Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TRANSFORMING HEALTHCARE WITH FEDERATED LEARNING: SECURING FOG SYSTEMS FOR THE NEXT GENERATION

TAYSEER ALKHDOUR[1], AITIZAZ ALI[2], MOHAMMED ALMAIAH[3,4], TING TIN TIN[5], MOHMOOD A. AL-SHAREEDA[6], ROMMEL ALALI[7],THEYAZAN ALDAHYANI[8] AND ABDALWALI LUTFI[9,10]

[1] College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2]School of IT, UNITAR International University, Malaysia.
[3] King Abdullah the II IT School, the University of Jordan, Amman 11942, Jordan
[4] Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
[5] School of Data Science, INTI International University, Nelai, Malaysia.
[6] Department of Communication engineering, Iraq University College, Basra, Iraq
[7]Associate Professor, The National Research Center for Giftedness and Creativity, King Faisal University, Saudi Arabia.
[8]Applied College in Abqaiq, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[9] College of Business, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[10] MEU Research Unit, Middle East University, Amman 541350, Jordan
Corresponding author: talkhdour@kfu.edu.sa

ABSTRACT

Recent advancements in fog computing, coupled with the Internet of Things (IoT) technology, encompass data analysis and artificial intelligence (AI) systems. Nonetheless, the inherent weakness of the current paradigm lies in its susceptibility to security risks and vulnerabilities. Security concerns and cyber-attacks remain significant challenges within fog computing environments. Collaborative attacks such as phishing assaults, along with replay attacks, exemplify common security threats. In this scenario, each layer the edge layer for sensing, the fog layer for processing, and the top layer encompassing storage and administration (cloud) - is vulnerable to attacks. The Internet of Things (IoT) in the fog (Fog-IoT) is widely acknowledged as the cornerstone of the contemporary world. Consequently, intelligent healthcare systems are increasingly prevalent. However, the rapid proliferation of IoT-based medical devices and technologies presents challenges in maintaining a comprehensive medical IoT system within budget constraints. While single Cloud Platforms (CP) would be immensely beneficial if standardized, achieving this through a decentralized fog computing system proves challenging. To address this, we propose a hybrid-deep learning protocol aimed at safeguarding electronic medical records from security breaches while simultaneously reducing latency. Additionally, we introduce scalable federated centered (FC) learning integrated with Blockchain-based data storage and retrieval. The proposed framework offers a secure, reliable, and low-latency approach to healthcare systems using a homomorphic distributed protocol.

Keyword: *EMR; IoMT; Cyber-risks; Sensors, Fog Computing; Cloud Computing; Security; Privacy.*

1. INTRODUCTION

With centralized cloud-based characteristics, handling significant data traffic in IoT (IoMT) has now become a severe problem and reason for concern [1]. As a result, patient safety and confidentiality concerns have grown while data collection, data ownership, location privacy, etc., will be at risk. By copying data and changing the identification of healthcare equipment, intruders, hackers can easily target the 5G enabled IoMT network. IoMT-Cloud currently has a single point of failure, malicious attacks, and privacy leaks [2]. To ensure network security and secure transmission, data transfer between IoMT and Cloud requires trust, device identification, and user authentication (UA) [3]. The protection of private human data is a persistent challenge. This matter has always been taken seriously in computer science. In the dynamic landscape of healthcare, the integration of cutting-edge technologies has become essential to ensure the security and efficacy of medical systems. Among these advancements, federated learning emerges as a pivotal force, particularly within fog computing environments.

This introduction delves into the transformative impact of federated learning in healthcare, highlighting its profound influence on enhancing security protocols and optimizing operations within fog systems. Healthcare is undergoing a revolution driven by the proliferation of Internet of Things (IoT) devices and the rise of fog computing. Fog systems, with their decentralized architecture and proximity to data sources, have become fundamental to modern healthcare infrastructure. However, alongside their numerous benefits come challenges, particularly regarding data security and processing efficiency.

Using federated learning, a groundbreaking approach that confronts these challenges by decentralizing the model training process. Unlike traditional methods reliant on centralized data aggregation, federated learning enables collaborative model training across multiple edge devices while preserving data privacy and security. This paradigm shift not only mitigates the risks associated with centralized data storage but also significantly reduces latency, a crucial aspect in time-sensitive healthcare applications. The synergy between federated learning and fog computing represents a significant advancement in healthcare technology. By harnessing distributed intelligence, healthcare providers can now safeguard sensitive medical data without sacrificing processing speed or efficiency. Furthermore, federated learning empowers healthcare systems to dynamically adapt to evolving patient needs, ushering in a new era of personalized and responsive medical care.

In this paper, we delve into the intricacies of federated learning within fog systems, examining its transformative potential in revolutionizing healthcare security and efficiency. Through a comprehensive analysis of its principles, applications, and real-world implementations, we aim to illuminate the growing role of federated learning in shaping the future of healthcare delivery. From enhancing cybersecurity measures to optimizing resource allocation, federated learning promises to usher in a new era of next-generation healthcare, where security, efficiency, and patient-centricity converge seamlessly. The Internet of Things (IoT) operates through layers: edge (sensing), fog (processing), and the top layer, public (storage and administration) in the cloud. Fog-IoT is pivotal today. Healthcare systems are evolving, utilizing IoT fog to overcome secure data access (SDA) and storage constraints. Medical IoT devices prioritize data security (DS) and scalability. However, rapid IoT device proliferation poses challenges in maintaining sophisticated systems on a budget. Standardizing Single Cloud Platforms (CP) would be beneficial. Decentralized fog computing integrates a hybrid-deep learning protocol, enhancing electronic medical records' security and reducing latency. Scalable federated centered (FC) learning, coupled with Blockchain-based data storage, is proposed. The architecture of the Industrial Internet of Medical Things (IoMT) is depicted in Figure 1. Research introduces an FC architecture with low overhead and latency, presenting a secure Blockchain-based Fog-BMIoMT communication mechanism.

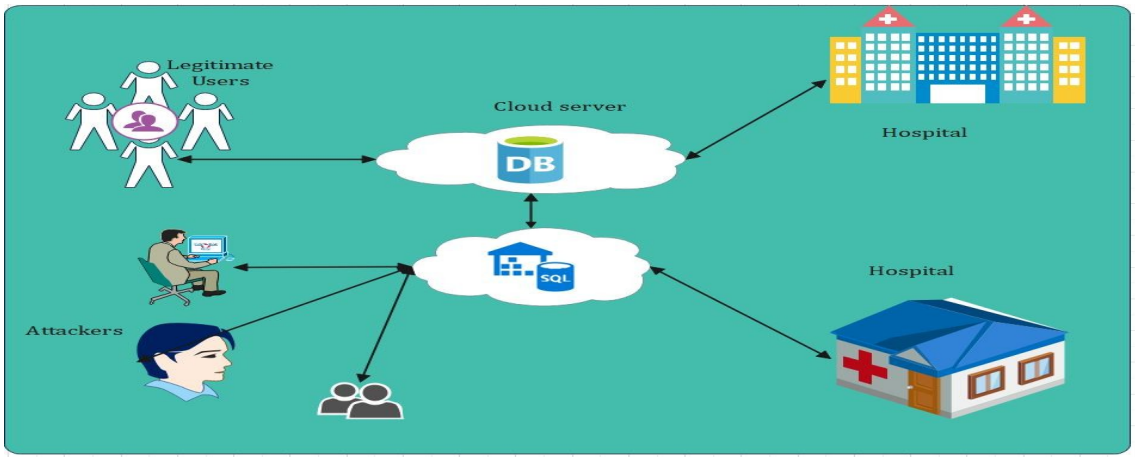

Figure 1. *Application of Fog and Cloud Environment*

2. LITERATURE REVIEW

In contemporary research, the protection of data security and privacy in IoT and healthcare systems often relies on a centralized device, leaving them vulnerable to security breaches. Notably, prevalent security threats such as DDoS, replay attacks, phishing attacks, and collusion attacks pose significant risks in such models [5]. Ensuring secure transactions between nodes is also paramount [6]. To tackle these challenges, an innovative approach has been devised: a hybrid-deep learning-based IoMT fog computing system. This system involves pre-training the model in the cloud and subsequently transferring the global model to local edge and fog computing devices. The proposed design offers enhanced security, privacy, low latency, and reduced computational and storage overhead.

