counterfeit drugs. The author states that the way to combat counterfeit drugs in health services and maintain and distribute health records is another major challenge. Because health records are vulnerable to confidentiality and integrity challenges, their security is a top priority. Neglecting these dangers might have serious repercussions for healthcare systems, such as patient mortality. Furthermore, Jain et al. [43] characterized the creation and distribution of counterfeit medications, particularly in poorer nations, as a critical and growing worldwide concern. Therefore, a blockchain-based solution is provided to overcome medicine counterfeiting.

Jaisimha and Kumar [44] carried out a systematic mapping study to explore blockchain's feasibility in the pharmaceutical sector's supply chain. The authors proposed the use of smart contract interaction with IoT devices to optimize the pharma supply chain. IoT is used for monitoring and regulation of critical things like temperature, weather, etc. Smart contract helps set the condition of easy transfer and purchase of the product when all the conditions are fulfilled; if not fulfilled, they do not go through. Humayun et al. [45] identified coordination flaws in the drug distribution market (DDM), coordination management, and lack of a centralized surveillance system capable of providing effective market management and providing real-time pricing, accessibility, and authentication data, as serious issues that significantly affect the global market for counterfeit drugs.

Gao et al. [46] conducted an in-depth examination of the drug companies to appreciate the advantages and disadvantages of blockchain for the industry, as well as customer impressions of blockchain application in the industry The study studies the relevant circumstances in the present healthcare industry, the understanding of blockchain technology, and evaluates the current state and issues of blockchain applications in the healthcare market as the target of research. Data security, privacy, preservation, data exchange, and interoperability are all important considerations identified as major issues and challenges faced by the pharmaceutical industry. Blockchain is a solution to break the bottleneck problems in the pharmaceutical sector [47]. Alagarsamy et al. [48] gave an overview of the application of IoT in the pharmaceutical sector. They identified the applications of IoT in facilitating and optimizing drug development, drug testing, and remote patient surveillance among other things. Table 1 summarizes the literature review.

The major drawback deduced from the list of the literature is the lack of a feedback mechanism system between the consumer and manufacturer to validate the product. This drawback causes a high rate of counterfeit drugs in the pharmaceutical supply chain. Another drawback examined from the existing work is the lack of data integrity. Therefore, developing appropriate and efficient quality systems is one of the crucial factors to consider for survival in the highly competitive pharmaceutical manufacturing industries. Creating a tailored feedback system for manufacturers and hospitals that is more grounded in real-world experiences is more dependable and sustainable than using standardized surveys [58].

3. Materials and Methods

For research, the study used a comprehensive analysis of qualitative information. There is significant research on IoT and blockchain in the pharmaceutical sector, but it is usually focused on a certain practice. Even though numerous articles have been published addressing the application of IoT and blockchain in the pharmaceutical business, there are still gaps in the literature in this field, which supports the current study. In this study, data from a few articles published in the recent five years (2017 to 2022) were carefully analyzed to emphasize what has been documented about the issue in both scholarly research and literature reviews.

The Methodi Ordinatio Methodology was used in this study, which describes the criteria for selecting scientific publications [48]. This approach selects articles using a modified version of the Prochnow-C, and works are rated by significance using an index called InOrdinatio.

3.1. Research Questions

(i) What are blockchain and IoT technology application areas in the pharmaceutical industry?

(ii) What are the drawbacks of the existing frameworks in the pharmaceutical industry?

Table 1: Summary of the literature review.

s/n	Authors and title	Work done	Strength	Drawback
1	Haq and Muselemu [21]	Proposed a model for counterfeit medications using a mobile app to check for verification and a permission blockchain	Traceability and transparency are achieved	IoT was not incorporated into this model. Other things, like the temperature of the medical product during transportation, were not achieved
2	Benchoufi et al. and colleagues [25]	Proposed a model for protecting patient data, improving clinical research, and ensuring consent for clinical trials	Traceability and transparency are provided for clinical data	They discussed the use case of blockchain in general for healthcare, but no further explanation was given for blockchain and IoT in the pharmaceutical industry
3	Rayan and Zubair [27]	An IoT-integrated blockchain model for supply chain traceability and transparency	Transparency and real-time monitoring using blockchain and IoT technology	No in-depth explanation of the proposed model by the authors No direct feedback mechanism between consumers and the manufacturer
4	Alam et al. [49]	A blockchain-based model to eliminate drug counterfeiting in the pharmaceutical industry	Transparency and traceability of the chain	(i) No explanation was given on how the consumer checks the validity of the product (ii) IoT was not integrated into the model that was proposed (iii) Nonavailability of a feedback system between the consumer and the manufacturer
5	Malik et al. [29]	The three-layered framework known as TrustChain uses consortium blockchain to solve trust issues with commodities and the integrity of data	Smart contract used for automation of reputation calculation	No direct feedback mechanism between the manufacturer and the consumer
6	Raj et al. [50]	Use of smart contracts and the blockchain to establish proof ownership of a product and the authenticity using the electronic product code	Automation of smart contracts in the supply chain process	No incorporation of IoT technology
			Transparency and supply chain history validity	No feedback mechanism between the manufacturer and the consumer
7	Pandey and Dhanalakshmi [30]	Smart contracts and blockchain provide solutions for drug counterfeiting	Pharmaceutical supply chain data were stored using an immutable ledger	Data integrity was not achieved. The systems depend on stakeholders storing data No incorporation with IoT No feedback mechanism between the manufacturer and the consumer
8	Pham et al. [31]	The anti-counterfeit medicine management system based on IPFS and ethereum network	Transparency in the proposed system using the blockchain	(i) No feedback mechanism between manufacturers and consumers
9	Makarov [34]	Evaluation of the use of smart contracts in pharmaceuticals	Application of blockchain	IoT as a solution to the problems of pharmaceuticals was not proposed No feedback mechanism was suggested between manufacturers and consumers
10	Plotnikov and Kuznetsova [32]	General overview of the importance of digital technologies to fostering economy and blockchain as a major contributor to today's economy	Insights into the applications and positive effects of blockchain's implementation	No framework was proposed to solve the issue of falsified and substandard medications
11	Zakari et al. [51]	A systematic literature review on the applications of blockchain in the pharmaceutical industry, challenges, and future directions	Challenges and future directions in the adaptation and adoption of blockchain were covered by the author	No framework was proposed to solve the pharmaceutical supply chain problem

Table 1: Continued.

s/n	Authors and title	Work done	Strength	Drawback
12	Subramanian et al. [35]	A model to eliminate drug counterfeiting through the use of smart contracts and blockchain	Transparency and traceability	(i) No incorporation with IoT (ii) No direct feedback mechanism between the manufacturer and the consumer
13	Jangir et al. [52]	Web 3 application built for pharmaceutical stakeholders that allow users to track products by querying the product ID	Traceability and transparency	No integration with IoT No feedback mechanism between manufacturers and consumers
14	Chiacchio et al. [36]	Utilization of nonfungible tokens as a solution to drug counterfeiting, tracking, and tracing	Digital uniqueness of NFTS	No feedback mechanism for manufacturers and consumers
15	Gogos and Rochelle [37]	Research work on blockchain potentials in the pharmaceutical industry	The result showed that blockchain can be used for traceability and privacy, amongst several other benefits	No model was proposed for solving the pharmaceutical supply chain problem
16	Shashi [39]	Study and analysis of the cold chain system in the pharma supply chain	Use of IoT technology as an enabler	Blockchain technology was not used
17	Jammula et al. [41]	Designed a model for temperature monitoring in the pharmaceutical supply chain	The use of IoT and blockchain	The authentication of the product stops at the end user, and no feedback mechanism between the manufacturer and the consumer
18	Kumari [42]	The proposed model to curb the wide spread of counterfeit medication in the healthcare sector	The blockchain-based model ensures transparency	No explicit knowledge of the methodology was proposed
19	Jain et al. [43]	Proposed a blockchain-based solution for medicine counterfeiting	Transparency and traceability because of the blockchain	No IoT-integrated framework No feedback mechanism between the manufacturer and the consumer
20	Sharma and Sikka [53]	A survey on the practical approaches to prevent drug counterfeiting using blockchain technology	Practical blockchain-based solution	No integration with IoT
21	Khubrani and Alam [54]	The supply chain management system using the IPFS and the ethereum network	Transparency and Scalability in the supply management system	An IoT framework was not integrated
22	Jaisimha and Kumar [44]	A systematic mapping study on the feasibility of blockchain in the pharma supply chain	IoT and smart contract integration for automated control of the system	No feedback mechanism in the supply chain model for the customer and the manufacturer
23	Humayun et al. [45]	A model for securing drug distribution from tampering using blockchain	Data coordination and data management using blockchain	No IoT framework was introduced
24	Gao et al. [46]	The study analyzes the future development of blockchain technology in the pharmaceutical industry and its general reception by consumers of healthcare facilities	Blockchain was found in this analysis and research as a solution to major challenges faced by the medical industry	No model was proposed on how to solve the problems faced by the medical industry The study did not cover the use of IoT
25	Alagarsamy et al. [48]	IoT applications in the pharmaceutical industry	The authors identified three main applications of IoT: IoT in pharmaceutical manufacturing, IoT in drug discovery, and IoT in clinical trials	No model was proposed on how to apply IoT in the pharma industry
26	Tehrani and Jin [55]		Wearable technology and personalized patient care through the use of IoT	The study only focused on the applications of IoT in the pharmaceutical industry, and there was no integration with blockchain technology No model was proposed to address the challenges faced in the pharmaceutical industry

Table 1: Continued.

s/n	Authors and title	Work done	Strength	Drawback
27	Bharny et al. [56]	The anti-counterfeit model to reduce and curb the widespread drug counterfeiting and false medications	Automation of the supply chain process using IoT, transparency of supply chain history with blockchain technology, and credibility of transactions using the smart contract	No feedback mechanism between the manufacturer and the final consumer
28	Jochumsen and Chaudhuri [57]	Analysis was carried out to learn in-depth information about blockchain's potential in the pharmaceutical industry as well as its potential for supply chains and procurement	Tracking, tracing, and securing IoT were identified as ways blockchain could impact the pharmaceutical supply industry	No model was proposed to implement blockchain technology in the pharmaceutical industry
29	Lingayat et al. [58]	A blockchain model was designed to enable the security of the pharmaceutical supply chain	Transparency and immutability of the blockchain allow all records to be visible and unchanged	No feedback mechanism between the manufacturer and the consumer
30	Fekih and Lahami [59]	General overview of the knowledge of blockchain technology and its different applications in the healthcare sector	Blockchain and IoT technology applications were covered in the healthcare sector	No framework was proposed for the implementation of IoT and blockchain in the pharmaceutical industry

(iii) What model can be used to address the drawbacks of the existing frameworks in the pharmaceutical industry?

The methodology of this system is based on a web3 application called a decentralized autonomous organization (DAO) which uses an incentive model to reward customers when they give feedback.

The incentive model is based on the use of a cryptocurrency token that powers the ecosystem of the DAO. This token has attached utility that gives it value such as governance and purchasing power of pharmaceutical products.

3.2. Analysis of Journal Reviewed. When the search procedure was used on the selected scientific database, 10800 articles were originally obtained. Six (0.03%) were from ScienceDirect, 721 (3.91%) from Pubmed, 120 (0.65) from Research Gate, and 9,953 (62.36%) from Google Scholar. After the preliminary title-based filtering, 9720 articles remained accessible. Each article title is examined independently using the inclusion and exclusion criteria, remaining 1270 papers. 773 publications were deleted because they had no relevance to the research topic (some were omitted because they were centered on features of IoT and blockchain that were unrelated to the pharmaceutical sector). 378 of them were chosen for further review based on their abstracts, introductions, and conclusions. 89 identical articles were removed using Endnote X8. Some articles were removed because their full contents were challenging to comprehend or their abstracts demonstrated that they had no relevance to the inquiry. Thirty publications having a Methodi Inordinatio index of more than 100 were selected for full document assessment; each was studied in its completeness, autonomously, and again using the inclusion and exclusion criteria. Table 1 contains a list of the thirty papers that were chosen as well as the data items that were retrieved.

3.3. Public Distribution of Journals. All of the publications selected were published between 2017 and 2022, highlighting the significance of IoT and blockchain in the pharmaceutical sector. It is stressed that the majority of the thirty articles picked ($n = 9$, 30%) were published in 2022, ($n = 5$, 16.67%) were published in 2021, ($n = 2$, 6.67%) were published in 2020, ($n = 8$, 26.67%) were published in 2019, and ($n = 5$, 16.67%) were published in 2018 while ($n = 1$, 3.33%) were published in 2017. Table 2 shows the collection of articles by year. Figure 2 displays the public distribution of the journals.

3.4. Geographical Distribution of Journals. Geographically, the articles were split into regions based on the primary author's address, with Asia (66.67%), Europe (16.67%), North America (13.33%), and Africa (3.33%) taking the lead. The following pie chart depicts the distribution. This breakdown demonstrated that IoT and blockchain in the pharmaceutical business and healthcare are not confined to a single region of the world but have extended around the globe, with the lowest activity coming from developing nations in Africa. Figure 3 displays the geographical distribution of the articles' sources.

Table 2: Analysis of articles by year of publication.

Years	Articles ($n = 30$)	Percentage (%)
2017	1	3.33
2018	5	16.67
2019	8	26.67
2020	2	6.67
2021	5	16.67
2022	9	30

3.5. Distribution of Articles Based on Research Questions. The publications were divided into three types based on the study's research objectives. Some of the chosen articles uniquely responded to the issues by addressing one specific aspect of blockchain and IoT in the pharmaceutical industry, while other articles mostly re-emphasized what was written in other articles. 14 of the chosen articles described the application areas of blockchain and IoT in the pharmaceutical Industry, while the remaining 16 articles either provided a framework that can be implemented or a solution to the existing problems faced by the pharmaceutical industry. Research in the existing models found that there was a lack of feedback mechanisms between manufacturers of pharmaceutical products and the final consumer. Through blockchain and IoT technology, customers can check the supply chain history of the pharmaceutical products and the temperature range at which they were transported and verify the authenticity and validity of the product based on specific requirements. Regardless of this fact, the supply chain process ends when the final consumer gets the products with no way for the manufacturers to understand critical things like business intelligence, what types of medications are to be produced based on effectiveness, general acceptability in the global market, side effects of the medications produced as they pertain to geography and demography, drug compliance with different geographies, amongst several other reasons. It also helps in increasing the reputation of the pharmaceutical company and fosters future developments as a way to deal with counterfeit medications.

