MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

# Opti-IntrusionNet: Hybrid Deep Learning Entrenched End-to-End Intrusion Detection System Framework Design for Blockchain Assisted Egde-IoMT Environment

D.Gowthami
Research scholar
Department of Computer Science and Engineering
Faculty of Engineering
Karpagam Academy of Higher Education
Coimbatore, Tamil Nadu, India
Corresponding Author: gowthamime16@gmail.com

Dr.M.Vigenesh
Associate Professor
Department of Computer Science and Engineering
Faculty of Engineering
Karpagam Academy of Higher Education
Coimbatore, Tamil Nadu, India
mvigenesh@gmail.com

***Abstract –*** Malicious cyber threats and data privacy were the major issue in Internet of Medical Things (IoMT) environment due adoption of cutting-edge technologies such Artificial Intelligence (AI) and Blockchain. There were lot of research works undertook by many of the existing works by designing Intrusion Detection System (IDS) using AI and blockchain technologies respectively. However, the essence of emancipating the security and privacy clutches in IoMT environment were not yet resolved. To address this issue, we have designed an End-to-End IDS framework for IoMT environment using hybrid deep learning method named Optimized Intrusion detection Network (Opti-IntrusionNet). Initially, we perform authentication by the Trusted Authority (TA) to resolve the unwanted malicious traffic at the initial stage using Hash based Block Cipher-256 (HBC-256) algorithm. Upon authenticated, the secrecy and privacy of the information is ensured by performing optimal channel selection method using Binary Grasshopper Optimization Algorithm (BGOA) based on adequate channel related metrics. Followed by, we perform malicious traffic detection at the distributed edge servers using hybrid of two deep learning algorithms named Optimized AlexNet and Gated Recurrent Unit (OA-GRU). The optimized AlexNet is utilized for feature extraction whereas the GRU is utilized for intrusion classification into normal and malicious traffic respectively. At last, all the IoMT environment information are stored in the cloud assisted blockchain using Delegated Proof of Accessibility (DPOA) consensus algorithm. The implementation of the proposed work is carried out using python 3.11.4 with valid python and machine learning libraries respectively. The performance of the proposed work is analyzed from several performance metrics such accuracy, precision, recall, F-score, and ROC-AUC that shows that the proposed Opti-IntrusionNet outperforms than the existing works.

***Index Terms – Internet of Medical Things (IoMT), Intrusion Detection System (IDS), Blockchain, Distributed Edge Computing, Authentication, and secure channel selection.***

## I. INTRODUCTION

The Internet of Things (IoT) represents network of physical objects which are embedded with sensor, software, processing ability and other technologies with the intention of connecting and exchanging data with device or over the internet [1]. In recent years, explode of IoT has gone tremendous day by day. According to the survey, it is estimated that the usage of IoT devices will increase to 525 billion by 2030. The advancement of IoT solutions is the main reason for such proliferation [2]. Many of the applications are correlated with IoT acquisition which mainly includes medical related application. The amalgamation of IoT with medical environment emerged to be the new field named Internet of Medical Things (IoMT) [3], [4]. The IoMT consist of many smart medical devices and sensors which senses the patients health status for providing timely assistance. The sensed information was pass through servers which can be accessed remotely by the IoMT users such as patients, doctors, and medical assistants. Although the benefits included in IoMT, the lack of security is the major issue in this technology [5], [6]. The attackers can easily tamper with user valuable medical information which affects the patient privacy and sensitive information thereby affects the Quality of Life (QoL), Quality of Service (QoS), and Quality of Experience (QoE) [7], [8].