The exposure of personal information, including precise user location and query content, can render individuals vulnerable to privacy attacks. Various attacks, such as localization and homogeneity attacks, can exploit this information. Consequently, reliance on Location-Based Service (LBS) providers poses serious privacy risks, as they have the capability to capture and store personal data with high spatial and temporal precision. Privacy attacks against LBS users encompass physical assault, robbery, harassment, and prediction attacks utilizing GPS-intercepted data. To mitigate these risks, it is advisable to disclose minimal information when necessary. This study investigates multiple privacy assaults on LBS users, which are further detailed in subsequent sections. Given that IoMT operates within a cloud-based environment, managing data flow has become a significant concern. Issues surrounding data collection, ownership, and location privacy threaten patient safety and confidentiality. The vulnerability of IoMT networks to attacks, such as data copying and device renaming, underscores the pressing need for enhanced security measures. Presently, weaknesses in IoMT-Security Cloud and privacy are compounded by their reliance on a single point of failure. To ensure secure data transmission between IoMT and Cloud, robust mechanisms for trust, device identity, and user authentication are indispensable. Implementation challenges include latency, network dependency, site failures, and the inability to facilitate instantaneous transactions. Fog or edge computing offers a promising avenue for addressing these challenges, facilitating time and resource-efficient services at the network periphery. Figure 1 illustrates fog IoMT models, aiding planners in expediting service delivery. The advent of 5G technology heralds a new era of connectivity, enabling the integration and control of machines such as drones in IoMT systems. However, this connectivity exacerbates existing concerns regarding data security and privacy. Safeguarding the 5G-enabled IoMT communication infrastructure against threats necessitates robust protocols, including access control, intrusion detection, and user/device authentication.

This study scrutinizes various 5G-enabled IoT communication models and their associated security threats, culminating in the implementation of secure networking solutions. Leveraging blockchain-based Fog Architecture (FA) further fortifies remote resource connectivity in the cloud. The hybrid service environment, encompassing the edge or secure IoMT layer servicing Blockchain, necessitates resilient management beyond traditional cloud computing paradigms. In summary, this study underscores the imperative of fortifying data security and privacy in IoT and healthcare systems, particularly within the burgeoning landscape of fog and 5G-enabled IoMT. By analyzing prevalent threats and proposing innovative solutions, we endeavor to pave the way for safer, more resilient medical data transfer systems in the era of interconnected healthcare ecosystems. Readers, Tactile Internet edge computing is studied by Aggarwal S. et al. The scientists are also interested. Ahad et al. [17] investigate smart healthcare possibilities enabled by 5G in the IoT. These include multi-cloud cascade architecture, low overhead native testing framework, and medical centralized data recovery [18]. Deepak et al. A smart service authentication (SSA) system can increase patient and doctor data security. The final gift came from this document will outline how LBS users' privacy is affected. In the rest of the paper: Below is sections on user privacy attacks: The adversary's portrayal is based on two main factors: prior knowledge and attack success rate. The attacker's class is discussed here. As seen in Figure 1, the adversary's representation is influenced by his previous knowledge advantage, the attacks that can be made, and their likelihood of success. The authors of [7] categorize the attacker's prior knowledge into temporal and

contextual in this dimension, two outcomes exist. First, a single user location is compromised in the initial attack. This case is famous for the extensive privacy measures employed. In the second case, the attacker gains access to multiple sites. This data can be leaked via a compromised central server or a service provider. If a central server is compromised, an attacker can obtain historical position data from several users [7]. Surrounding our own spatial and temporal information, we try to see if the enemy has any information. Indeed, an attacker may utilize this data to guess the user's whereabouts. As such, information should be protected. For example, a malicious attacker could reduce a user's darkening region by employing a road network map or a directory to determine the user's home address [8]. Most current solutions only contemplate an attacker reaching a single network point. In contrast, most LBS apps depict an enemy who has access to a set of positions and sometimes trajectories. Some LBS services keep track of all inquiries. These queries combine prior knowledge such as localization, trajectories, and location-based questions. While the adversary model's effectiveness relies on prior knowledge, the approaches and attack mechanisms' effectiveness is also contingent. The most typical attack strategies are discussed below and their applicability in our case.

3. CONTRIBUTION

In this paper, motivated by the above challenges, we design and implement a blockchain-based deep-learning framework for enhancing security and privacy in IIoT. The key contributions of this paper are as follows:

1. A new privacy-preservation and intrusion detection framework is designed by using a hyperledger fabric framework.

2. The design of a novel algorithm provides resistance to phishing and collusion attacks.

3. In the second level, a deep-learning-based privacy and security scheme is devised.

4. The performance of the proposed framework is evaluated using two publicly available IoT-based datasets, namely IoT-dataset.

4. RELATED WORKS

The Fog Computing-based IoMT is currently a hot topic. Previous research work missed important security issues like:

1. Healthcare IoMT devices send data to cloud servers that are frequently unencrypted and open to manipulation and attack. As As a result, sensitive patient information will likely be accessible.

2. To our knowledge, the need to identify IoMT medical devices, which leads to the verification and authentication of health data, is urgent. It can be accomplished quickly using a blockchain in the FC-IoMT system. Servers at the network's edge should perform more detailed authentication and verification [13].

According to a study [15] a privacy preservation model was presented by the author in [16], the author used a novel secure algorithm for privacy preservation for IoT data, but the issue related to this existing model is computational cost and more latency during the transaction. A secure surveillance system was proposed by [17]. The author explored the concept of deep convolutions neural network [18]. Aggarwal S. et al. [19] [21] [22] [23]. X. Cheng et al. [24] proposed a node security identity authentication; that provides a secure and reliable updating method for authentication keys and session keys. Ejaz, Muneeb et al. [25] work on Smart remote healthcare systems that require long working periods, low cost, network resilience, security, and confidence in highly dynamic network environments. J. Fu et al. [26] highlight the rising issues in IIoT information processing, storage, querying, and dynamic data collecting. Y. Sun et al. [27] proposed the case database and the current patient's privacy are protected whether the abstracts match or not.

A blockchain-based healthcare system survey was provided by the authors in references [28] [30] [31] [32]. The main objectives and themes of these surveys are to highlight the issues related to the current centralized system and the application of decentralized approaches such as blockchain technology. Moreover, the authors of these surveys provided a more detailed and intensive comparative analysis of the existing state of the art models. Similarly, the

security breaches associated with IoT and IoMT healthcare systems and their impact have been highlighted. Keeping all these in view, we have proposed a hybrid deep learning model using fog computing for IoMT systems to provide privacy preservation and low latency. Xu et al. [33] proposed a privacy-protection model for fine-grained access control of healthcare data based on blockchain. Rahman et al. [23] presented a secure and provenance enhanced framework for healthcare systems based on federated learning and differential privacy (DP). Blockchain and smart contracts perform trust management, edge training and authenticate the participating federated entities in this approach. Various studies have been conducted to demonstrate data privacy along with the application of intrusion detection in IoT and its applications [35], [35], [36], [37].

5. PROPOSED METHODOLOGY

Communication in the Internet of Medical Things (IoMT) realm integrates 5G, Blockchain, and Fog technologies. The role of 5G is paramount, necessitating smart antennas for IoMT communication within 5G networks (refer to Figure 2). These smart antennas leverage innovative technologies like Beam Shaping to enhance 5G coverage and capacity, particularly crucial with the increasing prevalence of mm-wave RF. The precision of Beam Shaping concentrates radiofrequency energy into pinpoint beams, vital for various applications such as vehicles and buildings. A well-aligned RF beam ensures optimal signal quality and transmission. However, challenges arise as the focal point shifts, impacting location accuracy. Intelligent healthcare systems are poised to leverage Machine-to-Machine (M2M) and IoMT capabilities within 5G networks. Yet, two primary issues emerge: the proliferation of dense terminal networks and security concerns for IoMT-based applications employing wireless sensors [9].The year 2015 marked the commencement of 5G network deployment and market research. Expectations for 5G networks include faster data rates, densification, and robust support for IoMT devices 10]. Intelligent medical applications reliant on IoMT necessitate high data throughput, scalability, low latency, dense deployment, reliability, energy efficiency, and sustained communication. Figure 3 illustrates a blockchain-based architecture for securing healthcare records within IoT devices.

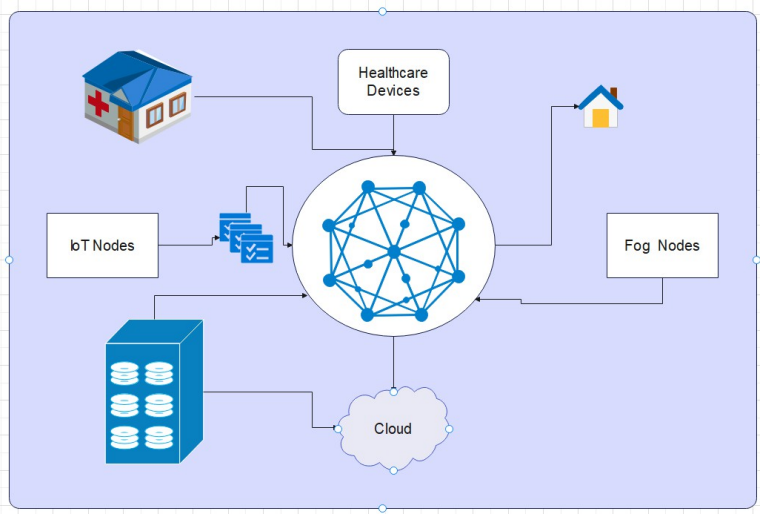

Figure 2. *Proposed Fog and Cloud Computing Environment*

5.1 Using Neural Network to Identify the Appointment Allocation Process

Our study utilized a novel hybrid deep learning strategy, combining Bidirectional Long Short-Term Memory (BLSTM) with Convolutional Neural Networks (CNN), to train the model with minimal CPU resources and low latency, while maintaining high accuracy. This innovative approach employs a predefined model that

monitors user interactions within the system, prioritizing decentralization and privacy. Each local device employs deep hybrid learning (BLSTM + CNN) to train and evaluate the model, with the BLSTM architecture incorporating both feed-forward and feed-backward modules. We utilized the IoT-ToN datasets from the UNSW Australia website, dividing the dataset into training and testing subsets. Specifically, 30% of the data was used for training, while 70% was reserved for testing and validation. Simulation results demonstrate that the proposed model outperforms benchmark models, exhibiting significantly lower latency, up to 20 ms.