To answer research question 3, a model was proposed that addresses the frameworks of the other previous models reviewed in this study (see Figure 4). This figure provides a mechanism for customer feedback in the pharmaceutical industry.

4. Discussion of the Model

As earlier stated, the drawback found in existing models is the lack of a feedback mechanism between manufacturers and the final consumers. Concerning that, this study proposes a model to help bridge existing frameworks' gaps and drawbacks. This model builds on existing blockchain and IoT frameworks that have been implemented and proposed to help track and trace the pharmaceutical supply chain,

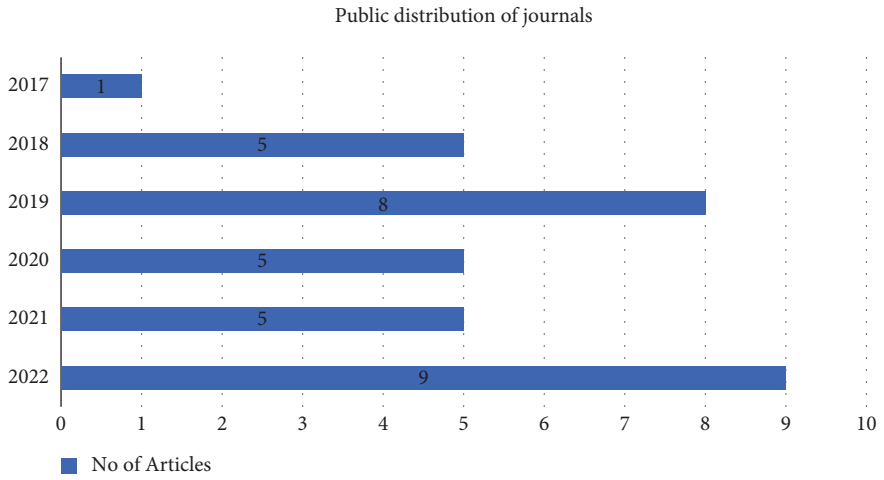


Figure 2: Public distribution of journals.

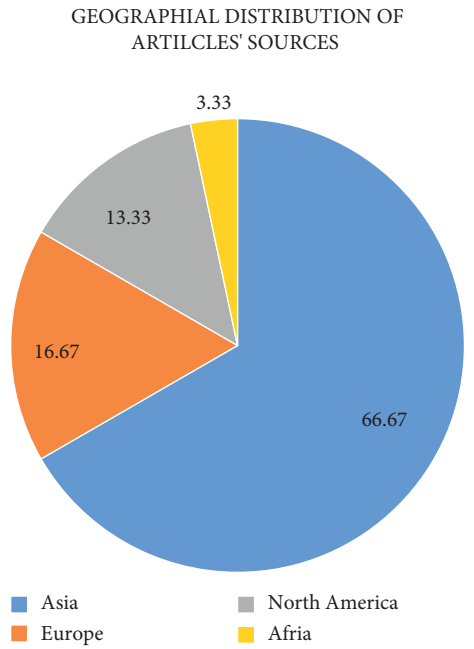


Figure 3: Geographical distribution of articles' sources.

ensure transparency, use smart contracts, proper conditions during the shipment of the products, and so much more.

For this system to be effective and widely accepted, an incentive model is attached whenever a user gives feedback to the system or manufacturer. This comes in the form of a token with several perks it offers as initially stated above. Manufacturers or producing pharmaceutical companies create a decentralized autonomous organization, and the URL is embedded in a QR code label on the product container.

The user acquires the pharmaceutical products, and after verifying the validity of the product, the user scans the QR code label on the drug using an IoT device (a smartphone, laptop, tablet, etc.). The user is then taken to the DAO and is required to access the site using a web3 service provider such as metamask or coinbase. Upon successful creation of a web3 account, the user is prompted and given full access to other features of the DAO and can give feedback on the particular product. After this is done, the system rewards the user with the crypto token of the DAO's ecosystem. Autonomous means that the user's identity is unrevealed, and the user can operate the system autonomously as no sign-up requiring personal details of the user is required, a special feature of blockchain technology and web3.

4.1. Analysis of the Result. Regarding the electronic databases, 0.03% (6 papers) of the articles were obtained from the science direct database. 3.91% (721 papers) were obtained from the PubMed database. 0.65% (120 papers) were obtained from the research gate database, and 62.36% (9953 papers) were obtained from the Google Scholar database.

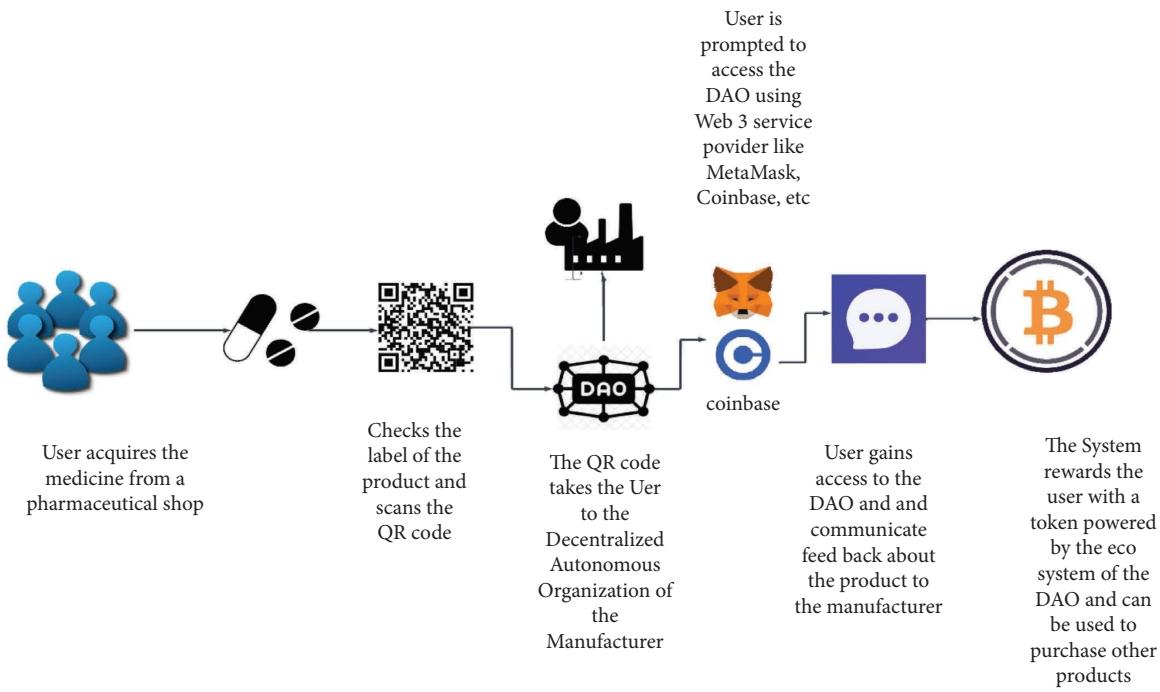


Figure 4: A hybrid framework of blockchain and IoT technology.

Table 3: Collection of the paper process.

Database	Science direct	Pubmed	Research gate	Google scholar
Papers	6	721	120	9953
%	0.03	3.91	0.65	62.36
Total		10800		

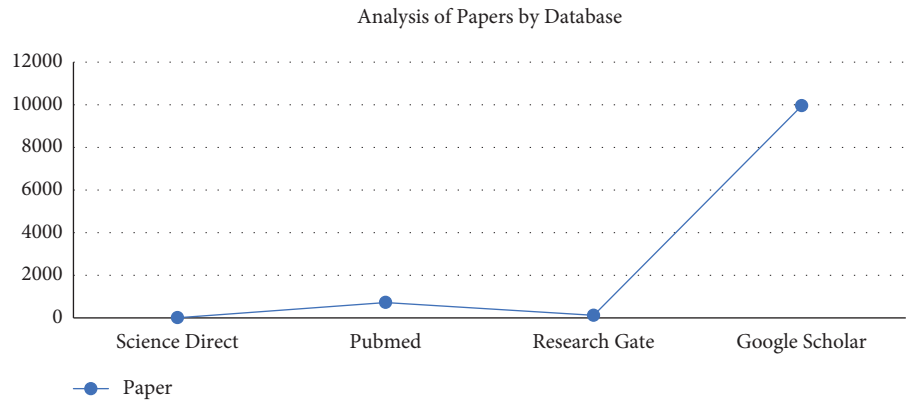


Figure 5: Public distribution of journals.

Table 3 shows the data analysis of articles extracted from various databases. Figure 5 displays the graphical representation of the paper collection. Table 4 displays the analysis of the state-of-the-art literature with the proposed study.

As shown in Table 4, only two articles offered a framework while utilizing blockchain and IoT technologies for medication delivery in the pharmaceutical sector. Many employed blockchain or IoT solely, while others proposed no framework. It was observed that the authors of references [41, 60] concentrated on bogus medication and drug counterfeit without taking into account the patient's feedback mechanism to the producer. Despite the growing relevance of blockchain and IoT, the literature has little practical research on the issue. This analysis reported that patients and drug manufacturers rarely interact with each other to obtain feedback on their products [57]. This research proposed a framework incorporating blockchain and IoT technology to allow patients to communicate with the manufacturer and provide feedback on the drugs.

Table 4: Analysis of the state-of-the-art literature.

S/N	Author	Model	Company	Methodology	Proposed solution
1	Bharany et al. [56]	Yes	Pharmaceutical	Blockchain and IoT	Curb false medications
2	Jochumsen and Chaudhuri [57]	No	Pharmaceutical	IoT and blockchain	Tracking of drugs
3	Tehrani and Jin [55]	No	Pharmaceutical	IoT	Monitoring patient
4	Alagarsamy et al. [48]	No	Pharmaceutical	IoT	Drug discovery for clinical trials
5	Gao et al. [46]	No	Pharmaceutical	Blockchain	Analyzed the future of blockchain
6	Humayun et al. [45]	Yes	Pharmaceutical	Blockchain	Drug distribution
7	Jaisimha and Kumar [44]	Yes	Pharmaceutical	IoT and smart contract	Optimize pharma supply chain
8	Sharma and Sikka [53]	Yes	Pharmaceutical	Blockchain	Avoiding drug counterfeit
9	Fekih and Lahami, [59]	No	Medicine	Blockchain and IoT	General overview of the two technologies
10	Lingayat et al. [58]	Yes	Pharmaceutical	Blockchain	Security of drug distribution
11	Proposed work	Yes	Pharmaceutical	Hybrid blockchain/IoT	Provide feedback to the patient and enhance security in the drug distribution chain

5. Conclusions

This study carried out a systematic literature review to understand the application areas of blockchain and IoT technology in the pharmaceutical industry and the existing frameworks that have been proposed to solve challenges relating to the pharmaceutical industry. Articles and literature were reviewed from chosen databases and analyzed. In addressing the drawbacks found in existing models of the pharma industry, a hybrid framework of blockchain and IoT was proposed for a feedback mechanism. The under-listed contributions were made to existing knowledge of this study.

(i) This study shows the research gap in blockchain and IoT technology applications in the pharmaceutical industry.

(ii) Analyzes the different methodologies and frameworks used in the pharmaceutical industry.

(iii) A model was proposed to get feedback from customers/consumers directly to manufacturers through the use of smart contracts to verify the validity and authenticity of pharmaceutical products and also help define other metrics such as effectiveness, duration of time usage, business intelligence, and drug compliance. Therefore, this study recommends the following for the future work.

(iv) A practical implementation of the proposed feedback mechanism model.

(v) Introduction of nonfungible tokens (NFTs) in the pharmaceutical industry to curb drug counterfeiting, spread awareness of diseases and symptoms, and also as a source of revenue.

The Internet of Things has impacted the pharmaceutical industry's logistics department and has created numerous opportunities. IoT integration in blockchain has significantly improved logistic operations. The Internet of Things simplifies supply chain operations and decreases the dangers that could lead to long-term disasters.

5.1. Future Scope. This study identifies gaps in the literature, highlights existing research activities, and proposes a research agenda for future investigations. The study's findings may help management construct a safe supply chain in medicine distribution and give a standardized feedback system in the pharmaceutical business, hence fostering decision-making processes. As a result, the findings of this study may serve as a guideline for medication manufacturers worldwide in terms of information. Because of the search criterion limitations in English, current blockchain and IoT publications published in other languages are omitted from this study. Some academic databases also are excluded. However, expanding this comprehensive study of the literature may be interesting for future research. Future studies can focus on new models, methods, and approaches for the pharmaceutical industry. The proposed framework in this study can be developed into more robust strategies for effective information dissemination and decision-making in the pharmaceutical industry.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020.

[2] W. H. Organization, *Monitoring the Building Blocks of Health Systems: A Handbook of Indicators and Their Measurement Strategies*, World Health Organization, Geneva, Switzerland, 2010.

[3] M. Shuaib, S. Alam, R. Ahmed, S. Qamar, M. S. Nasir, and M. S. Alam, "Current status, requirements, and challenges of blockchain application in land registry," *International Journal of Information Retrieval Research*, vol. 12, no. 2, pp. 1–20, 2022.

[4] B. A. Liang, "Fade to black: importation and counterfeit drugs," *American Journal of Law and Medicine*, vol. 32, no. 2-3, pp. 279–323, 2006.

[5] M. Schneider and C. Maillefer, "How Europe deals with private imports of counterfeit and pirated goods," *Journal of Intellectual Property Law and Practice*, vol. 10, no. 4, pp. 262–268, 2015.

[6] J. L. Bikoff, D. K. Heasley, V. Sherman, and J. Stipelman, "Fake it'til we make it: regulating dangerous counterfeit goods," *Journal of Intellectual Property Law and Practice*, vol. 10, no. 4, pp. 246–254, 2015.

[7] H. R. Campbell and R. A. Lodder, "Monetary incentives for producing counterfeit, adulterated, and misbranded medicine: case studies and examples," *CIC Pharmacy Science*, vol. 1, 2021.

[8] H. A. Barrett, A. Ferraro, C. Burnette, A. Meyer, and M. P. S. Krekeler, "An investigation of heavy metal content from disposable batteries of non-US origin from Butler County, Ohio: an environmental assessment of a segment of a waste stream," *Journal of Power Sources*, vol. 206, pp. 414–420, 2012.

[9] K. K. Kones, *Transnational Threats and National Security in Kenya*, University of Nairobi, Nairobi, Kenya, 2017.

[10] E. A. Blackstone, J. P. Fuhr, and S. Pociask, "The health and economic effects of counterfeit drugs," *Am. Heal. drug benefits*, vol. 7, no. 4, p. 216, 2014.

[11] A. Moore, *Not a child. Not old. Not a boy. Not a gir': Representing Childhood in 'Let the Right One In*, Inter-Disciplinary Press, Oxfordshire, OX, UK, 2020.

[12] M. Jaberidoost, S. Nikfar, A. Abdollahiasl, and R. Dinarvand, "Pharmaceutical supply chain risks: a systematic review," *DARU Journal of Pharmaceutical Sciences*, vol. 21, no. 1, pp. 69–77, 2013.

[13] L. Allen and H. C. Ansel, *Ansel's Pharmaceutical Dosage Forms and Drug Delivery Systems*, Lippincott Williams and Wilkins, Philadelphia, PS, USA, 2013.

[14] W. Abramowicz and R. Corchuelo, "Business Information Systems," in *Proceedings of the 22nd International Conference*, Seville, Spain, June 2019.

[15] M. Ur Rahman, B. Guidi, and F. Baiardi, "Blockchain-based access control management for decentralized online social networks," *Journal of Parallel and Distributed Computing*, vol. 144, pp. 41–54, 2020.

[16] Y. I. Alzoubi, A. Al-Ahmad, H. Kahtan, and A. Jaradat, "Internet of things and blockchain integration: security, privacy, technical, and design challenges," *Future Internet*, vol. 14, no. 7, p. 216, 2022.

[17] Y. Sun and S. I. Ali, "Internet of things (IoT) and blockchain applications in pharmaceutical supply chain provenance to achieve traceability, transparency, and authenticity," in *Advancing Smarter and More Secure Industrial Applications Using AI, IoT, and Blockchain Technology*, pp. 1–36, IGI Global, Hershey, PS, USA, 2022.

[18] R. M. A. Haseeb-Ur-Rehman, M. Liaqat, A. H. M. Aman et al., "Sensor cloud frameworks: state-of-the-art, taxonomy, and research issues," *IEEE Sensors Journal*, vol. 21, no. 20, pp. 22347–22370, 2021.

[19] M. K. I. Rahmani, M. Shuaib, S. Alam et al., "Blockchain-based trust management framework for cloud computing-based internet of medical things (IoMT): a systematic review," *Computational Intelligence and Neuroscience*, vol. 2022, p. 14, 2022.

[20] A. Srivastava, J. A. Hollenbach, P. K. Singh, M. Shuaib, and T. Alam, "The immunogenetics of COVID-19," *Immunogenetics*, vol. 12, no. 2, pp. 1–12, 2022.

[21] I. Haq and O. Muselemu, "Blockchain technology in pharmaceutical industry to prevent counterfeit drugs," *International Journal of Computer Application*, vol. 180, no. 25, pp. 8–12, 2018.

[22] M. Shuaib, N. H. Hassan, S. Usman et al., "Land registry framework based on self-sovereign identity (SSI) for environmental sustainability," *Sustainability*, vol. 14, no. 9, p. 5400, 2022.

[23] M. Sahoo, S. S. Singhar, and S. S. Sahoo, "A blockchain based model to eliminate drug counterfeiting," in *Machine Learning and Information Processing*, pp. 213–222, Springer, Berlin, Germany, 2020.

[24] S. Bhatia, S. Alam, M. Shuaib, M. Hameed Alhameed, F. Jeribi, and R. I. Alsuwailem, "Retinal vessel extraction via assisted multi-channel feature map and U-net," *Frontiers in Public Health*, vol. 10, Article ID 858327, 2022.

[25] M. Benchoufi, R. Porcher, and P. Ravaud, "Blockchain protocols in clinical trials: Transparency and traceability of consent," *F1000Research*, vol. 6, 2017.

[26] M. Shuaib, N. H. Hassan, S. Usman et al., "Self-sovereign identity solution for blockchain-based land registry system: a comparison," *Mobile Information Systems*, vol. 2022, Article ID 8930472, 17 pages, 2022.

[27] R. A. Rayan and M. A. M. Zubair, "IoT-integrated blockchain in the drug supply chain," in *EAI/Springer Innovations in Communication and Computing*, pp. 105–117, Springer, Berlin, Germany, 2021.

[28] M. Shuaib, N. Hafizah Hassan, S. Usman et al., "Identity model for blockchain-based land registry system: a comparison," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 5670714, 17 pages, 2022.

[29] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trustchain: trust management in blockchain and iot supported supply chains," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 184–193, July 2019.

[30] P. Pandey and R. Dhanalakshmi, "A counterfeit solution for pharma supply chain," *EAI Endorsed Transactions on Cloud Systems*, vol. 3, no. 11, Article ID 154550, 2018.

[31] H. L. Pham, T. H. Tran, and Y. Nakashima, "Practical anti-counterfeit medicine management system based on blockchain technology," in *Proceedings of the Technology Innovation Management And Engineering Science International Conference 4th 2019*, Bangkok, Thailand, December 2019.

[32] V. Plotnikov and V. Kuznetsova, "The prospects for the use of digital technology 'blockchain' in the pharmaceutical market," *MATEC Web of Conferences*, vol. 193, pp. 02029–2036, 2018.

[33] S. Alam, "A blockchain-based framework for secure educational credentials," *urkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, 2021.

[34] A. M. Makarov, "Blockchain technology in the production and supply of pharmaceutical products," *Advances in Economics, Business and Management Research*, vol. 105, pp. 929–933, 2019.

[35] G. Subramanian, A. SreekantanThampy, N. Valbosco Ugwuoke, and B. Ramnani, "Crypto pharmacy – digital medicine: a mobile application integrated with hybrid blockchain to tackle the issues in pharma supply chain," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 26–37, 2021.

[36] F. Chiacchio, D. D. Urso, L. M. Oliveri, D. Giordano, A. Spitaleri, and C. Spampinato, "A non-fungible token solution for the track and trace of pharmaceutical supply chain," *Applied Sciences*, vol. 12, 2022.

[37] G. Gogos and L. Rochelle, "Exploring supply chain blockchain potential in the pharmaceutical industry," in *Proceedings of the International Conference on Industrial Engineering and Operations Management*, pp. 1529–1540, Istanbul, Turkey, March 2022.

[38] T. Aslam, A. Maqbool, M. Akhtar et al., "Blockchain based enhanced ERP transaction integrity architecture and PoET consensus," *Computers, Materials and Continua*, vol. 70, no. 1, pp. 1089–1109, 2022.

[39] D. M. Shashi, "Digitalization of pharmaceutical cold chain systems using IoT digital enabler," *International Journal of Engineering and Advanced Technology*, vol. 11, no. 5, pp. 133–137, Jun. 2022.

[40] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, S. M. Sam, and G. A. L. N. Samy, "Effect of quantum computing on blockchain-based electronic health record systems," in *Proceedings of the 2022 4th International Conference on Smart Sensors and Application (ICSSA)*, pp. 179–184, Kuala Lumpur, Malaysia, July 2022.

[41] M. Jammula, S. Navuduri, S. Krishna, and P. Ramayanam, "Iot based blockchain temperature monitoring and fake medicine prevention," *Sensors*, vol. 5, pp. 78–84, 2022.

[42] K. Kumari, "Cfdd (counterfeit drug detection) using blockchain in the pharmaceutical industry," *International Journal Of Engineering Research and Technology*, vol. 8, no. 12, pp. 591–594, 2019.

[43] M. Jain, A. Bijur, N. Chavan, and S. Rupani, "Blockchain to Overcome Counterfeiting of Medicines," *International Journal of Engineering Research and Technology*, vol. 9, no. 3, pp. 28–31, 2021.

[44] D. Jaisimha and P. Kumar, "Deployment of smart contract based blockchain to optimise pharma," *Supply Chain*, vol. 5, no. 1, pp. 67–73, 2022.

[45] M. Humayun, N. Z. Jhanjhi, M. Niazi, F. Amsaad, and I. Masood, "Securing drug distribution systems from tampering using blockchain," pp. 1–14, 2022.
[46] R. Gao, X. Yu, and Z. Zhang, "Blockchain for the future development of the pharmaceutical industry," *Proceedings of the 2021 3rd International Conference on Economic Management and Cultural Industry (ICEMCI 2021)*, vol. 203, pp. 2563–2568, 2021.
[47] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, N. A. A. Bakar, and N. Maarop, "Performance evaluation of DLT systems based on hyper ledger fabric," in *Proceedings of the 2022 4th International Conference on Smart Sensors and Application (ICSSA)*, pp. 70–75, Kuala Lumpur, Malaysia, July 2022.
[48] S. Alagarsamy, R. Kandasamy, D. P. Selvamani, and L. Subbiah, "Applications of Internet of Things in Pharmaceutical Industry," *SSRN Electron*, vol. 17, 2019.
[49] S. Alam, M. Shuaib, W. Z. Khan et al., "Blockchain-based initiatives: current state and challenges," *Computer Networks*, vol. 198, Article ID 108395, 2021.
[50] R. Raj, N. Rai, and S. Agarwal, "Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership," in *Proceedings of the 2019 IEEE Region 10 Conference (TENCON)*, pp. 1572–1577, Kochi, India, December 2019.
[51] N. Zakari, M. Al-Razgan, A. Alsaadi et al., "Blockchain technology in the pharmaceutical industry: a systematic review," *PeerJ Computer Science*, vol. 8, pp. 8400–e926, 2022.
[52] S. Jangir, A. Muzumdar, A. Jaiswal, C. N. Modi, S. Chandel, and C. Vyjayanthi, "A novel framework for pharmaceutical supply chain management using distributed ledger and smart contracts," in *Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, Kanpur, India, July 2019.
[53] M. Sharma and G. Sikka, "Blockchain based approaches for preventing drug counterfeit: a survey," *International Journal of Engineering Research and Technology*, vol. 7, no. 9, pp. 1–6, 2021, https://www.ijert.org/blockchain-based-approaches-for-preventing-drug-counterfeit-a-survey.
[54] M. M. Khubrani and S. Alam, "A detailed review of blockchain-based applications for protection against pandemic like COVID-19," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 4, pp. 1185–1196, 2021.
[55] N. Tehrani and Y. Jin, "How advances in the internet of things (IoT) devices and wearable technology will impact the pharmaceutical industry," *Journal of Applied Research*, vol. 4, pp. 1530–1533, 2018.
[56] S. Bharany, S. Badotra, S. Sharma et al., "Energy efficient fault tolerance techniques in green cloud computing: a systematic survey and taxonomy," *Sustainable Energy Technologies and Assessments*, vol. 53, Article ID 102613, 2022.
[57] M. L. Jochumsen and A. Chaudhuri, "Blockchain's impact on supply chain of a pharmaceutical company," *EUROMA Conf*, pp. 0–8, 2018.
[58] V. Lingayat, I. Pardikar, S. Yewalekar, S. Khachane, and S. Pande, "Securing pharmaceutical supply chain using blockchain technology," *ITM Web Conferences*, vol. 37, Article ID 01013, 2021.
[59] R. B. Fekih and M. Lahami, *Application of Blockchain Technology in Healthcare: A Comprehensive Study*, Vol. 12157, Springer International Publishing, Berlin, Germany, 2020.
[60] S. Bharany, S. Sharma, J. Frnda et al., "Wildfire monitoring based on energy efficient clustering approach for FANETS," *Drones*, vol. 6, no. 8, p. 193, 2022.

Hindawi
Mobile Information Systems
Volume 2022, Article ID 9156514, 16 pages
https://doi.org/10.1155/2022/9156514

Research Article

A Malware Detection Scheme via Smart Memory Forensics for Windows Devices

Muhammad Rashid Naeem,[1] **Mansoor Khan**,[1] **Ako Muhammad Abdullah**,[2,3] **Fazal Noor**,[4] **Muhammad Ijaz Khan**,[5] **Muhammad Asghar Khan**,[6] **Insaf Ullah**,[6] **and Shah Room**[7]

[1]*School of Electronic Information and Artificial Intelligence, Leshan Normal University, Leshan 614000, China*
[2]*University of Sulaimani, College of Basic Education, Computer Science Department, Sulaimani City, Kurdistan Region, Iraq*
[3]*Department of Information Technology, University College of Goizha, Sulaimaniyah, Kurdistan Region, Iraq*
[4]*Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia*
[5]*Institute of Computing and Information Technology, Gomal University, DIK, Pakistan*
[6]*Hamdard Institute of Engineering & Technology, Islamabad, Pakistan*
[7]*Ghalib University, Herat, Afghanistan*

Correspondence should be addressed to Mansoor Khan; khan007_bet@yahoo.com and Shah Room; zai_fhs@foxmail.com

Received 3 July 2022; Revised 20 August 2022; Accepted 5 September 2022; Published 3 October 2022

Academic Editor: Junaid Shuja

With the introduction of 4G/5G Internet and the increase in the number of users, the malicious cyberattacks on computing devices have been increased making them vulnerable to external threats. High availability windows servers are designed to ensure delivery of consistent services such as business activities and e-services to their customers without any interruption. At the same time, a cyberattack on any of the clustered computer can put servers and customer devices in danger. A memory dump mechanism can capture the contents of memory in the event of a system or device crash such as corrupted files, damaged hardware, or irregular CPU power consumption. In this paper, we present a smart memory forensics scheme to recognize malicious attacks over high availability servers by capturing the memory dump of suspicious processes in the form of RGB visual images. Second, the local and global properties of malware images are captured using local binary patterns (LBP) and gray-level co-occurrence matrices (GLCM). A state-of-the-art t-distributed stochastic neighbor embedding scheme (t-SNE) is applied to reduce data dimensionality and improve the detection time of unknown malwares and their variants. An optimized CNN model is designed to predict malicious files harming servers or user devices. Throughout this study, we employed public data set of 4294 malicious samples covering malware variants and benign executables. A baseline is prepared to compare the performance of proposed model with state-of-the-art malware detection methods. The combined LBP + GLCM feature extraction along with t-SNE dimensionality reduction scheme further improved the detection accuracy by 98%, whereas the detection time is also increased by 73x. The overall performance shows that memory forensics is more effective for malware detection in terms accuracy and response time.