To safeguard the model's privacy, lightweight and homomorphic encryption techniques were applied. Homomorphic encryption allows for additive and multiplicative operations on encrypted data, ensuring secure computation. The proposed framework is applicable to various healthcare systems across domains. Moving forward, our future efforts involve integrating a Particle Swarm Optimization (PSO) algorithm into a federated learning system, aimed at improving the effectiveness of the current framework. During this phase, we elaborate on the novelty of our proposed smart contracts and the methodology for distributing appointments to users based on neural network predictions. The appointment selection process for users involves the following steps:

1. **Step 1:** Generate a block file for recording the current block contents when stored in the block file, and it is named based on the blocks' hash value.

2. **Step 2:** Choose a single participant of the transaction and identify its user transaction identifier from the B+-Tree index with the user's name derived from the user collection.

3. **Step 3:** Identify the key from the user block file based on the user transaction identifier of the participating users. If the user transaction identifier exists, then the value is extended. Further, the block's name is written at the end of the value to sort them based on the order of timestamp. On the other hand, if it does not exists, then key-value metadata is appended. Finally, the key is the user transaction identifier, file name, and updated B+-tree index.

4. **Step 4:** Until the complete set of users complete their processing and operate extension, repeat steps 2 and 3 for processing the successive transaction user.

6. PROPOSED ALGORITHM

We have proposed a novel algorithm for our proposed fog computing system to secure the EMR for a smart healthcare system. Each algorithm plays an important role in our proposed framework. The function of each algorithm is explained by pseudo-code. For example, algorithm 1 is based on EMR encryption and uses the SHA256 encryption method to encrypt the data. SHA256 is supported by fog based Blockchain system for healthcare. Algorithm 2 is based on Homomorphic encryption (HE). We have implemented HE encryption techniques which provides the facilities to do any type of operation on an encrypted data without decryption it. The details and working of algorithm 2 is mentioned as below.

Algorithm 1 Algorithm EMR encryption

1: Enhance Manifold Analy Eval of both the IoMT end
2: Set IoMT device for comm
3: Get acquisition, ω, $electronicmedicalrecords(EMR)ExtractEMR\ f\ romBC$
4: EMR, valid SHA256 checkHash if EMR, valid $\leq T$,
5 : $thenGettheLusingConnectlength(CL)$
6: Generate(CL)
7: IF Blockchain trans $\leq addAnalysis(i, \omega)delLocalEMRendi\ f\ (EMR)$
8: end
9: end

Algorithm 1 is called the client registration algorithm. The proposed algorithm provides a facility for the user to register the client. We have proposed novel algorithms for our proposed deep learning-based healthcare system using Blockchain technology. Figure 2 represent our proposed cloud-based fog computing environment and its working through illustrations. Each algorithm is explained through pseudo-code. HE is the encryption technique that provides operation on the encrypted script without decryption. It provides anonymity and security to the Electronic health records (EHR) Algorithm 2 represents the Homomorphic encryption (HE), and the working of HE algorithm has explained below.

Algorithm 2 Algorithm Homomorphic Encryption

1: Init an arr T_{Set} of size B
2: Each val is an arr of S rec of type rec
3: Init an arr free of size B whose value are int
4: Init all set to 1... S
5: Choose a rand k K_T of (PRF) F
6: Let W be the set of keyw in D_B
7: For every w belongs to W do
8: Set $s_{tag} \leftarrow F(K_T, w)$ and $t \leftarrow T[w]$
9: For each $i = 1$
10: Set s_i as the i-th string in t
11: Set $(b, L, K) \leftarrow H(F(s_{tag}, i)$
12: If empty array b is an empty set
13: restart $T_{Set_{Setup}}(T)$ with fresh key K_T
14: Choose j belongs to r free array b and remove j from set free array b
15: Set bit β as 1 if i less than $|t|$ and 0 if i equal $|t|$
16: Set $T_{Set}[b, j]$ label appr L
17: $T_{Set}[b, j]$ label $\leftarrow (\beta\ s_i)$
18: Output (T_{Set}, K_T)
19: Output $s_{tag} \leftarrow F(K_T, w)$
20: 1 Init - t as an empty list, bit β as 1, and counter i as 1
21: 2 - Rept the following loop while $\beta = 1$
22: Set $((b, L, K) \leftarrow H(F(s_{tag}, i))$
23: Retrieve an array $B \leftarrow T_{Set}[b]$
24: Search for index j belongs to 1... S s.t. $B[j]$ lable = L
25: Let $v \leftarrow B[j]$ value K
26: Let β be the first bit of v and s the remaining $n\ \omega$ bits of v
27: Add str s to the list t and increment i
28: Output t
29: End procd

6.1 Hmomorphic Encryption

The majority of currently available encryption techniques prevent operating on data until it has been decoded. On the other hand, decrypting the data is a violation of privacy regulations. Furthermore, once someone has encrypted the data, it must first be decrypted before processing, making it subject to unwanted access and manipulation. HE eliminates the requirement for data to be decrypted before being used. In other words, the integrity and privacy of the data are preserved while the data is being processed. In cryptography, HE is a mechanism that allows data-loss prevention (DL) procedures to execute over encrypted data without losing its context. It eliminates the need for a trade-off between data usefulness and data privacy, and it assures that data stays secure even when in an untrustworthy setting. In the case of DL, the algorithm can be

taught and tested on data that has been securely encrypted. If the DL method achieves a high level of prediction accuracy, it can be implemented. In real-world situations, it will be able to provide a decision on the encrypted information. The data obtained can be decrypted by the user with the help of a secret key that is unique to him. As a result, the confidentiality and security of the data are preserved. A general classification of homomorphic encryption algorithms can be separated into three subcategories: Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SWHE), and Fully Homomorphic Encryption (FHE). FIGURE 3 depicts the classification of homomorphic encryption and its organizational structure. PHE only allows for a single type of mathematical operation on the encrypted information.

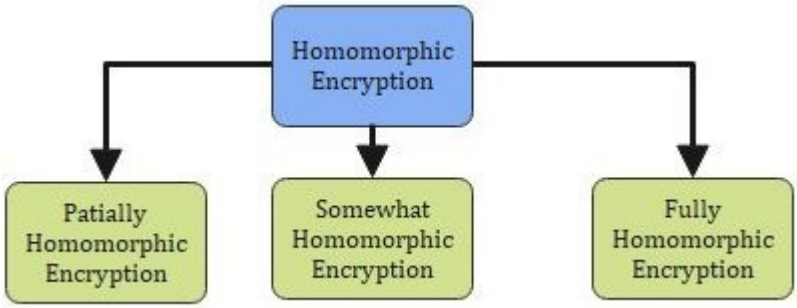

Figure 3. Classification Of Homomorphic Encryption

PHE schemes are, in general, more efficient than SHE and FHE, mainly because they are homomorphic about only one type of operation (addition or multiplication). SHE is more prevalent than PHE since it supports more operations; however, it can perform them on only a limited range. The main drawback of FHE is its slow computation speed. The whole of the proposed methodology is being described in two subsections, i.e., 5G-enabled IoMT communication, and Blockchain and Fog-based architecture for IoMT communication. SHE enables all addition and multiplication operations with only a limited range on the encrypted data. On the other hand, FHE enables various assessment operations on encrypted data with an unbounded range. Figure 4 represents the proposed fog computing architectures and their working. The devices at each layer and their working is illustrated in Figure4.