1. Introduction

Due to extreme and rapid development of Internet technology, the e-business and e-services has become a key part of daily life. Meanwhile, malicious software also known as malwares keep evolving and posing a security threat to the user devices. To overcome the security threats, the establishment of a fast and secure malware detection system is essential for high services of services. The well-known and commonly used malware detection methods rely on signatures, which use the sequences of binary patterns to uniquely identify malwares [1]. Antivirus programs detect malwares of similar behavior by matching malicious signatures of the scanning files. Signature-based malware

detection methods generally provides outstanding accuracy with fewer false positives. When a new malicious program enters a victims' device, the extraction process takes time to extract and read signatures leaving connected devices vulnerable for some time. Researchers have also suggested heuristic measures to detect suspicious files that could harm computer devices in order to tackle such vulnerabilities [2]. Heuristic methods were developed to detect unknown malwares by preserving suspicious program features. For instance, if an unknown packer is being used to protect detection, it could be listed as a suspicious software attempting to hide or modify its original signatures. Such methods have the potential to detect new unknown malwares, but their false positive rate is relatively high. Since many commercial software developers use packers or similar tools to stop hackers from breaching or manipulating their products for free. Researchers have been developed many strategies to overcome limitations of malware detection such as static, dynamic, and hybrid strategies [3].

Static methods can easily recognize from other detection techniques since they need less malware detection time and do not require real-time malware execution. These methods typically analyze various aspects of suspicious programs such as sequences, byte patterns, opcode, API calls, and other relevant properties from portable executables (PEs) [4]. These aspects of suspicious program are collectively referred as signature, which is an algorithm or unique hash used to distinguish one malware from another such as malware families. As a result, no real-time execution or computational resource is required. However, static methods have some shortcomings such as code obfuscation or encryption, which can easily deceive malware detection strategy [5]. Therefore, an alternative and faster strategy is essential to detect obfuscated and encrypted malwares with a higher true positive.

Dynamic methods generate similar outcomes regardless of whether malware binaries are obfuscated or encrypted. Rather than examining the underlying features of a malicious code, a dynamic approach depends on examining discriminative behavior caused by real-time program execution. Dynamic methods generally execute programs in virtual environments such as sandboxes or virtual machines that are designed to monitor malware behavior. To be more specific, a dynamic method examines function calls to uncover suspicious anomalies in order to detect malware [6]. However, these malware activities are further classified into several observation strategies such as function parameter analysis, function call analysis, information workflow analysis, trace and tack analysis, and dynamic visual analysis of malware execution. Apart from that, numerous activity analyzer tools are also accessible online for dynamic analysis of malware binaries and executables. These activity analyzer tools include TT analyzer, CW Sandbox, and Anubis, etc. Dynamic methods detect malware more effectively with fewer false positives, but extracting dynamic malware characteristics is more complicated and more time consuming than static analysis. Therefore, many researchers have developed hybrid strategies to overcome the shortcomings of static and dynamic methods to generate high positives ratios in small amount of time.

Given the drawbacks of static and hybrid methods, cybersecurity businesses are shifting toward artificial intelligence [7]. Artificial intelligence algorithms are proven to be more successful in assessing malware patterns than static or dynamic methods. An AI algorithm uses smart visual representation to capture malware characteristics using DWT (discrete wavelet transform), SURF (speeded up robust feature), GIST, and SIFT descriptors. The DWT and GIST descriptors can be used to capture global characteristics such as structural patterns, while the SURF and SIFT descriptors can be employed to capture local information of malicious binaries. Few studies have adopted a combined approach to capture both local and global characteristics in order to enhance malware detection methods [8]. However, the cybercriminals are actively creating new malwares variants making their detection more challenging that may require new strategies to overcome security threats [9].

Recently, memory forensics such as examining the volatile memory has shown to be a more effective compared to static, dynamic, and signature-based malware detection methods. Memory forensic-based malware detection is determined into two phases. The first phase involves the transformation of virtual or physical memory data into memory dump files, while the second phase involves numerous analyzers to uncover anomalies or malicious behavior caused by malware execution. Lastly, the smart techniques like artificial intelligence are used to detect actual malware binaries [5]. According to Dai et al. [10], a malware executable in a volatile memory is most likely to be uncovered compared to mapping malicious signatures. Although some malwares can disguise themselves using encryption or packing, but eventually exposes their vital information such as code and data segmentation during real-time process execution. As a result, memory forensics can detect malware by examining victims' computer RAM. Furthermore, latest malware variants can escape detection by eradicating the evidence of their existence that may overshadowed by traditional detection methods. Fortunately, such malwares stay in volatile memory until malicious task is completed. A memory utilization strategy can effectively detect these malwares by obtaining memory dumps. Given the capability and flexibility of memory forensics, we can transform volatile memory binary data into RBG images as a source of information from dumped processes. The feature descriptors can further extract discriminating information for faster detection using artificial intelligence algorithms. The main contributions of this paper are listed as follows:

(i) A malware detection architecture is proposed for windows devices that applies memory forensics to capture discriminating behavior of malware and benign samples instead of malware signatures, which can be obfuscated and encrypted to evade detection.

(ii) We used RGBs of different resolutions such as 224×224 and 300×300 to capture the effects of memory dumps on malware samples. Few malware binaries consist of small resolutions compared to

others that may not capture sufficient discriminating information. Instead, we used different resolutions and 3-channel RGB images to extract malicious features from both malware and benign samples.

(iii) We used combined LBP + GLCM descriptors for feature extraction instead of single image descriptor. LBP has the ability to recognize unchanging pitch and variation against monotonic grayscale contrast with great precision. The smoothness, softness, and roughness characteristics of image can be used to measure the textural variations. Alternatively, the GLCM captures the spatial distributions of pixels that holds textual information. It further exploits degree of correlation between two adjacent gray pixels separated by distance at certain position to measure discrimination of global characteristics. Lastly, both local and global characteristics are fused to capture both types of textural features.

(iv) We further applied t-SNE dimensionality reduction and visualization to transform high-dimensional and complex features into low-dimensional space. Since LBP and GLCM generate large number of features from a single malware image. Therefore, the artificial intelligence algorithms require an extensive amount of time over data training and prediction, which is improved by t-SNE algorithm.

(v) An optimized fine-tuned CNN model is ensembled for a public data set of 4294 malware + benign executables to perform malware detection and variant classification. The proposed model is further compared to state-of-the-art models and related works to evaluate performance.

This study is structured as follows: Section 2 describes a literature review on malware detection strategies. Section 3 describes the overall architecture of malware detection covering data selection, feature analysis, extraction methods, and evaluation matrices. Section 4 examines experimental findings and state-of-the-art comparison. Section 5 concludes this research and outlines the future works.

2. Literature Review

Since the 5G network has been deployed worldwide, the demands for high-performance service delivery are rapidly increasing. The global Internet traffic via Internet devices has been grown to 54.8% since the first quarter of 2017 [11]. The number of malicious attacks is expected to grow further in future as the demand for Internet devices expands, which is also one of the major tasks in future Internet of things. Many studies on malware detection have been undertaken, but the malware detection via image processing has proven to be more effective. In this approach, the meta information of malware is retrieved from executables or binaries and then transformed into grayscale or color images to achieve predictive malware detection. This section discusses the pros and cons of some of these approaches.

Han et al. [12] used graph theory and information entropy-based associations to find distinguishing malware characteristics. Hidden patterns were first identified and transformed into grayscale images. Later, entropy graphs were generated to expose potential malware families. The empirical analysis of 1000 malware samples achieved around 97.9% overall accuracy. Barath et al. [13] further extracted textural patterns from malware images and conduct PCA assessment on the collected features. The principal components were then loaded into a nearest neighbor classifier to perform detection. The empirical analysis of 10,000 samples produced an average accuracy of 96% on eight malware families. Xiaofang et al. [14] retrieved localized hashing patterns from malware images using SIFT descriptor and achieved n accuracy of 85% on a data set of 8410 malware samples consisting of 25 families. Although, the SURF descriptor has proven to be robust than the SIFT descriptor while extracting local textual characteristics, but SURF is not resilient to pixel rotation and illumination.

Several studies exploited the capabilities of deep neural networks to overcome the limitations of simple machine learning methods. For instance, Bozkir et al. [15] analyzed malware and benign files using several neural network models. In the beginning, raw malware and benign binaries were collected from executables and transformed into colored images. Later, a public data set of 12,394 malicious files was partitioned into 8750 train and 3644 test images for performance analysis. The empirical study achieved 97.48% malware detection accuracy on the "DenseNet" framework. Natraj et al. [16] extracted local binary patterns from visual malwares using the GIST descriptor. First, malware binaries were transformed to grayscale images, and afterward classification algorithms were employed to analyze extracted patterns. Their proposed model obtained 97% accuracy on a data set of 9339 malware samples from 25 families.

Malware attacks are not only affecting Windows PCs but also the Internet and industries. As a result, Ullah et al. [17] developed a CNN model to identify malware attacks on industries over the Internet. For visualization, the Internet malware binaries were first transformed into colored images. Hemalatha et al. [18] proposed an efficient DenseNet neural network model for malware detection based on grayscale images. Experimental evaluation of four public malware data sets Malimg [16], BIG-2015 [19], MaleVis [15], and Malicia [20] produces 98.23%, 98.46%, 98.21%, and 89.48%, respectively. Multi neural networks can optimize the performance of single neural network [21]. Ullah et al. [22] used a hybrid multimodel image representation for malware classification to improve prediction time and accuracy. Their multimodel approach able to produce 98% to 99.4% accuracy on two different malware data sets. Federated learning allows devices to combinedly learned and scared prediction model. Rey et al. [23] federated learning approach able to produce 99.92% accuracy on known devices and 98.59% accuracy on unknown devices, respectively.

Memory forensic has recently gained more popularity for malware detection. Dai et al. [24] used HOG descriptor to extract features based on memory dumps. The extracted features were then used to train deep neural networks on

grayscale images. Grayscale images greater than 4 MB were resized to 4096 pixel width using the bicubic interpolation method. As per the empirical study, the accuracy performance was improved by 96.7% on malware detection. In another study, Bozkir et al. [25] employed memory forensics and computer vision to detect malware and their variants. Instead of grayscale images with limited characteristics, a malware data set consisting of 4294 colored images is prepared with public access. They further used UMAP feature reduction strategy and GIST + HOG descriptors to improve detection accuracy on different predictive models. The empirical evaluation achieved up to 96.39% detection accuracy with an average detection time of 3.56 seconds. HOG is a well-studied descriptor that performs well on human-based detection but also sensitive toward image rotation as it uses only one direction for each image pixel. It is quite possible that feature extraction process may lose some discriminating information as many malwares are obfuscated or encrypted to avoid detection. In our study, we use LBP that uses eight directions for each pixel. Therefore, LBP can effectively map discriminating behavior regardless of obfuscation or encryption. Furthermore, GLCM extract spatial relationship among different pairs of pixels. Hence, a smart memory forensic approach with combined LBP + GLCM descriptor and t-SNE dimensionality reduction can overcome such limitations.

3. Malware Detection via Memory Forensics for Windows Devices

The malware detection architecture for windows is designed to examine memory dump files for the identification of potential malware from interconnected user devices. The memory dump files can capture malware anomalies and execution process in real time. As a result, we can identify the discriminating behavior of malware and benign executables more efficiently. This section briefly explains the data set and descriptors along with dimension reduction strategy used to implement malware detection architecture. Figure 1 presents the overall structure of malware detection framework based on memory forensics. In the first phase, we focused on generating dump files from volatile memory of malicious process using a virtual machine. The second phase focused on binary file representation of malware into 224×224 and 300×300-dimensional RGB images. Next, feature extraction process is carried out using LBP and GLCM descriptors to extract discriminating characteristics of malware and benign samples. Malware visual images consist of both local and global textures. The local features refer to those patterns that depict distinct structure such as an edge, a point, or a small patch. Alternatively, the global features refer to those patterns associated to the whole image shape or structure. Since a single descriptor can only capture the limited information. Therefore, a feature fusion strategy can facilitate neural network to learn image features from their rich internal and external information. The resulting feature set can effectively classify both malware and benign samples regardless of computational complexity and obfuscation. Next, the t-SNE dimensional reduction and data visualization are also applied to reduce high-dimensional data into low-dimensional feature space. Lastly, several state-of-the-art algorithms were utilized to evaluate malware detection and classification performance. In this study, we utilized memory forensics instead of traditional signature-based methods. Memory forensics analyze the process under execution rather than matching signature of malicious structure or code of malware executable. The memory forensic process transforms physical memory data into dump files to uncover anomalies or malicious behavior of a malware sample throughout its execution. Any malware in a volatile memory is most likely to be exposed compared to signature matching. Since many malwares disguise themselves via encryption or packing. However, such malwares expose their vital information such as code and data segmentation during real-time execution. As a result, memory forensic process detects malware by examining RAM data of a computer or user device. The advanced malware variants can avoid detection by erasing traces of their activity, enabling them to escape detection from traditional methods. These malwares remain in volatile memory until the malicious process is executed. A memory forensic method can detect such malwares by obtaining memory dumps of terminated processes.

3.1. Dumpware10 Data set . Several public malware data sets have been widely studied in the literature to detect and validate different types of malwares and their variants. Although these data sets have greatly improved malware detection strategies, they are restricted by two fundamental limitations. The first limitation is the unavailability of portable executables due to security concerns of data sharing. The second limitation is the lack of benign samples, which is essential for discriminating between actual malware and benign samples apart from malware variants. The negative samples are essential in classification tasks. For instance, benign samples serve as negative samples in malware detection process; alternatively, malware classification without benign samples is regarded as a close-set problem [25]. The primary objective of our study is to develop a classification model capable of identifying suspicious processes whether malicious or not. This study focuses on employing memory forensics to identify suspicious processes, which may simply overlook by traditional signature-based malware detection techniques possibility due to obfuscation and encryption. As a solution, we selected a public malware data set Dumpware10, which is entirely based on memory forensics and contains 3686 malware and 608 benign samples. We further partitioned the data set into 80% train, 20% validation, and 20% test sets for malware detection and classification.

3.2. LBP Feature Descriptor. The LBP descriptor is one of the simplest and most reliable methods for extracting local features from textural images such as malware representation. LBP has the ability to recognize grayscale micropatterns from visual images with great precision [26]. In computer vision, the texture properties of an image are used

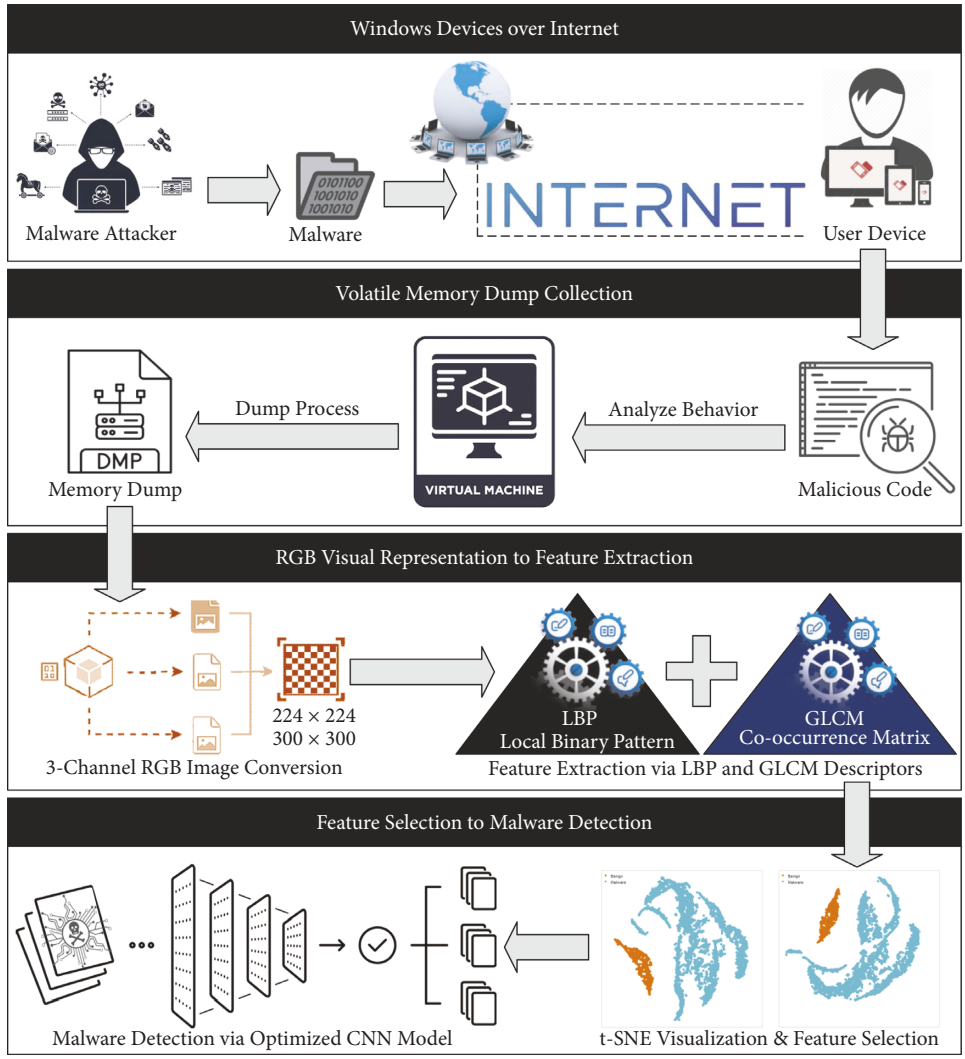


Figure 1: An overall malware detection framework for windows devices via smart memory forensics.

to characterize the degree of variations or spatial changes in textual patterns. The smoothness, direction, softness, and roughness characteristics of each surface can be used to measure textural variations. Such patterns required a strong descriptor to extract all distinctive features. We adopt the LBP descriptor to capture the unchanging pitch or variations produced by irregular malware patterns.

The LBP descriptor measures intensity in a digital image using a threshold value for adjacent pixels. Following that, LBP further assigns a decimal label to that threshold pixel. Figure 2 presents a 3×3-pixel block to demonstrate how the LBP descriptor extracts discriminating characteristics from a malware image. A 3×3-pixel block is chosen to examine each pixel intensity, with the central pixel of the block acting as the threshold value for neighboring pixels, i.e., 130. Subsequently, all pixels in the block with values greater than the threshold have been assigned a bit value of 1, while all remaining pixels in the block with values less than the threshold have been assigned a bit value of 0. In this way, each neighboring pixel has an assigned value to it is either 0 or 1. Next, the LBP descriptor locates all values clockwise other than the central pixel and returns an 8 bit binary number, which in our case is 10101101. Lastly, the central pixel's 8 bit value is transformed to a decimal number, which is 173 for the binary number 10101101 used in this example. Once, labels are assigned to pixels, the final feature set is calculated from pixel values in the form of a histogram.

The LBP descriptor has proven to be very successful in visual malware analysis; however, resultant images may have large dimensions. As a result, the characteristic of the larger structures cannot be retrieved using only 3×3-pixel block. To overcome this problem, we used LBP descriptor with different radiuses depending on the size of malware images. The final LBP feature set was constructed and merged after calculating histograms for each radius. The computational execution of LBP descriptor is further detailed in the form of four-step procedure:

(i) For each pixel on the x- and the y-axes, select surrounding pixels P within a defined radius R.

(ii) Determine difference in the intensity between the current pixel on the x and y axes and the surrounding pixels P.

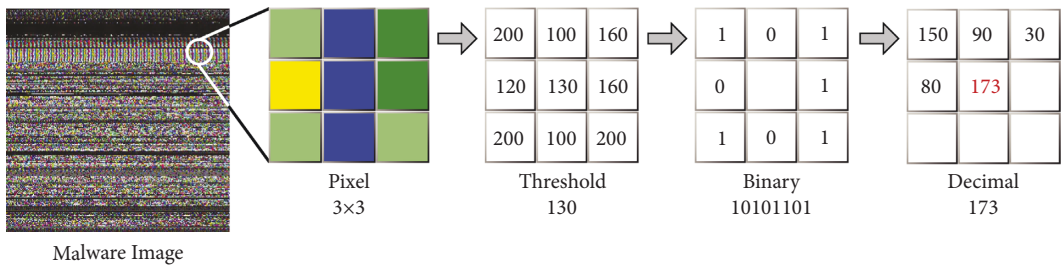


Figure 2: Example of LBP estimation for 3×3-pixel block from RGB malware image.

(iii) Choose a threshold value for the surrounding pixels P and use intensity difference to assign 0 and 1 as single bit values.

(iv) Transform the bit sequence of the surrounding pixels P to decimal values and replace the original intensity value of current pixel with the computed decimal value.

The LBP descriptor decimal value for each pixel is computed as follows:

$$\mathrm{LBP}(P, R) = \sum_{P=0}^{P-1} f\left(g_p - g_c\right) 2^p. \quad (1)$$

Here g_c and g_p are the intensity differences between the current pixel and its surrounding pixels, whereas P is the number of surrounding pixels for a given radius R.

3.3. GLCM Feature Descriptor. Haralick et al. [27] proposed the gray level co-occurrence matrix (GLCM) descriptor for extracting global features from digital images. The GLCM descriptor primarily built on the concept that the spatial distribution of pixels holds the textural information of the image. GLCM exploits a co-occurrence matrix to estimate the joint probability distribution of two gray pixels separated by distance d at certain position in the image. GLCM employs three important aspects: direction (θ), variation amplitude (d), and neighboring interval or gray level to extract integrated information from a grayscale image. The direction (θ) refers to the change in grayscale angle, which includes the primary direction of texture changes such as 0^o, 45^o, 90^o, and 135^o among others. The offset (d) is the distance between two pixels in a grayscale image, whereas two adjacent pixels indicate the gray level orientation and offset value of pixels equal to 1. The gray-level orientation of pixels indicates maximum grayscale value plus 1, which is used to signify grayscale compression. Figure 3 demonstrates the feature extraction process of an RBG image with offset value 1 in the direction of 0 degree and gray level 3. The first step in the GLCM descriptor is to transform an RGB-colored image to grayscale in order to apply compression. The grayscale compression is useful for reducing matrix dimensions and feature extraction time for larger images. In order to generate co-occurrence matrix, pixel pairs were selected on position i and j for each element in the matrix. The initial co-occurrence value for a matching pair is 1 which is incremented by 1 when the next identical matching pair is recognized. The numbers are then multiplied by 2 to reconstruct the co-occurrence matrix in the opposite direction. The GLCM descriptor offers a significant number of co-occurrence matrices that cannot be used as a final feature set. As a result, we simply employed four co-occurrence matrix properties to build the final feature. The selected GLCM properties of the visual images are energy, contrast, correlation, and homogeneity indicators. The final GLCM feature set consists of 20 columns, with each indicator comprising of 5 directions, resulting in 4 indicators × 5 directions.

LBP and GLCM descriptors are quite effective in terms of malware classification with few minor limitations. For instance, LBP is not insensitive to pixel rotations. The size of feature set increases the number of neighbors, which may also increases the computational complexity of descriptor. The structural information of LBP is also restricted as it only captures the pixel variations. Alternatively, the GLCM descriptor characterizes textural patterns by assessing the occurrences of pixel pairs in specific spatial relationship. A large number of computational resources are required as multiple matrices are computed to identify pixel pairs. Furthermore, GLCM features are also not insensitive to pixel rotation as well as changes in textual scaling. Although computational complexity is a significant issue when descriptors applied to large number of images. To overcome this limitation, we resized malware images into 200×200 and 300×300 dimension to resolve computation cost overhead in effective manner.

3.4. t-SNE Visualization and Dimensionality Reduction. The t-distributed stochastic neighbor embedding (t-SNE) is a nonlinear dimension reduction strategy used to visualize high-dimensional data in two or three low-dimensional planes with apparent distinction [28]. The t-SNE method reduces high dimensionality in 2 steps. In the first step, high-dimensional data points are assigned to similar objects with a higher probability of selection. In the second step, t-SNE minimizes divergence in low-dimensional space by adopting a uniform probability distribution. The t-SNE visualization is highly popular due to its potential to scale high-dimensional data into low-dimensional space. The t-SNE algorithm begins processing by employing stochastic neighbor embedding (SNE) on the data points and then transforms the high-dimensional distance between elements into the probability of similarities. The similarity between two data points from x_j to x_i is represented in terms of conditional probability $p_{j|i}$ using equation (2).

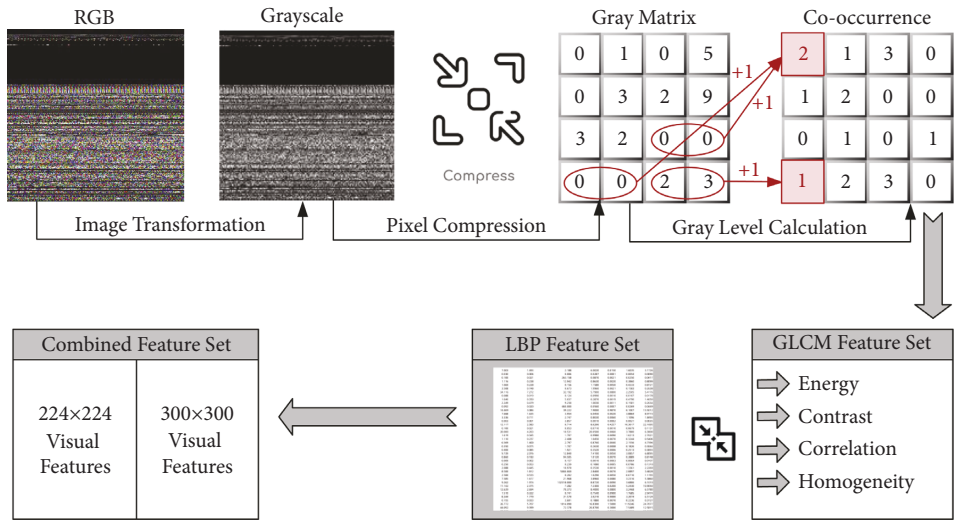


Figure 3: GLCM co-occurrence estimation using four properties from RGB malware image.

$$P_{j|i} = \frac{\exp\left(-1\left\|x_i - x_j\right\|^2 / 2\sigma_i^2\right)}{\sum_{k \neq i} \exp\left(-\left\|x_i - x_k\right\|^2 / 2\sigma_i^2\right)}. \quad (2)$$

The probability of similarity in the original feature space is statistically determined using equation (3).

$$P_{i,j} = \frac{P_{i|j} + P_{j|i}}{2n}. \quad (3)$$

Here n represents the length of a data set. The t-SNE method requires an input parameter termed as "perplexity," which can be interpreted as an uniform measurement of an effective number of clusters [29]. Mathematically, perplexity can be expressed as

$$\text{Prep}\left(P_i\right) = 2^{H\left(P_i\right)}. \quad (4)$$

Depending on the pairwise distances between data points, t-SNE method automatically determines the variance σ_i, such that the effective number of clusters corresponds to the user-defined perplexity value. To minimize congestion between data points, t-SNE adopts the student t-distribution based on single degree of freedom. The probability at low dimension q_{ij} is estimated using the matching distribution, as shown in equation (5).

$$q_{ij} = \frac{\left(1 + \left\|y_i - y_j\right\|^2\right)^{-1}}{\sum_{k \neq l} \left(1 + \left\|y_k - y_l\right\|^2\right)^{-1}}. \quad (5)$$

Many studies [30] stated that t-SNE distribution plots can be viewed as visual clusters of common distributions. These visual clusters can be improved further by adjusting parameters such as perplexity value and number of iterations. To construct optimal visual clusters, one must grasp the t-SNE parameters and information provided. Moreover, exploratory analysis and supplemental data can facilitate in the selection of appropriate parameters and the verification of the outcomes. The structure of visual clusters formed by t-SNE is more isolated resulting in a more reliable and observable shape. However, effectiveness of t-SNE algorithm is always influenced by input data. t-SNE reduces dimensionality by utilizing local data properties, which may fail if the data has an exceptionally high-dimensional structure. In addition, several optimization parameters may be necessary to locate the constructed solution. In this study, we integrated both descriptors into a single vector for each malware image and used t-SNE to capture discriminating behavior of both descriptors into three dimensions. We then fed the t-SNE output into a deep learning model to evaluate performance in terms of accuracy and training time.