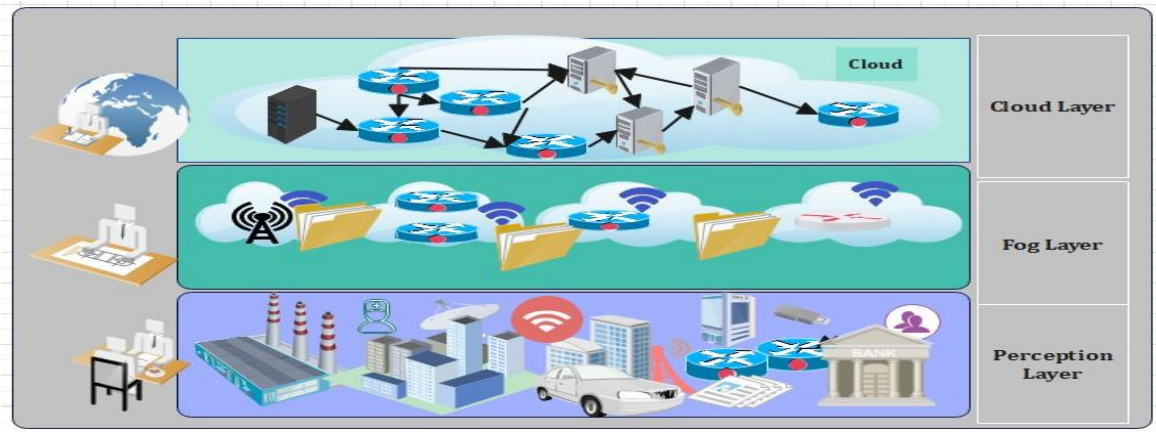

Figure 4. Proposed Fog And Cloud System Architecture And Its Function Using Biosensors And Iot Devices.

6.2 Privacy-Preserving Deep Learning

In training and testing deep learning models, data privacy is a critical consideration, particularly when sensitive data (such as health records, financial details, location logs and satellite photos) is being used for training and inferring. Therefore, numerous PPDL strategies were

developed to allow multiple input sources to train and evaluate DL models without disclosing their private information in their original form. There are three categories of techniques that can be classified as follows: cryptography, perturbation, secure enclaves, and hybrid in its most basic form.

technologies. To train and test deep learning systems on encrypted data, cryptographic methods are employed. F represents the implementation of a privacy-preserving technology.

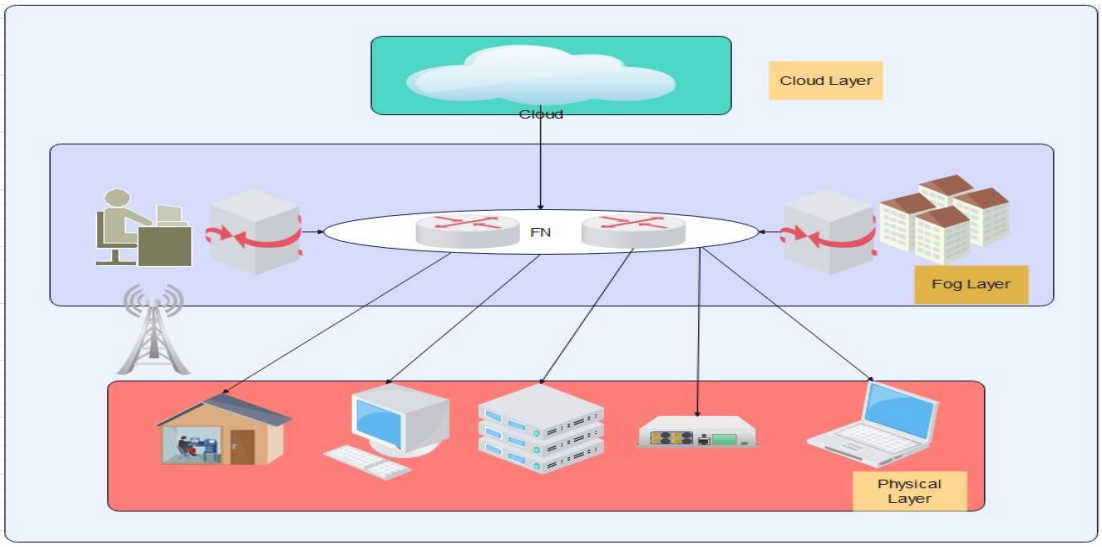

Figure 5. Proposed Fog and Cloud Computing Environment

Homomorphic Encryption (HE), Secret Sharing (SS), Secure Multi-Party Computation (SMPC), and Garbled Circuit are examples of approaches in this category (GC). Using perturbation methods, it is possible to modify data values while maintaining individual record confidentiality [13]. Differential Privacy (DP) and Dimensionality Reduction (DR) are two approaches that fall under this category (DP). Techniques that use secure enclaves send both the prediction model and the data to a trusted, secure enclave environment for execution, rather than sending both together as they would in a traditional approach. For their part, hybrid methods attempt to improve data privacy by mixing multiple PPDL techniques in a single operation. This one is among the results of a recent survey on privacy-preserving deep learning algorithms. Nonetheless, many of these systems are inefficient when dealing with complex data and are only effective when dealing with simple classification problems, such as MNIST or CIFAR-10. Furthermore, they frequently incur a significant amount of computational and transmission overhead. Furthermore, due to estimated activation functions, there is always a trade-off between privacy and model accuracy, which must be considered.

$$SVF = \pi(CS1) = EXP1P\pi = 1TR\tau \int CS1 \longrightarrow AT1 \Rightarrow C1 \quad (1)$$

6.3 Blockchain and Fog Based Architecture for IoMT

The Internet of Medical Things (IoMT) and fog nodes (FN) are linked together by a blockchain and fog network (IoMT-Fog). By combining high performance and low latency, distributed technology may provide on-demand services (LL). It will raise the bar for monitoring people's health to a higher level. Faster data processing is made possible by the FC paradigm, which assists IoMT elements with low latency (LL). The proposed IoMT-Fog, as depicted in Figure 4, maybe a more appropriate medical equipment (ME) option in some situations.

To show Figure 4, the intended architecture is composed of several layers. By processing IoMT data on fog nodes (FN), the initial layer (IL) of FN minimizes latency. This also enables the user to realize his desire for quick service. In future, IoMT devices, a multi-layered design, as depicted in Figure 2, have been proposed for applications involving large amounts of data. The devices connected and FN are shown in the first layer of this design. Figure 6 represents the transaction flow through our proposed model based on Fog computing and a secure encrypted database using HE encryption techniques. Connected devices communicate with one another, and Blockchain technology provides security. The second level of FN's latency is reduced because of IoMT device communication. As a result, users' requirements are encountered. The proposed fog Computing (FC) model determines the usage of FC at the network edge of IoMT devices and blockchain technology to connect, transfer, and exchange data amongst IoMT nodes.

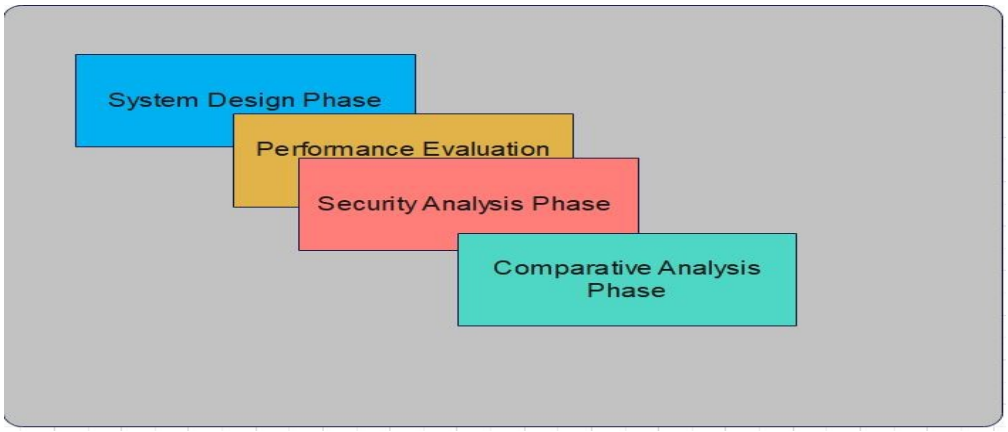

Figure 6. Simulation results based on the displacement and Biosensors output

A peer-to-peer (P2P) transmission network topology is used in the proposed system. In the network, miners are a type of IoMT-NODE. They are utilized in the network to validate transactions. When transactions are confirmed, they are converted into blockages, added to an existing blockchain, and broadcast to the network. Miners are essential for a newly generated block's network adjustment. In this investigation, we tested it and found it to be adequate. We analyzed and used simulation coda tools. Coda is a blockchain development tool. The docker composite was installed on the system. The codecov Test Coverage Tool is a network coverage evaluation tool for IoMT devices. R3 Corda is a distributed Hyperledger platform with work-proof methods (PoWs) and a peer-to-peer network. Extraordinary blockchains are built using the R3 Corda technology. Registration for IoMT nodes procedure to request transactions, which are carried out as follows in Algorithm 3.