3.5. Memory Dumps of Malicious Processes. Malware detection via memory forensics has recently gained more popularity since process information is stored in volatile memory throughout its execution. As a result, suspicious activity can be retained from volatile memory in the form of memory dumps. One significant advantage of memory forensics is their resistance to obfuscation and packing as the runtime behavior of process remains unchanged. Memory dumps are system core dumps that are frequently used for troubleshooting particularly in application development process. When the system dumps a process, it preserves all of its processing data including thread stacks, data segments, heap sectors, and the calling sequence in the form of raw binaries. We can further utilize memory dumps to extract potential abnormal behavioral information from physical memory. Figure 4 presents the memory forensics lifecycle of a malicious process that begins with runtime behavioral analysis and terminated with RGB image transformation. In this example, a cryptojacking malware i9prlkgopr.exe is retrieved via *JOESandbox* (https://www.joesandbox.com/) that infects the victim device using *XMRig* (https://xmrig.com/) miner. This malware performs two malicious activities

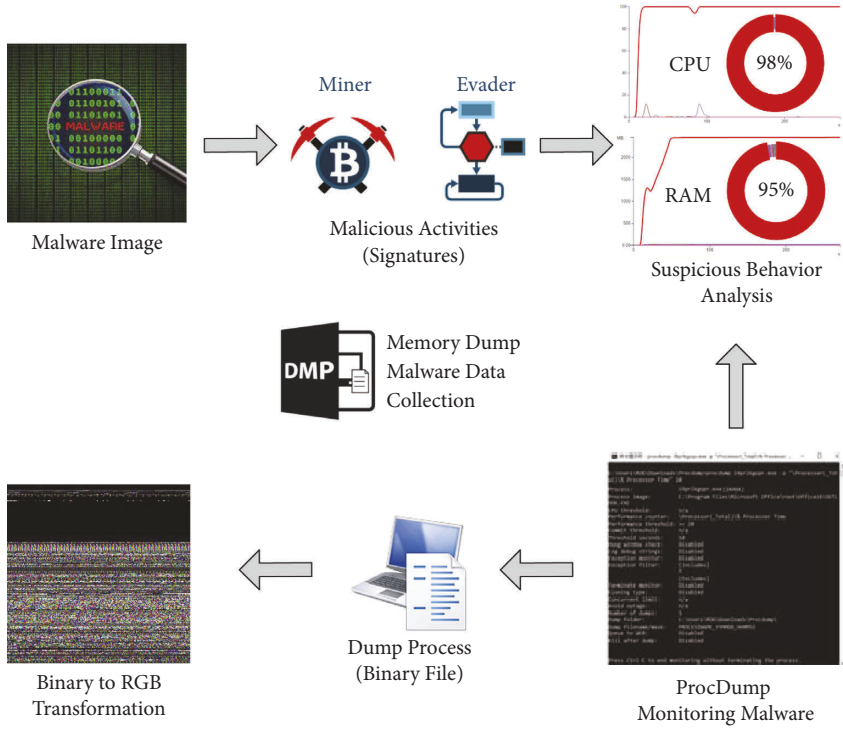


Figure 4: Memory forensics lifecycle for visual malware behavioral analysis.

to affect the victim computer. First, malware evades operating system protection using obfuscation and nonstandard tools. Second, it installs a miner script on the victim device in order to mine cryptocurrencies using the host CPU/GPU power. The miner script implemented by this malware can consume up to 98% CPU and 95% RAM depending on the configuration of the victim system. The malware is operated in a sandbox environment, while *ProcDump* is used to monitor suspicious activities. The *ProcDump* utility terminates the process and generates a raw memory dump file of the terminated process on detection of suspicious activity. Lastly, the raw dump binaries are transformed into RBG visual images to extract LBP and GLCM features for malware detection.

3.6. Optimized Convolutional Neural Network (O-CNN). The following section provides the overview of O-CNN model used to train deep learning models for malware detection and variant classification. Four parameter tuning components have been selected to construct the O-CNN model. The first component is the input layer used to initiate training process. The second component is a convolutional layer used to reduce noise and improve image characteristics. To optimize the learning performance, we additionally employed convolutional kernel width and learning rate. Next, a pooling layer and a dense layer have been utilized to transform two-dimensional image properties into a one-dimensional feature set. Figure 5 shows the internal structure of proposed O-CNN model including neural network layers. The brief overview of each layer and its fine-tuned functions is given below:

3.6.1. Convolutional Layer. The CNN layer collects crucial characteristics of input images such as interpretation, rotation, and scaling of invariance to reduce training parameters. It significantly decreases overfitting and increases the generalization capability of the proposed DCNN model. The input value of CNN layer consists of several building blocks [31]. The output mapping variable is computed based on total addition to input building block of CNN layer. The CNN mapping for random input x_j^l is shown in equation (6).

$$x_j^l = f\left(\sum_{i\epsilon M_j} x_j^{l-1} \times k_{ij}^l + b_j^l\right), \tag{6}$$

where M_j is the building block for CNN input; k_{ij}^l is a convolutional kernel that is combined with the i^{th} input and j^{th} output features; bias for the i^{th} input feature is represented by b_j^l; and f is an activation function associated to the corresponding CNN layer.

$$\delta_j^l = \delta_j^{l+1} W_j^{l+1} \times f'\left(u^l\right) = \beta_j^{l+1} \mathrm{up}\left(\delta_j^{l+1}\right) \times f'\left(u^l\right), \tag{7}$$

where $l+1$ signifies a pooling layer, W denotes the current convolution kernel, and $\beta_j^{l+1}\mathrm{up}(\delta_j^{l+1})$ specifies Upsampling for minor class. The partial derivative ∂ and error cost function of convolution kernel are computed as shown below:

$$\frac{\partial E}{\partial b_j} = \sum_{s,t}\left(\delta_j^l\right)u, v, \tag{8}$$

where $(\delta_j^l)u, v$ represents a patch value for each convolution kernel in a stack.

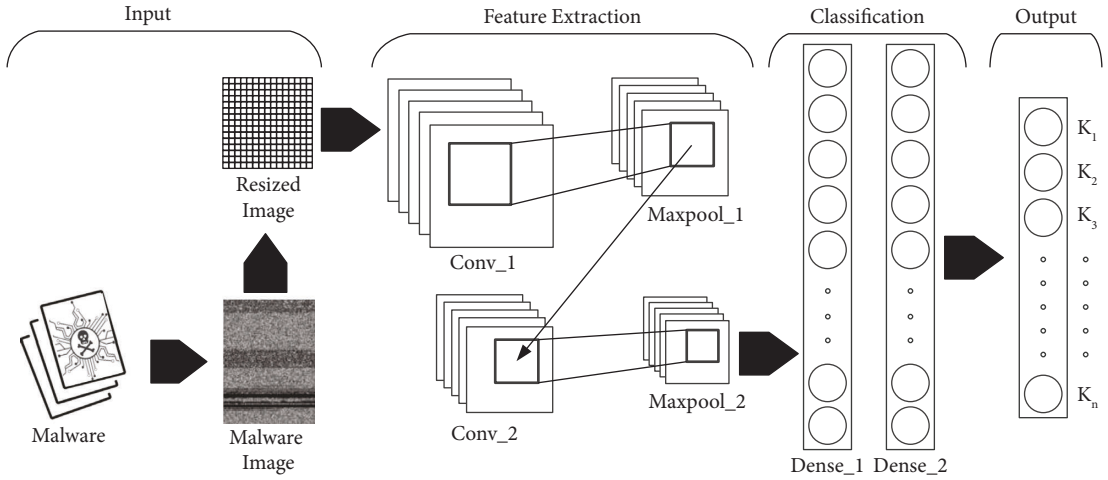


Figure 5: Internal structure of O-CNN model depicting convolutional, pooling, dense and output layers.

3.6.2. Pooling Layer. The DCNN model employs two types of pooling: maximal and average pooling. It has no effect on backward propagation but minimizes the effects of image deformation during DCNN training phase. The pooling layer further improves model performance while reducing the size of the visual input feature set:

$$x_j^l = f\left(\text{do wn}\left(x_j^{l-1}\right) + b_j^l\right), \tag{9}$$

where $\text{do wn}\,(x_j^{l-1})$ is a pooling task and b is the bias value. The overall sensitivity can be computed using following formula:

$$\delta_j^l = \delta_j^{l+1} W_j^{l+1} \times f'\left(u^l\right). \tag{10}$$

3.6.3. Dense Layer. In TensorFlow Keras, the output of the pooling layer is further characterized based on the dense layer. The neurons inside the dense layer are all interconnected to the neurons in the pooling layer. It flattened the two-dimensional feature vector into a one-dimensional feature space prior transferring it to the output layer of proposed DCNN model.

3.6.4. Output Layer. In the output layer, test samples of memory dump images were labeled as malware or benign files. To validate the performance of the train and test models, we employ the SoftMax-Cross Entropy loss function throughout the DCNN model. Equation (9) can be used to estimate the training and testing data loss.

$$\text{Loss} = -\log\left(\frac{\exp\left(f_{zt}\right)}{\sum_k \exp\left(f_{zt}\right)}\right), \tag{11}$$

where f_{zt} is the rank of the k^{th} class label. The Adam optimizer is also used to learn DCNN model parameters that minimize training data loss.

3.7. Evaluation Matrices. We selected several evaluation metrics also used in previous studies to measure the performance of malware detection. The independent variables of the study are true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN). TP refers to malware samples that have been correctly labeled, whereas FP refers to benign samples that have been mistakenly labeled as malware. Similarly, TN refers to benign samples that have been correctly labeled, whereas FN refers to malware samples that have been mistakenly labeled as benign. In addition to the base definitions, we utilized accuracy, precision, recall, and F_1-score as dependent variables to assess the overall predictive performance of the O-CNN and state-of-the-art detection models.

$$\begin{aligned}
\text{Accuracy} &= \frac{TP + TN}{TP + FP + TN + FN} \\
\text{Precision} &= \frac{TP}{TP + FP} \\
\text{Recall} &= \frac{TP}{TP + FP} \\
F_1 - \text{Score} &= 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \textit{Recall}}
\end{aligned} \tag{12}$$

4. Empirical Evaluation and Discussion

This section examines the impact of feature extraction descriptors on predictive models. First, the proposed O-CNN model is tested on both 224×244 and 300×300-dimension images. Second, the optimal feature set is applied to several predictive models for state-of-the-art comparison. The best outcome is further compared to existing studies. Finally, the selected features are visualized using t-SNE and overall performance on both image dimensions is evaluated.

4.1. Malware Detection via Proposed O-CNN Model. We examine the impact of 224×224 and 300×300-dimensional malware images on malware detection. Table 1 compares performance of three feature sets on O-CNN model. The

Table 1: Comparison of detection performance of DCNN model on three types of feature sets.

Feature	Dimension	Accuracy	Sample	Precision	Recall	F_1-score
LBP	224×224	0.9297	Malware	0.90	0.61	0.73
			Benign	0.93	0.99	0.96
	300×300	0.9399	Malware	0.97	0.96	0.96
			Benign	0.80	0.82	0.81
GLCM	224×224	0.8873	Malware	0.95	0.28	0.43
			Benign	0.88	1.00	0.94
	300×300	0.8929	Malware	0.87	0.36	0.50
			Benign	0.89	0.99	0.94
LBP + GLCM	224×224	0.9780	Malware	0.97	0.98	0.98
			Benign	0.98	0.97	0.98
	300×300	0.9807	Malware	0.98	0.99	0.98
			Benign	0.99	0.98	0.98

accuracy of all three feature sets is above 88% on both dimensions. The lowest accuracy is achieved by GLCM feature set on 224×224, while the highest accuracy is achieved by combining LBP + GLCM feature set on 300×300 dimensional images. The combined approach outperforms LBP and GLCM descriptors by achieving above 97% accuracy on both image dimensions. The main purpose of this study is to categorize malware and benign samples; therefore, we distinctly measure the precision, recall, and f1-score of malware and benign categories. GLCM recall value is pretty low compared to other descriptors, which is 0.28 on 224×224-dimensional images and 0.36 on 300×300-dimensional images. The observation shows that a large number of benign files were incorrectly classified as malware samples, even though the precision and recall of their benign samples are above 88%. LBP recall is 0.61 on 224×224-dimensional images, while the recall on 300×300-dimensional images is 0.96, respectively. From this observation, we conclude that local features are more effective in detecting malware patterns compared to global textural features. However, obfuscation and encryption strategies can evade detection. As a result, some textural global features can facilitate predictive model to effectively detect obfuscated malware samples.

The fine-tuned parameters are used to optimize the predictive performance of deep learning models. As a result, the model accuracy and model loss are observed on number of epochs to visualize potential overfitting or underfitting of deep learning models. We observed train and test accuracy of all three feature sets on 200 epochs for 224×224 and 300×300-dimensional images as shown in Figure 6. In comparison to LBP and GLCM feature sets, combine LBP + GLCM strategy fits train and test accuracy more effectively on proposed O-CNN model. In Figure 6(a), the LBP train and test accuracy begins at 0.86 and remains between 0.92 and 0.99 after 20 epochs, whereas the model accuracy of train data is 5% higher than model accuracy of test data. In Figure 6(b), the model accuracy of GLCM feature set is between 0.85 and 0.91, respectively. The overall model accuracy of LBP has shown to be better than GLCM. In Figure 6(c), the accuracy of combined LBP + GLCM feature set has shown to be most effective than all. The train and test model perfectly fit on each other without any visible differences. This observation showed that the fine-tuned parameters of O-CNN model can detect more unknown malware samples when local and global features of LBP and GLCM are deployed together.