The proposed algorithm 4 main function is initialization. In the initialization algorithm, the keywords are initialized, and a secret key is assigned to the participant—the participant search for the keyword using the physical layer of the proposed system. So the user doesn't need to decrypt each keyword encrypted by HE encryption techniques. Through the initialization algorithm, the participant's search doesn't reveal the participant's identity due to HE methods. Hence, our proposed algorithm keeps the participants' identities secret, such as Doctors, patients, nurses, and lab clinicians.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Algorithm 3 Client Registration Algorithm

1: Step 1: The client's request for registeration
2: Step 2: A key and User ID is assigned.
3: Step 3: Check if the client exists.
4: Step 4: If the val $\leq$ 1 *then*==1
5: Step 5: The transac has been rej.
6: Step 6: Return to the prev state.
7: Step 7: if not, then
8: Step 8: If user exist, then
9: Step 9: The tran has been completed.
10: Step 10: Cli is authorized then allow Fn.
11: Step 11: Else
12: Step 12: Set up the cli data.
13: Step 13: Connect the data to the send addr.
14: Step 14: Add to the client list.
15: Step 15: th and END
16: Step 16th and END

Algorithm 4 Initialization Algorithm

1: Initialize $T \leftarrow\!- \phi$ indexed by keywords W
2: Select key K_S for P_{RF} F
3: Select keys K_X, K_I, K_Z for P_{RF} F_p with range
4: Z p and parse D_B as $(id_i, W_i\ d_i)d_i = 1$
5: Initialize $t \leftarrow\!-$ ...; and let $K_e \leftarrow\!-$ $F(K_S, w)$
6: for id belongs to $D_B(w)d_o$
7: Set a counter $c \leftarrow\!-$ 1
8: Compute $x_{id} \leftarrow\!-$ $F_p(K_I, i_d)$, $z \leftarrow\!-$ $F_p(K_Z, w||\ c)$
9: y $x_{idz} \leftarrow\!- 1\ e$ $- E_{nc}(K_e, i_d)$
10: Set $x_{tag} \leftarrow\!-$ $g\ F_p(K_X, w)x_{id}$ and $X_{Set} \leftarrow\!-$ X_{Set} union x_{tag}
11: Append (y, e) to t and $c \leftarrow\!-$ $c + 1$
12: end for
13: $T[w] \leftarrow\!-$ t
14: end for
15: Set $(T_{Set}, K_T) \leftarrow\!-$ T_{Set} Setup(T)
16: Let $E_{DB} = (T_{Set}, X_{Set})$
17: return E_{DB}, $K = (K_S, K_X, K_I, K_Z, K_T)$
18: Token generation $(q(w), K)$
19: Client's input is K and query $q(w = (w_1, \ldots\ldots, w_n))$
20: Computes stag T_{Set} Get $Tag(K_T, w_1)$
21: Client sends s_{tag} to the server
22: for $c = 1, 2, \ldots\ldots$until the server stops do
23: for $i = 2, \ldots, n$ do
24: $x_{token}[c, i] \leftarrow\!-$ $g\ F_p(K_Z, w1||\ c)F_p(K_X, w_i)$
25: end for

26: $x_{token}[c] \leftarrow (x_{token}[c, 2], .., x_{token}[c, n])$
27: end for
28: $T_{okq} \leftarrow (s_{tag}, x_{token})$
29: return T_{okq}
30: Searching technique

31: $E_{Res} \leftarrow ...$
32: : $t \leftarrow T_{Set_{(Retrieve)}}(T_{Set}, s_{tag})$
33: End

Algorithm 5 represents the main function is to create and access transactions. The transaction is securely transferred, and only authenticated users can access the EMR. The working of algorithm 5 is explained below.

Algorithm 5 Algorithm Transaction Creation and Access

1: Init an array T_{Set} of size B
2: Every integer S records of type record

3: Init an array of size B whose elements are integer sets

4: Init all set to 1, ..., S

5: Choose a ran key K_T of (PRF) F 6: Let W be the set of keywrd in D_B 7: For every w belongs to W do
8: Set $s_{tag} \leftarrow F(K_T, w)$ and $t \leftarrow T[w]$
9: For each $i = 1$
10: Set s_i as the i-th string in t
11: Set $(b, L, K) \leftarrow H(F(s_{tag}, i)$
12: If free array b is an empty set

13: restart $T_{Set_{Setup}}(T)$ with fresh key K_T
14: Select j belongs to r free array b and remove j from set free array b

15: Set bit β as 1 if i less than $|t|$ and 0 if i equal $|t|$
16: Set $T_{Set}[b, j]$ label approaches L
17: $T_{Set}[b, j]$ label $\leftarrow (\beta | s_i)$
18: Output (T_{Set}, K_T)
19: Output $s_{tag} \leftarrow F(K_T, w)$
20: 1 - Initialize t as an empty list, bit β as 1, and counter i as 1

21: 2 - Repeat the following loop while $\beta = 1$

22: Set $((b, L, K) \leftarrow H(F(s_{tag}, i))$
23: Retrieve an array $B \leftarrow T_{Set}[b]$
24: Search for index j belongs to 1... S s.t. $B[j]$ lable = L

25: Let $v \leftarrow B[j]$ value K
26: Let β be the first bit of v and s the remaining $n\,\omega$ bits of v
27: Add string s to the list t and increment i

28: Output t
29: End procedure

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6.4 Mathematical Modeling

This section carried out mathematical modelling to prove my proposed model encryption and decryption process. Moreover, we have also carried out mathematical modelling for the number of rounds.

$$y2 \bmod q = (x3 + ax + b) \bmod, q, \quad (2)$$

where a, b, x, and y belong to q and 4 = (4 a 3 + 27 b 2) mod q 6 = 0. If a point P(x,y) satisfies the 15. and Eq (a, b), then the point P(x, y) is a point on an elliptic curve, and the point Q(x, y) is the negative point of P(x, y) i.e. P=Q. Let points P(x1, y1) and Q(x2, y2) be points on the elliptic curves Eq (a, b) and P 6 =Q, the line 'l' passes through the points P and Q, and intersects the elliptic curve at the point R0 = (x3, y), the points of R0 symmetrical about the x-axis are R=(x3, y3) and R=P+Q. The points on the elliptic curve Eq (a, b) and the infinite point O together form an additive cyclic group of prime order q as

Gq = (x, y) : a, b, x, y belong to Fq, (x, y) belong to Fq, (a, b). (3)

kP = P + P + ... + P(k belong to Zq), (4)

Where k is ... and Zq is ... .

((ui + vi) ∗ G), if i = S, (5)

where ui is the distance from one node to another node in the network graph, vi is the vertex, G is graph, and S is signature

(ui G + (vi + wi)) ∗ p ki, if i =!S, (6)

Ri = ∑(ui + wi) ∗ H0(p ∗ ki), if i = s, (7)

RI = ∑ ui ∗ H0(p ∗ ki) + (vi + wi) ∗ Is if i = s, (8)

where RI is real number and Is is integer value .

h = H2(m||r), (9)

where h is ..., H2 is ..., m is ..., and r is ... .

$i = \sum_{i=1} H1(h, L1, ..., Ln, R1, ..., Rn) \sum s$, (10)

where Ci is ..., H1 is ..., h is ..., L1 is ..., Ln is ..., R1 is ..., Rn is ..., and n is ... .

Di t = ∑(ui + vi)ci ∗ s ki, (11)

Di t = ∑ ui if i = s. (12)

Yi = di ∗ G + ci ∗ p ki, (13)

where Yi is ... and di is ... .

i = di ∗ H0(p ki) + ci ∗ Is. (14)

where Ki's are ... .

where δi's are ... .

$\sum_{ß=1}^{n} = H1(h, Y1, Y2, ..., Yn, K1, K2, ..., Kn)$, (15)

$\sum_{i=1}^{n} = H1(h, Y1, Y2, ..., Yn, \delta1, \delta,..., \delta n)$, (16)

Yi = di ∗ G + ci ∗ p ki = ui ∗ G + (vi + wi) ∗ p ki = Li (17)

Zi = di ∗ H0(p ki) + ci ∗ Is = ui ∗ H0(p ki) + (vi + wi) ∗ Is = Ri, (18)

where Zi is ... and di is ... .

When i = s, the conversions of (Ki) and (Zi) are expressed as

$Ki = di * G + ci * p\,ki,$ (19)

$Zi = [(ui + vi) - ci * s\,ki] * G + ci * p\,ki,$ (20) respectively.

$= ui * G + vi * G,$ (21)

$\delta i = di * H0(p\,ki) + ci * Is.$ (22)

$= [(ui + vi) - ci * s\,ki] * H0(p\,ki) + ci * s\,ks * H0(p\,ks).$ (23)

$= ui * H0(p\,ki) + vi * H0(p\,ki).$ (24)

Therefore, according to the above relationship, the correctness of the Homomorphic encryption proposed in this paper is verified as

$= H1(h, Y1, Y2, ..., Ys, ..., Yn, \delta1, \delta2, ..., \delta s, ..., \delta n),$ (25)

$= H1(h, L1, L2, ..., Ls, ..., Ln, R1, R2, ..., Rs, ..., Rn),$ (26)

where CS is ... Cipher-text!!. n

$CS = \sum, i=1$ where Ci's is ...n (27)

$= \sum Ci,$ where Ci's is ... n. (28)

Figure 7 represents the diagram and layout of our proposed neural network system based on a neural network and hybrid system. The complexity of our proposed hybrid neural network system can be identified from the number of hidden layers. The more the hidden layers, the more will be the complex system.

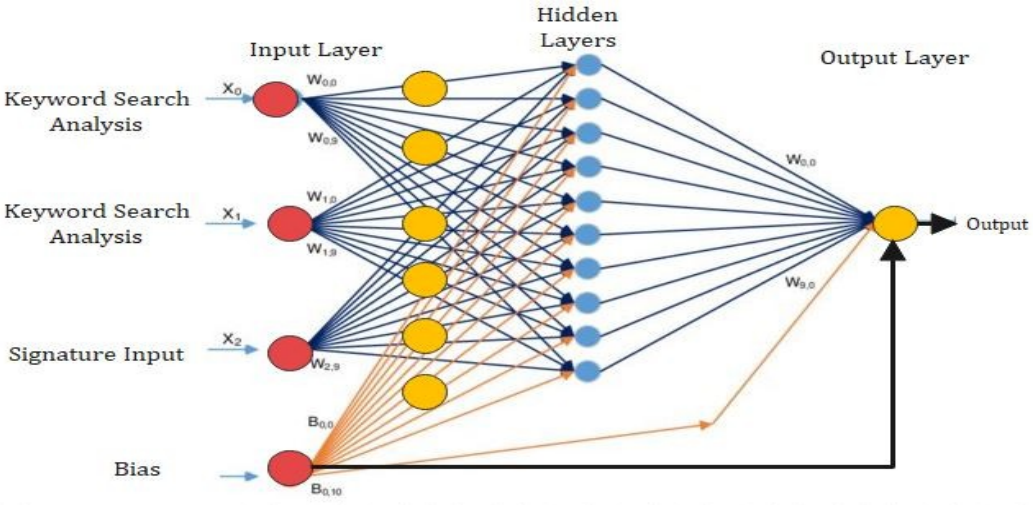

Figure 7. Proposed deep learning and hybrid neural network system for Blockchain based Fog computing

6.5 Secure Training

When doing the secure training phase, it is required to run the DL algorithm on the encrypted dataset to achieve good performance on class recognition. Specifically, we will compare and contrast the performance of multiple deep learning algorithms when applied to Paillier-encrypted photographs for the objectives of this research. One of the most difficult problems to solve in this situation is to find an appropriate balance between how accurate the DL algorithm is in identifying classes and the behaviours of intruders. To

evaluate the first point, it will be good to compare how well the selected DL algorithms work on both plain and encrypted data. When only a tiny difference in accuracy exists between the DL algorithm on basic data and the DL technique on encrypted data, we can infer that the DL algorithm performs well and can be applied in real-world settings. If not, the encryption approach employed for the proposed model is insufficient, as it precludes the deep learning algorithm (DL) from learning from encrypted images. In this study, we used MobileNetV2, a CNN made of three layers that we created ourselves and used in this study. In its place, any transfer learning approach, including the MobileNetV2 algorithm, can be employed, including the one described above.

6.6 Security Testing and Validation

The certification of security measures is an essential component of constructing successful defense mechanisms. A freshly created countermeasure's ability to alleviate or at the very least attenuate security threats can be determined by designers using this technique. The application scenario, the adversaries' capabilities, and the additional protection that may be achieved compared to existing solutions must all be carefully considered. The analysis for each of the applications above situations is provided in the following subsection.

7. ANALYSIS AND RESULTS

The Hyperledger Fabric tool and Ethereum remix IDE were utilized for blockchain design and transaction for our trial evaluation on the Linux platform, and the results were quite positive. We made use of the MatLab library to do statistical data analysis. The advantage of adopting the Matlab lib package was that it allowed for the importation of pandas, which can be used for data analysis and modification. To plot the graphs for evaluation, we employed the Python programming language. The Wireshark tool was used to record network data, then stored in a pcap format. It contains TCP files, the transfer and receiving timings, and the source and destination ports. The calliper tool for transaction and blockchain analysis provides the most accurate picture. In the evaluation phase, transaction rates, throughputs, latency, the number of peers, and CPU and storage utilization are all measured and analyzed. It was necessary to use the Matlab lib package to display multiple points of view graphically throughout the evaluation process. To assess the overall performance of our PHR system, we have carried out and evaluated each experiment. In the insights and discussion section, the performance of our framework is compared to the performance of the benchmark framework. In this proposed research, several use cases are carried out to validate our simulation. We separated each use case into four groups: one organization - one peer, two organizations - one peer, three organizations - one peer, two organizations - two peers, three organizations - two peers, two organizations - two peers, two organizations - two peers, and three organizations - two peers. Furthermore, we put the suggested framework through its paces by conducting a cross-domain analysis on the proposed global domain. Each organization has several ledger peers in the network, each responsible for transporting a copy of the ledger. A single ordere host will be in charge of producing blocks, while the Caliper host will be in the order of executing the workloads. In this way, every host is a component of the star topology and performs the measurements and evaluations.

We have used the IoT dataset for our experimental work and simulations publicly available on the UNSW website. Furthermore, we have divided the dataset into two categories: training and testing. Moreover, the training dataset we used was 30% data, whereas, for the testing purpose, we used 70% data. The proposed hybrid deep learning consists of two-layer including hidden nodes 50, 25 were used during training. Moreover, we pre-trained the model and then distributed the trained model in a distributed way on blockchain to predict and detect the attacks and the behaviour of the users. The proposed model is configured with optimizer= N adam, epochs=20, batch size= 50. The result parameters concerning accuracy (acc) and loss shows that the proposed approach has efficiently learned from both datasets. The proposed model has achieved about 94.34% acc and 8.89 loss using the IoT dataset, while with IoT-Botnet model obtains 88.38% acc and 8.92% loss. Further, the effectiveness of the proposed two-level privacy architecture is evaluated as a utility system based on BiLSTM model. The hyperparameters are configured by an input layer fed from both datasets, 5 hidden layers, with hidden nodes= 200, 100, 50, 25, 15, respectively. The results are obtained before and after

applying the two-level privacy-preservation technique. The BiLSTM model with transformed ToN-IoT dataset has achieved 0.0167 loss and 99.58 acc, while 0.0052 loss and 99.89 acc with the actual dataset. Similarly, with transformed IoT-Botnet dataset model has obtained 5.5116 loss and 90.86 acc, while 0.0685 loss and 99.98 acc with the real dataset. We also evaluate the proposed BiLSTM model regarding class wise prediction 0% results, i.e., PR, DR, F1 and FAR metrics. In Table IV, we see that the model with the actual and transformed ToN-IoT dataset has achieved an average of 90%-100% values for PR, DR and F1 scores and has reduced FAR close to 0%. Similarly, for various types of attacks such as DoS, DDoS, Reconnaissance, and Normal group of actual IoT-Botnet dataset, the model has achieved an average of 99%-100% values for PR, DR, F1 metrics.

8. DISCUSSION

This section briefly explains the experimental analysis of our proposed work in a wider context. It also elucidates the dataset used, experimental setup, and comparative analysis. Referring to an IIoT environment, multiple security issues can be raised from the above-discussed risks. For example, industrial devices such as PLCs RTUs send and receive IO signals back and forth with field's sensors and actuators. Therefore, this data should only be transmitted between local sources and destinations. Moreover, this data is considered critically confidential as it can show the functionality and the logic of control processes. With this permission less solution, all the devices in this network will have access to the full transaction history. Any compromise in any of these devices will expose this information. If it gets into the wrong hands, it can allow malicious actors to reverse engineer these machines and possibly find ways to attack them and potentially disrupt their critical operations. Therefore, it's hard to justify using Consortium Blockchain and other technologies in cold and vital environments such as IIoT. Figure 8 illustrates the proposed model's simulations results, which justify that our proposed framework is more efficient regarding cache hit rate and execution time.

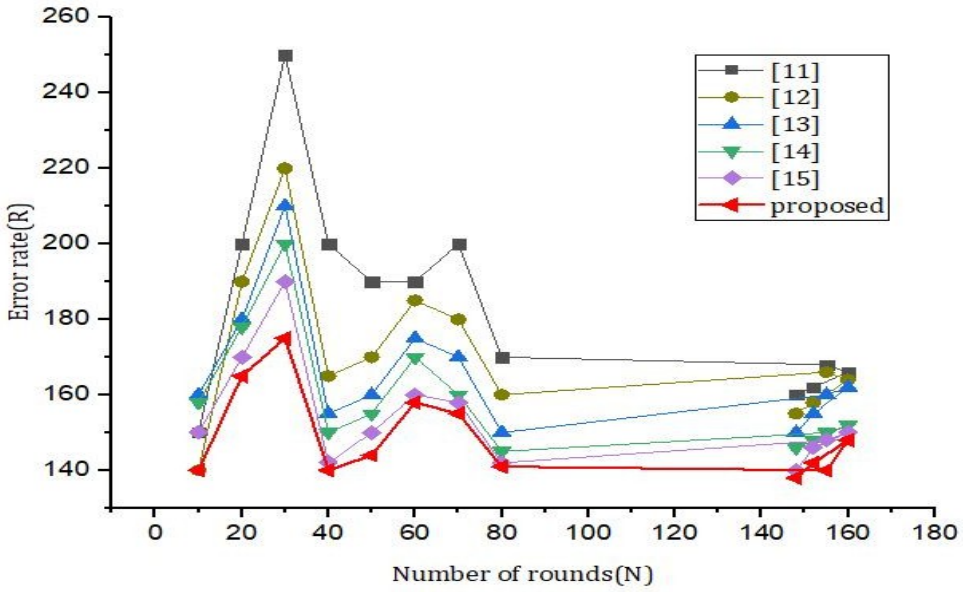

Figure 8. Simulations Results Using DL Techniques And Comparative Analysis With The Benchmark Models

In Figure 9, we have carried out the simulations results based on the number of rounds and error rate. From Figure 9, it is very clear that our proposed framework's error rate is very low compared to the benchmark model; hence, it shows that our proposed approach is more secure and efficient. Figure 9 represent the simulations results based on execution time and cache hit

rate. Figure 9 represent that our proposed framework is better than the benchmark model.