A model loss is an outcome of a wrong prediction by a deep learning model. We use loss function to indicate how bad a model predicts on each test sample. Higher loss indicates worst prediction model for given samples. Figure 7 shows the train and test loss generated by proposed O-CNN model for three types of feature sets. In case of LBP feature set, the model loss of train and test samples have a difference of 30%. The lowest loss generated by train samples is 0.03, while the lowest loss generated by test samples is 0.30 on 200 epochs. In case of GLCM feature set, the difference in model loss of train and test samples is constant throughout epoch iterations that is around 9%. The combined LBP + GLCM approach proved be more effective by outperforming single feature descriptors. The train loss of combined LBP + GLCM feature set is less than 0.10, while the test loss of combined LBP + GLCM feature set is less 0.20 only.

A confusion matrix visualizes correct and incorrect samples predicted by deep learning models. Figure 8 shows a normalized confusion matrix of our best feature set combined LBP + GLCM on both 224×224 and 300×300-dimensional images using proposed O-CNN model. In the case of 224×224-dimensional images, the misclassification of benign samples is higher than malware samples. In confusion matrix, 3% benign samples were misclassified as malware, while 2% malware samples were misclassified as benign. For 300×300-dimensional images, the performance is further improved by achieving only 2% misclassification on benign samples and 1% misclassification on malware samples. From the observations of Figures 6–8, we conclude that the combined LBP + GLCM on 300×300-dimensional images is an optimal choice.

4.2. Performance Comparison with Related Works. We implemented optimal feature set on state-of the-art machine learning and deep learning classifiers for comparative evaluation of proposed DCNN model. Table 2 presents the performance of optimal feature set on five machine learning and four deep learning algorithms. The overall accuracy of combined LBP + GLCM feature set is above 80%. The lowest

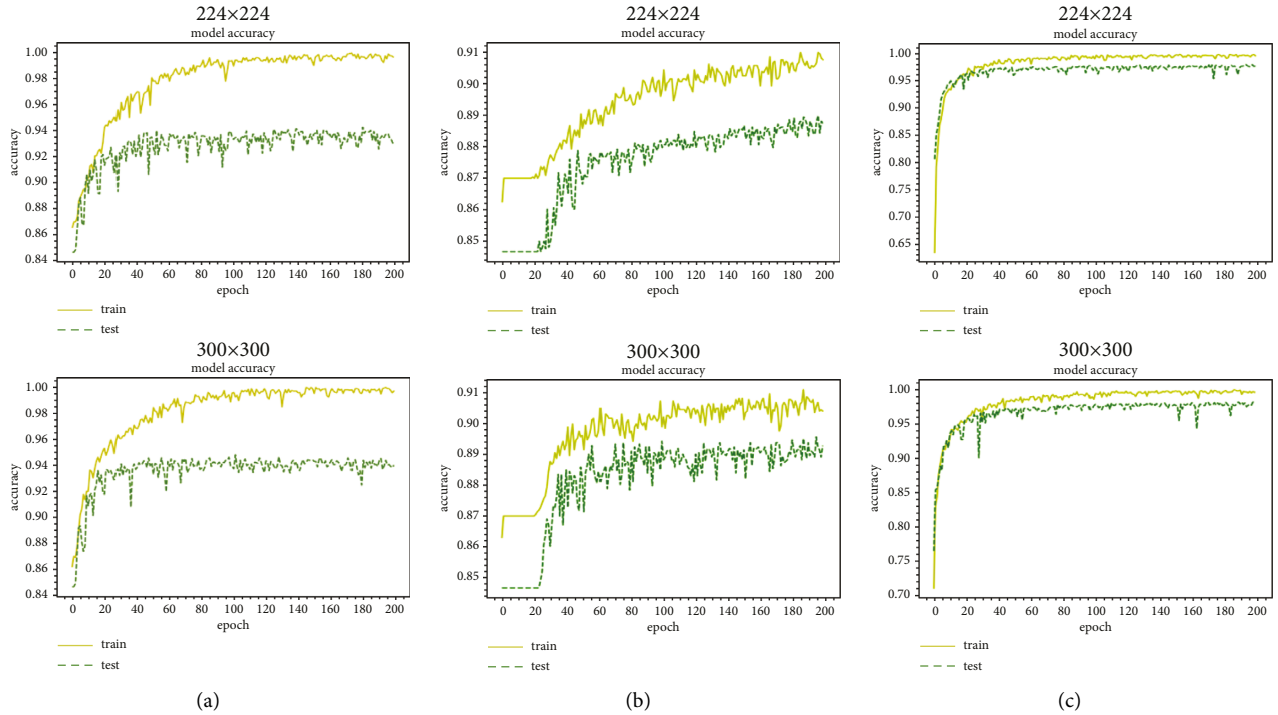


Figure 6: Train and test accuracy of three feature sets on proposed DCNN model. (a) LBP. (b) GLCM. (c) LBP + GLCM.

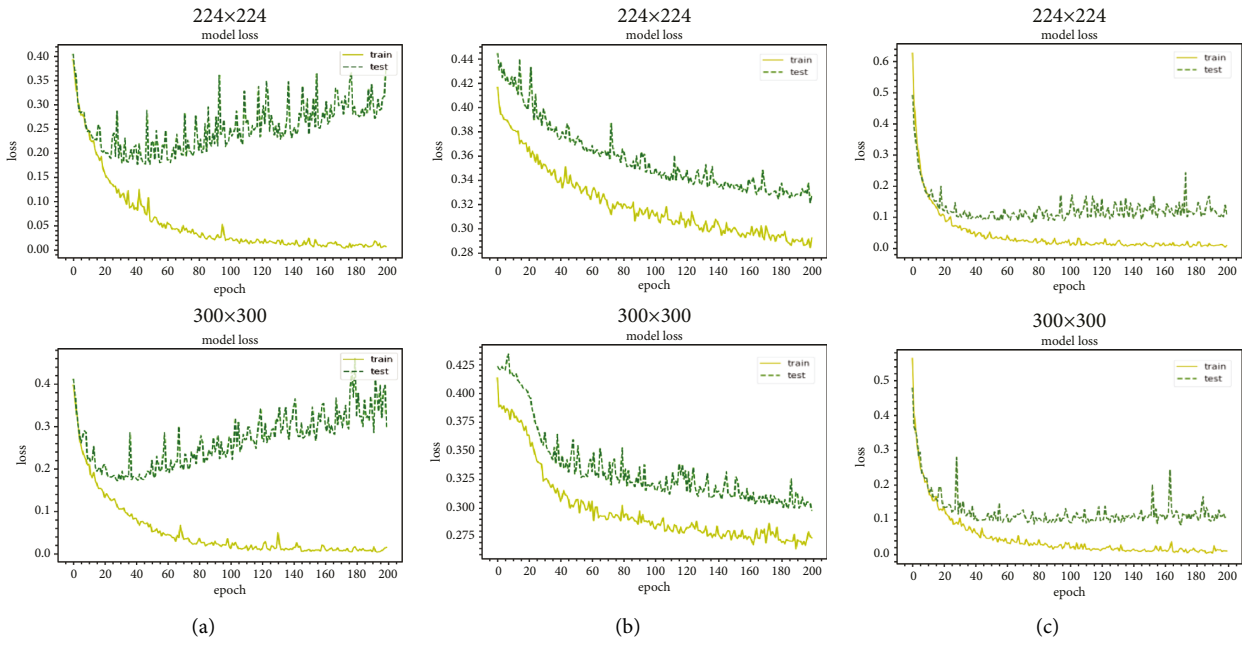


Figure 7: Train and test loss of three feature sets on proposed DCNN model. (a) LBP. (b) GLCM. (c) LBP + GLCM.

accuracy is achieved by naïve bayes classifier that is also above 80.4%, whereas the highest accuracy is achieved by the proposed O-CNN model. The proposed model outperforms other classifiers on all performance indicators. The average precision, recall, and f_1-score is 98% and model loss is 10%, respectively. In this observation, we conclude that the optimal feature not only performs efficiently on proposed model but also flexible to other predictive classifiers.

The optimal outcomes generated by proposed O-CNN model are compared to similar studies directed on various image dimensions. For instance, Nataraj et al. [16] used multidimensional images spanning between 32×32 to 1024×1024, and Dai et al. [10] used 2048×2048 and 4096×4096-dimensional images to implement their predictive models. Since the large images generate more features, therefore, enhancing the predictive performance of

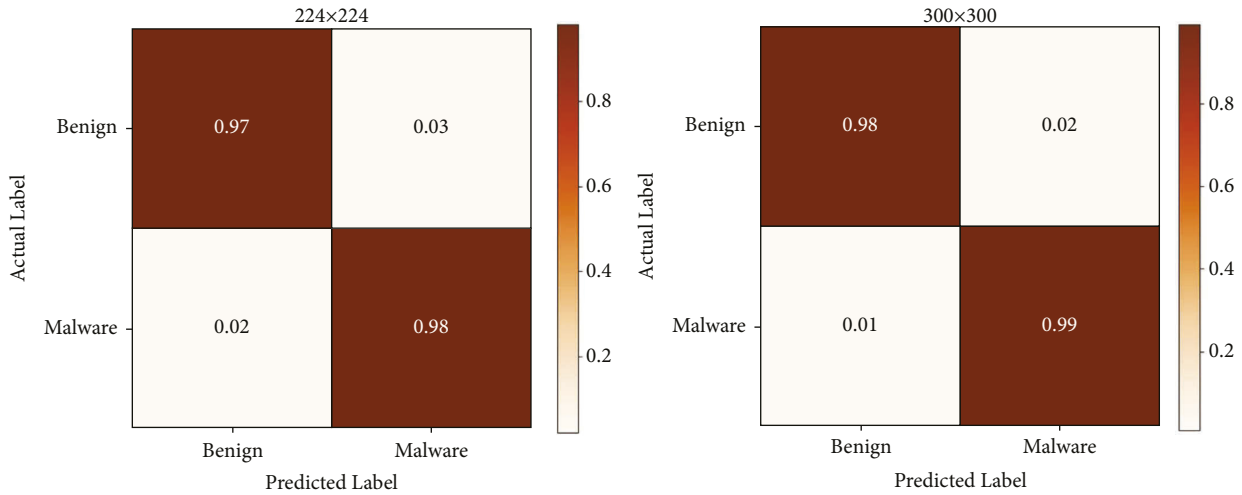


Figure 8: Confusion matrix of LBP + GLCM for 224×224 and 300×300-dimensional images.

Table 2: Comparison of state-of-the-art predictive models on optimal feature set

Classifier	Accuracy (%)	Precision (%)	Recall (%)	F_1-score (%)	Loss (%)
Logistic reg.	89.4	89.8	89.4	87.1	*N/A*
Naïve bayes	80.4	85.4	80.4	82.2	*N/A*
K-near neighbor	94.8	94.7	94.8	94.5	*N/A*
Decision tree	87.1	86.8	87.1	86.9	*N/A*
Random forest	91.5	91.4	91.5	90.4	*N/A*
DNN	84.7	72.0	85.0	78.0	43.0
GRU	94.7	95.0	95.0	95.0	20.0
RNN	85.9	91.0	86.0	87.0	36.0
LSTM	94.5	94.0	95.0	94.0	22.0
Proposed model	**98.1**	**98.0**	**98.0**	**98.0**	**10.0**

Table 3: Comparison of proposed DCNN model with other reference studies.

Study	Dimension	Accuracy (%)	Precision (%)	Recall (%)	F_1-score (%)
Nataraj et al. [16] (2011)	32×32 1024×1024	91.4	91.5	91.4	91.5
Dai et al. [10] (2018)	2048×2048 4096×4096	94.5	94.6	94.5	94.5
Rezende et al. [32] (2018)	224×224	96.9	97.0	96.9	96.9
Bozkir et al. [25] (2021)	224×224 300×300	96.3	96.4	96.4	96.4
Our method (optimal)	**224×224** **300×300**	**98.1**	**98.0**	**98.0**	**98.0**

deep learning models. Unfortunately, the larger images required more computational time and resources to extract all features. Rezende et al. [32] and Bozkir et al. [25] used 224×224 and 300×300 and generate more than 96% accuracy on four performance indicators. Table 3 shows the performance of proposed model compared to reference studies. In comparison to related studies, our combined LBP + GLCM strategy outperforms them by achieving more than 98% accuracy on same performance indicators.

4.3. t-SNE Visualization and Performance of Dimensionality Reduction. The t-SNE algorithm is an alternative way for cross-validation that does not require any data training like supervised algorithms. As an unsupervised algorithm, t-SNE does not use labels to classify but only reveals the structure of feature set and similarity between data points. t-SNE use perplexity value to balance local and global aspects of data on resulting plot. In general, it is observed that lower the perplexity value, the more local structure is preserved whereas with higher perplexity more global structure is preserved. We applied t-SNE visualization on both LBP, GLCM, and combined LBP + GLCM feature sets. We visualize the best separation of malware and benign classes by providing best perplexity values such as 10, 30, 70, and 100, respectively. In Figure 9, the t-SNE plot shows only two clusters for malware and benign samples, which indicates low-dimensional t-SNE data have the ability to categorize

Figure 9: t-SNE visualization and dimensional reduction using optimal perplexity values on LBP, GLCM and combine LBP + GLCM feature sets.

Table 4: Comparison of proposed O-CNN model with other reference studies.