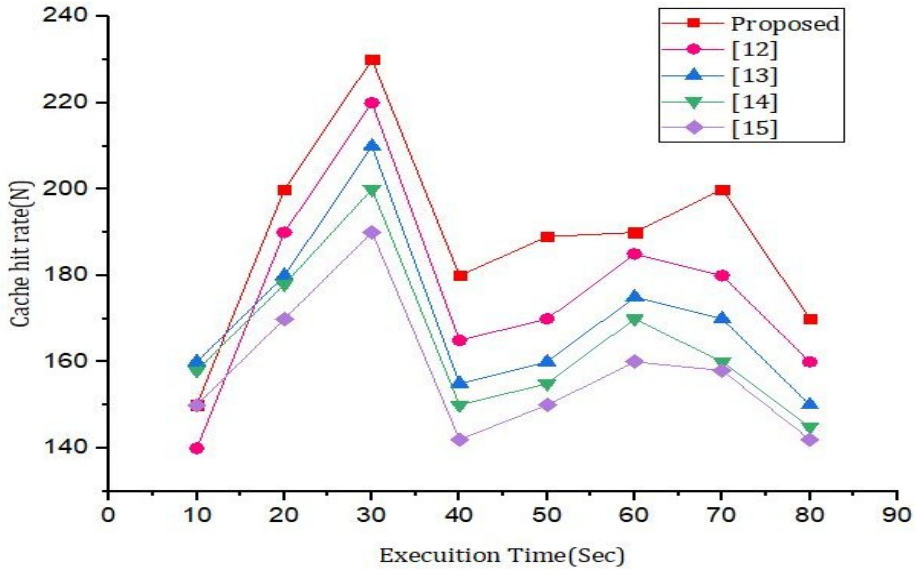

Figure 9. Simulations Results Based On The Number Of Rounds And Error Rate

Figure 10 has carried out simulations based on attributes and error rate. From the simulations in Figure 10, it is very clear that our proposed framework has a much less error rate than the benchmark model. This is because the proposed model trains with time and learns from the user behaviour and interaction using deep learning techniques; as our proposed model knows, the error rate becomes low compared to the benchmark models. Therefore, it justifies that our proposed model is more secure and accurate than the previous models.

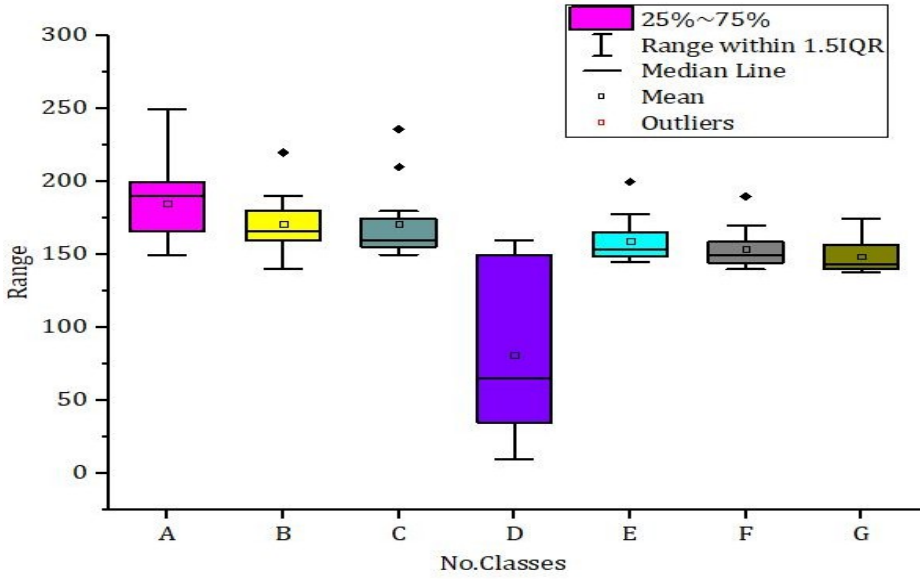

Figure 10. Simulations Based On Attributes And Error Rate

Figure 11 is shown the simulations results based on the search time and cache size. In Figure11 x-axis represent the search time, and the y-axis represents the cache size. We have implemented our proposed algorithm to use less cache size with maximum search time.

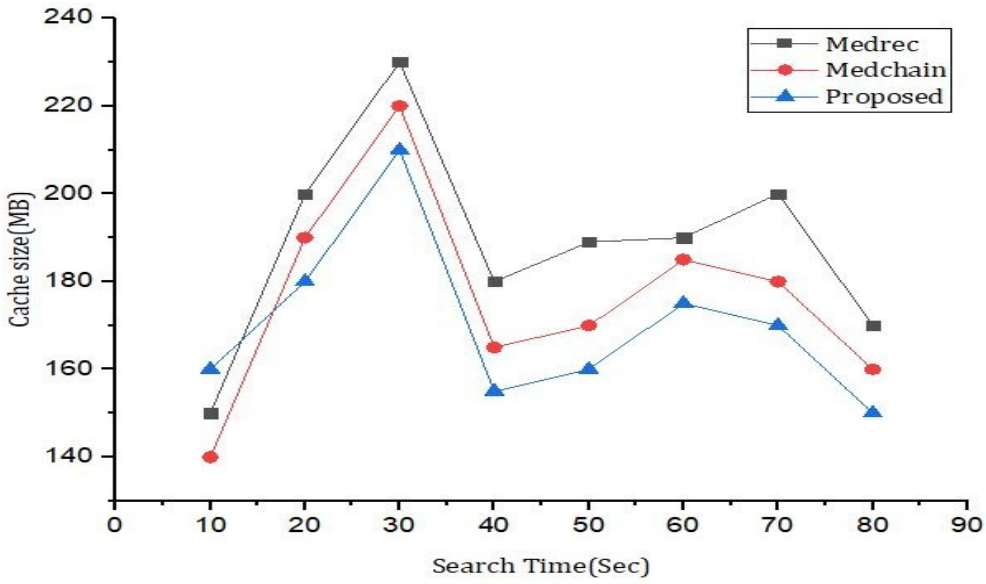

Figure 11. Simulations Results Based On The Search Time And Cache Size

Figure12 represent the simulations results based on False-negative and true positive. Figure15 also illustrates that our proposed model receives more accuracy than the benchmark model. From the simulations results, the proposed model gets the accuracy up to 97%.

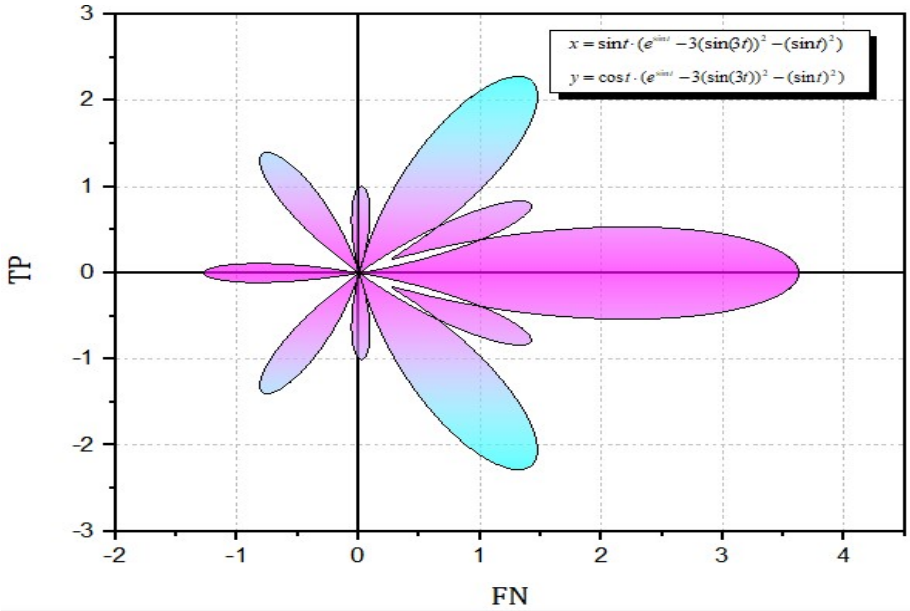

Figure 12. Simulation Results Based On True False And False Negative Values In Order To Validate The Accuracy

9. CONCLUSIOSN

This paper has devised a novel hybrid deep learning model for securing IoMT data using fog computing. The issues related to real-time environments such as IoMT and Fog computing environments are highlighted, and an efficient solution is devised. The privacy issues in other blockchain and cloud-based models were explored, and a lightweight protocol was developed. We have improved the latency of the existing benchmark models and the accuracy. With the integration of a hybrid-deep learning protocol, the proposed model trains the model at each fog node and uses the local data of each model to protect it from security breaches. The proposed model was deployed against the threat model to spoof against collusion, replay, and DDoS attacks. The proposed model is an application in a cross-domain framework where exist multiple healthcare systems located in different geographic locations.

ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Research No. Grant No. 6084).

RFERENCES

[1] Ayatollahi, H., & Shagerdi, G. (2017). Information Security Risk Assessment in Hospitals. The Open Medical Informatics Journal, 11(1), 37–43. https://doi.org/10.2174/1874431101711010037

[2] Chen, Q., Lambright, J., & Abdelwahed, S. (2016). Towards Autonomic Security Management of Healthcare Information Systems. Proceedings - 2016 IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2016, 113–118. https://doi.org/10.1109/CHASE.2016.58

[3] Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors, 22(2), 572.

[4] Almaiah, M. A., & Al-Khasawneh, A. (2020). Investigating the main determinants of mobile cloud computing adoption in university campus. Education and Information Technologies, 25(4), 3087-3107.

[5] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 international conference on information technology (ICIT) (pp. 779-786). IEEE.

[6] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. Sensors, 22(4), 1448.

[7] Adil, M., Khan, R., Ali, J., Roh, B. H., Ta, Q. T. H., & Almaiah, M. A. (2020). An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. IEEE Access, 8, 163209-163224.

[8] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors, 20(8), 2311.

[9] Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A Conceptual Model for Investigating the Effect of Privacy Concerns on E-Commerce Adoption: A Study on United Arab Emirates Consumers. Electronics, 11(22), 3648.

[10] Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Abou Elazm, A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. Computational Intelligence and Neuroscience, 2021.

[11] Almaiah, M. A., Ali, A., Hajjej, F., Pasha, M. F., & Alohali, M. A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors, 22(6), 2112.

[12] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. IEEE Access, 8, 176495-176520.

[13] Alabadleh, A., Aljaafreh, S., Aljaafreh, A., & Alawasa, K. (2018). A RSS-based localization method using HMM-based error correction. Journal of Location Based Services, 12(3–4), 273–285.

[14] Almaiah, M. A., Al-Zahrani, A., Almomani, O., & Alhwaitat, A. K. (2021). Classification of cyber security threats on mobile devices and applications. In Artificial Intelligence and

Blockchain for Future Cybersecurity Applications (pp. 107-123). Cham: Springer International Publishing.

[15] Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV based mutual authentication scheme for constraint oriented networks. IEEE Access, 8, 44459-44469.

[16] Almomani, O., Almaiah, M. A., Alsaaidah, A., Smadi, S., Mohammad, A. H., & Althunibat, A. (2021, July). Machine learning classifiers for network intrusion detection system: comparative study. In 2021 International Conference on Information Technology (ICIT) (pp. 440-445). IEEE.

[17] Adil, M., Khan, R., Almaiah, M. A., Binsawad, M., Ali, J., Al Saaidah, A., & Ta, Q. T. H. (2020). An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. IEEE Access, 8, 148510-148527.

[18] Alsyouf, A., Lutfi, A., Al-Bsheish, M., Jarrar, M. T., Al-Mugheed, K., Almaiah, M. A., ... & Ashour, A. (2022). Exposure detection applications acceptance: The case of COVID-19. International Journal of Environmental Research and Public Health, 19(12), 7307.

[19] Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity concerns in smart-phones and applications: A survey. In 2021 international conference on information technology (ICIT) (pp. 725-731). IEEE.

[20] Almaiah, M. A. (2021). A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In Artificial intelligence and blockchain for future cybersecurity applications (pp. 217-234). Cham: Springer International Publishing.

[21] Schmeelk, S. (2020). Creating a standardized risk assessment framework library for healthcare information technology. Proceedings of the Annual Hawaii International Conference on System Sciences, 2020-January, 3881–3890. https://doi.org/10.24251/hicss.2020.474.

[23] Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. Risk Management and Healthcare Policy, 9, 75–85. https://doi.org/10.2147/RMHP.S99908.

[24] Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Hwaitat, A. K. A., ... & Aldhyani, T. H. (2022). Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels. Electronics, 11(21), 3571.

[25] Almaiah, M. A., Dawahdeh, Z., Almomani, O., Alsaaidah, A., Al-Khasawneh, A., & Khawatreh, S. (2020). A new hybrid text encryption approach over mobile ad hoc network. Int. J. Electr. Comput. Eng.(IJECE), 10(6), 6461-6471.

[26] Alrawad, M., Lutfi, A., Alyatama, S., Elshaer, I. A., & Almaiah, M. A. (2022). Perception of occupational and environmental risks and hazards among mineworkers: A psychometric paradigm approach. International journal of environmental research and public health, 19(6), 3371.

[27] Almaiah, M. A., Al-Rahmi, A., Alturise, F., Hassan, L., Lutfi, A., Alrawad, M., ... & Aldhyani, T. H. (2022). Investigating the effect of perceived security, perceived trust, and information quality on mobile payment usage through near-field communication (NFC) in Saudi Arabia. Electronics, 11(23), 3926.

[28] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics, 11(20), 3330.

[29] Albalawi, A. M., & Almaiah, M. A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. J. Theor. Appl. Inf. Technol, 100, 2988-3011.

[30] Kemboi, L., & Ronoh, L. (2021). Security Control Model for Electronic Health Records. International Journal of Applied Sciences: Current and Future Research Trends, 12(1), 43-52.

[31] Al-Mejibli, I. S. (2019). A Fuzzy Analytic Hierarchy Process for Security Risk Assessment of Web based Hospital Management System. International Journal of Advanced Trends in Computer Science and Engineering, 8(5), 2470–2474. https://doi.org/10.30534/ijatcse/2019/92852019

[32] Alsubaei, F., Abuhussein, A., & Shiva, S. (2017). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017, September 2018, 112–120. https://doi.org/10.1109/LCN.Workshops.2017.72.

[33] Qasem, M. H., Obeid, N., Hudaib, A., Almaiah, M. A., Al-Zahrani, A., & Al-Khasawneh, A. (2021). Multi-agent system combined with distributed data mining for mutual collaboration classification. IEEE Access, 9, 70531-70547.

[34] Almudaires, F., & Almaiah, M. (2021, July). Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In 2021 International Conference on Information Technology (ICIT) (pp. 732-738). IEEE.

[35] AlMedires, M., & AlMaiah, M. (2021, July). Cybersecurity in industrial control system (ICS). In 2021 International Conference on Information Technology (ICIT) (pp. 640-647). IEEE.

[36] Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., ... & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using sem. Sustainability, 15(13), 9908.

[37] Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17), 3618.

[38] Mohamed, M. A., Shawai, Y. G., Almaiah, M. A., Derahman, M. N., Lutfi, A., & Bakar, K. A. A. (2024). Challenges in data representation for efficient execution of encryption operation. Bulletin of Electrical Engineering and Informatics, 13(2), 1207-1216.

[39] Scientific, L. L. (2024). ENHANCING CLOUD SECURITY BASED ON THE KYBER KEY ENCAPSULATION MECHANISM. Journal of Theoretical and Applied Information Technology, 102(4).

[40] ALKHDOUR, T., ALMAIAH, M. A., ALI, A., LUTFI, A., ALRAWAD, M., & TIN, T. T. (2024). REVOLUTIONIZING HEALTHCARE: UNLEASHING BLOCKCHAIN BRILLIANCE THROUGH FUZZY LOGIC AUTHENTICATION. *Journal of Theoretical and Applied Information Technology*, *102*(4).

[41] ALMAIAH, M. A., ALI, A., SHISHAKLY, R., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). A NOVEL FEDERATED-LEARNING BASED ADVERSARIAL FRAMEWORK FOR AUDIO-VISUAL SPEECH ENHANCEMENT. *Journal of Theoretical and Applied Information Technology*, *102*(4).

[42] ALMAIAH, M. A., ALI, A., SHISHAKLY, R., ALKHDOUR, T., LUTFI, A., & ALRAWAD, M. (2024). BUILDING TRUST IN IOT: LEVERAGING CONSORTIUM BLOCKCHAIN FOR SECURE COMMUNICATIONS. *Journal of Theoretical and Applied Information Technology*, *102*(3).

[43] Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors*, *24*(2), 713.

[44] Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaayah, M. A. (2024). Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *37*(1), 115-127.