MalwareVariants	Before t-SNE reduction				After t-SNE reduction			
	224 × 224		300 × 300		224 × 224		300 × 300	
	Correct	Incorrect	Correct	Incorrect	Correct	Incorrect	Correct	Incorrect
Adposhel	0.99	**0.01**	1.00	0.00	1.00	0.00	1.00	0.00
Allaple	0.95	**0.05**	0.94	**0.06**	1.00	0.00	1.00	0.00
Amonetize	0.97	**0.03**	0.96	**0.04**	0.98	**0.02**	0.98	**0.02**
Autorun	0.73	**0.27**	0.75	**0.25**	0.96	**0.04**	0.96	**0.04**
Browsefox	0.91	**0.09**	0.85	**0.15**	0.99	**0.01**	1.00	0.00
Dinwod	0.71	**0.29**	0.89	**0.11**	1.00	0.00	1.00	0.00
Installcore	0.99	**0.01**	0.99	**0.01**	1.00	0.00	1.00	0.00
Multiplug	0.84	**0.16**	0.84	**0.16**	1.00	0.00	1.00	0.00
Vba	1.00	0.00	1.00	0.00	0.99	**0.01**	1.00	0.00
Vilsel	1.00	0.00	1.00	0.00	1.00	0.00	1.00	0.00
Average (%)	**0.90**	**0.09**	**0.92**	**0.08**	**0.99**	**0.01**	**0.99**	**0.01**
Time (s)	**117s**		**119s**		**30 seconds (74.3x)**		**32 seconds (74.1x)**	

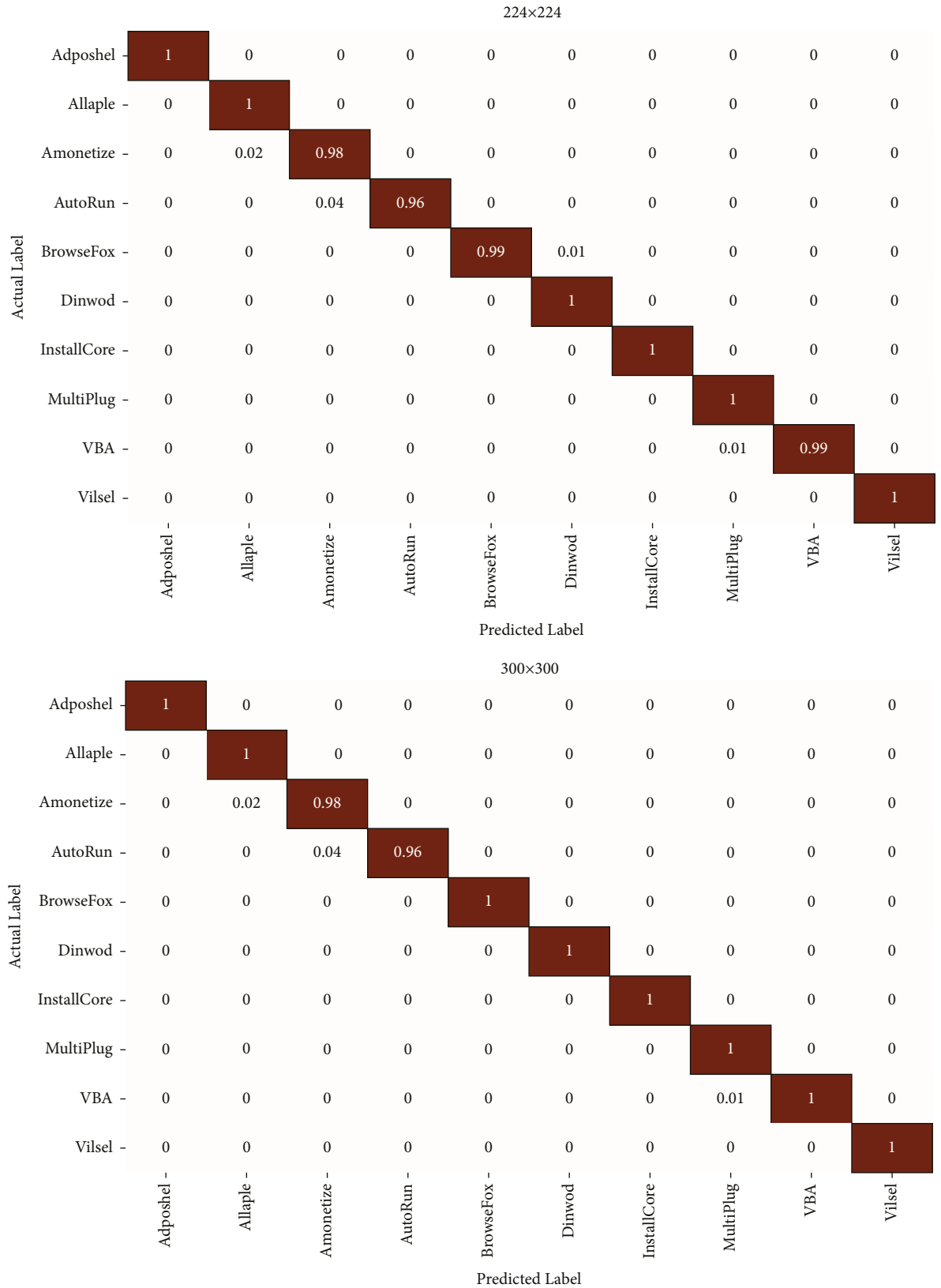


Figure 10: Confusion Matrix of proposed O-CNN model for 224×224 and 300×300-dimensional images.

samples into their respective categories. LBP feature set shows clear separation when perplexity value is 70 and 100. Comparatively, GLCM feature set shows clear separation at perplexity 30. One probable explanation is that the LBP feature set comprises of edges and small visual patches. Therefore, multiple cluster points are visible and separated from each other. Alternatively, GLCM feature set consists of visual content and textural characteristics. The combined LBP + GLCM consists of both edges and textural characteristics. All nonoverlapping clusters are clearly visible with the exception of a few outlier values. In general, t-SNE applies dimensionality reduction on data set and facilitate exploratory analysis for appropriate selection of parameters. The visual clusters formed by t-SNE are more isolated that can improve classification performance.

The performance of t-SNE dimensionality reduction on malware detection and variant classification is further evaluated for proposed O-CNN model. Table 4 presents the classification outcomes before and after using t-SNE reduction on both 224×224 and 300×300-dimensional images. Before t-SNE reduction, the average percentage of correct classifications are greater than 0.90 on both dimensional images. However, few samples from some malware variants are also misclassified. For instance, *Autorun* variant has more than 25% misclassified samples. After t-SNE reduction, the classification is improved by producing only 0.01 misclassified variants. In the case of *Autorun* variant, the misclassified samples are also reduced from 25% to 2%. Furthermore, the average detection and variant classification time is also improved by 74.3x and 74.1x on for both dimensional images. From this observation, we conclude that t-SNE dimensionality reduction not only improves the accuracy of malware variant classification but also optimizes the malware detection time which will be the major requirement in windows devices and high availability servers. Lastly, Figure 10 presents the confusion matrices of 224×224 and 300×300-dimensional images generated using proposed O-CNN model after t-SNE reduction. The figure shows that the majority of malware variant classes are effectively detected with less than 2% to 4% accuracy loss.

5. Conclusion

Malware detection is a critical security issue for Windows users who interact with the Internet on a regular basis. Because of the popularity of 5G Internet devices and the growing number of Internet users, malware attacks have become a big threat for Windows devices. This study has focused on performing memory forensics in order to detect malware attacks and their potential variants. First, we extracted local and global features using LBP and GLCM feature descriptors from textual images of memory dump files. Next, the proposed O-CNN model was fine-tuned on fused features of LBP and GLCM descriptors to detect malware and benign samples from test models. The widely studied performance indicators were selected to compare proposed methods with state-of-the-art models and related studies. The empirical evaluation showed that the proposed O-CNN model achieved above 98% accuracy on individual malware and benign samples. Furthermore, t-SNE dimensionality reduction is applied on different feature sets to visualize malware and benign samples as isolated visual clusters. t-SNE feature set achieved upto 99% accuracy on malware variant classification as well as improved the training time of 0-CNN by 74%. We believe that memory forensics store execution information of malware samples into RAM which significantly facilitate cybersecurity analyst to detect malware presence regardless of obfuscation and encryption. In the future, we planned to develop a combined blockchain and memory less malware detection model to overcome malware processing cost under limited resource capabilities.

Data Availability

The malware data set investigated during the current study is available in the *Dumpware10* repository (https://web.cs.hacettepe.edu.tr/~selman/dumpware10/).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Damodaran, F. D. Troia, C. A. Visaggio, T. H. Austin, and M. Stamp, "A comparison of static, dynamic, and hybrid analysis for malware detection," *Journal of Computer Virology and Hacking Techniques*, vol. 13, no. 1, pp. 1–12, 2017.

[2] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar, "A survey on malware detection using data mining techniques," *ACM Computing Surveys*, vol. 50, no. 3, pp. 1–40, 2018.

[3] R. Sihwail, K. Omar, K. A. Zainol Ariffin, and S. Al Afghani, "Malware detection approach based on artifacts in memory image and dynamic analysis," *Applied Sciences*, vol. 9, no. 18, p. 3680, 2019.

[4] D. Gibert, C. Mateu, and J. 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, Article ID 102526, 2020.

[5] I. Ullah, M. A. Khan, F. Khan et al., "An efficient and secure multimessage and multireceiver signcryption scheme for edge-enabled internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2688–2697, 2022.

[6] Y. Cheng, W. Fan, W. Huang, and J. An, "A shellcode detection method based on full native api sequence and support vector machine IOP Conference Series: materials Science and Engineering," *IOP Conference Series: Materials Science and Engineering*, vol. 242, no. 1, Article ID 012124, 2017.

[7] B. Alhayani, H. Jasim Mohammed, I. Zeghaiton Chaloob, and J. Saleh Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," *Materials Today Proceedings*, 2021.

[8] H. Naeem, B. Guo, F. Ullah, and M. R. Naeem, "A cross-platform malware variant classification based on image representation," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 7, pp. 3756–3777, 2019.

[9] M. A. Khan, H. Shah, S. U. Rehman et al., "Securing internet of drones with identity-based proxy signcryption," *IEEE Access*, vol. 9, pp. 89133–89142, 2021.

[10] Y. Dai, H. Li, Y. Qian, and X. Lu, "A malware classification method based on memory dump grayscale image," *Digital Investigation*, vol. 27, pp. 30–37, 2018.

[11] J. Clement, "Share of global mobile website traffic 2015-2020," *Statista: Mobile Internet Usage Worldwide*, 2020, https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/.

[12] K. S. Han, J. H. Lim, B. Kang, and E. G. Im, "Malware analysis using visualized images and entropy graphs," *International Journal of Information Security*, vol. 14, no. 1, pp. 1–14, 2015.

[13] N. Barath, D. Ouboti, and M. Temesguen, "Pattern recognition algorithms for malware classification," in *Proceedings of the 2016 IEEE Conference of Aerospace and Electronics*, pp. 338–342, Dayton, OH, USA, July 2016.

[14] B. Xiaofang, C. Li, H. Weihua, and W. Qu, "Malware variant detection using similarity search over content fingerprint," in *Proceedings of the 26th Chinese Control and Decision Conference (2014 CCDC)*, pp. 5334–5339, IEEE, Changsha, China, May 2014.

[15] A. S. Bozkir, A. O. Cankaya, and M. Aydos, "Utilization and comparision of convolutional neural networks in malware recognition," in *Proceedings of the 2019 27th Signal Processing and Communications Applications Conference (SIU)*, pp. 1–4, IEEE, Sivas, Turkey, April 2019.

[16] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware images: visualization and automatic classification," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, pp. 1–7, Pittsburgh, Pennsylvania, USA, July 2011.

[17] F. Ullah, H. Naeem, S. Jabbar et al., "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[18] J. Hemalatha, S. A. Roseline, S. Geetha, S. Kadry, and R. Damaševičius, "An efficient DenseNet-based deep learning model for malware detection," *Entropy*, vol. 23, no. 3, p. 344, 2021.

[19] R. Ronen, M. Radu, C. Feuerstein, E. Yom-Tov, and M. Ahmadi, "Microsoft malware classification challenge," 2018, https://arxiv.org/abs/1802.10135.

[20] A. Nappa, M. Z. Rafique, and J. Caballero, "The MALICIA dataset: identification and analysis of drive-by download operations," *International Journal of Information Security*, vol. 14, no. 1, pp. 15–33, 2015/02/01 2015.

[21] F. Ullah, M. R. Naeem, H. Naeem, X. Cheng, and M. Alazab, "CroLSSim: cross-language software similarity detector using hybrid approach of LSA-based AST-MDrep features and CNN-LSTM model," *International Journal of Intelligent Systems*, vol. 37, no. 9, pp. 5768–5795, 2022/09/01 2022.

[22] F. Ullah, S. Ullah, M. R. Naeem, L. Mostarda, S. Rho, and X. Cheng, "Cyber-threat detection system using a hybrid approach of transfer learning and multi-model image representation," *Sensors*, vol. 22, no. 15, p. 5883, 2022.

[23] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, "Federated learning for malware detection in IoT devices," *Computer Networks*, vol. 204, Article ID 108693, 2022.

[24] Y. Dai, H. Li, Y. Qian, R. Yang, and M. Zheng, "SMASH: a malware detection method based on multi-feature ensemble learning," *IEEE Access*, vol. 7, pp. 112588–112597, 2019.

[25] A. S. Bozkir, E. Tahillioglu, M. Aydos, and I. Kara, "Catch them alive: a malware detection approach through memory forensics, manifold learning and computer vision," *Computers & Security*, vol. 103, Article ID 102166, 2021.

[26] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971–987, 2002.

[27] R. M. Haralick, K. Shanmugam, and I. H. Dinstein, "Textural features for image classification," *IEEE Transactions on systems, man, and cybernetics*, vol. 6, pp. 610–621, 1973.

[28] L. Van der Maaten and G. Hinton, "Visualizing data using t-SNE," *Journal of Machine Learning Research*, vol. 9, no. 11, 2008.

[29] C. R. García-Alonso, L. M. Pérez-Naranjo, and J. C. Fernández-Caballero, "Multiobjective evolutionary algorithms to identify highly autocorrelated areas: the case of spatial distribution in financially compromised farms," *Annals of Operations Research*, vol. 219, no. 1, pp. 187–202, 2014.

[30] N. Pezzotti, B. P. F. Lelieveldt, L. v. d. Maaten, T. Höllt, E. Eisemann, and A. Vilanova, "Approximated and user steerable tSNE for progressive visual analytics," *IEEE Transactions on Visualization and Computer Graphics*, vol. 23, no. 7, pp. 1739–1752, 2017.

[31] J. Bouvrie, *Notes on Convolutional Neural Networks*, Cambridge, MA, USA, 2006.

[32] E. Rezende, G. Ruppert, T. Carvalho, A. Theophilo, F. Ramos, and P. de Geus, "Malicious software classification using VGG16 deep neural network's bottleneck features," *Information Technology-New Generations*, vol. 738, pp. 51–59, 2018.