To overcome these issues, many of the existing works go through several researches however they are lack with security, high complexity and high-power consumption [9]. In addition, former existing research perform authentication, deployment of firewall and gateways to enhance the security but they are also lack with insufficient security and high time consumption. Some works performs either authentication and access control methods to breach the primary vulnerable attacks [10]. The authentication methods were different for devices and users. For devices, device identity and location were utilized. In some cases, the Medical Access Control (MAC) and Internet Protocol (IP) were utilized. Whereas, for the users the PIN, finger print, and voice recognition methods were utilized. The acquired inputs from the users and devices were processed by cryptographic algorithms [11], [12]. Some of the common cryptographic algorithms utilized were Elliptical Curve Cryptography (ECC), Advanced Encryption Standard (AES), Elliptical Curve Digital Signature Algorithm (ECDSA). Besides, the existing access control methods were purely role, attribute, or trust based which lacks with proper access control for both the users and devices [13], [14]. On the whole, both the authentication and access control methodologies provides only initial level security which were resist against only few types of attacks. Whereas the most complex and unknown attacks were originated from the malicious group through network traffic [15]. To defeat this complication, the IDS was trained along with Artificial Intelligence (AI) technology to improve the training and detection efficiency. There are several types of IDS such as Application & Protocol Entrenched IDS (APEIDS), Protocol Entrenched IDS (PEIDS), Host Entrenched IDS (HEIDS), Network Node Entrenched IDS (NNEIDS), and Network IDS (NIDS). Further, the methods involved in IDS such as signature, anomaly, and hybrid IDS respectively [16], [17]. The major drawbacks in the convention IDS listed were lesser specificity, centralized, less robust nature, and less accurate.

The machine learning (ML), deep learning (DL) and neural network (NN) algorithms are plays major role in training the IDS to perform intrusion detection [18]. However, these algorithms are lack with high complex, power consumption and ineffective training due to its instability. For IoMT environment lesser complexity and timely detection was highly recommended. In addition, the blockchain technology was implemented in several existing works to improve privacy preservation however, the utilization of traditional blockchain lack with confidentiality, and non-scalability which leads to security breaches [19], [20]. Some of the notable existing problems faced by the state-of-the-art works are listed below,

To detect the intrusion effectively, many existing works exploited AI approaches with ML/DL to amplify the detection performance. However, the existing works are lack with high complexity, lack of security and heterogeneity problems. The problems are described below,

- In most of the existing works, the communication between the server and users are not performed through the secure channel where the attackers can easily access the user valuable private information. In addition to that, the intrusion information exchanges (i.e. prevention measures) among the servers also left unsecure leads to poor security.
- Some existing works either performs authentication or access control methods respectively for securing their whole IoMT

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

environment which lacks the environment to resist against complex and unknown attacks. Furthermore, the adoption of state-of-the-art IDS methods affects the accuracy and specificity during attack detection.

- Finally, the utilization of conventional ML and DL algorithms increases the complexity in detecting the intrusions. Furthermore, the conventional ML/DL algorithm did not have the ability to process the traffic related features for intrusion detection.

The aforesaid existing problems motivates us to propose a research with aim and scope of perform effective intrusion detection and prevention system in IoMT environment using edge computing and AI technology. In addition, the research also identifies the problems of considering lack of security, ineffective training, high complexity and high false alarm rate. The major objective of this research is described below,

- To reduce communication overhead, the 6G technology was deployed which sought for better reliability.
- The transaction certainty is improved by modified blockchain technology and secure channel selection which enhance privacy preservation.
- All the users are authenticated, which only allows the legitimate users to access the network for enhancing network security.
- To ameliorate IDS performance, enhanced DL model is designed along with model optimization strategy to boost up the training efficiency.
- To reduce the unwanted access by performing access control and risk evaluation strategies respectively.

## II. Related Works

This section reveals the notable contributions of the state of the works on securing the IoMT environment using different security approaches. The various security and privacy approaches includes IDS, authentication schemes, and federated learning schemes respectively.

S. Nandy et al [21] designed an IDS framework by exploiting swarm entrenched neural networks. The swarm entrenched neural network effectively assesses the network data at the time of transmission in the network edge to improve the detection accuracy. A. Ghourabi et al [22], exploits transformer and light gradient boosting machine algorithm for securing the IoMT environment. Different from the other works, this work performs both the intrusion and malware detection respectively to provide the complete security. F. Khan et al [23] designs a fog & cloud-based architectures for attack detection using ensemble learning method. The algorithm ensembled in this work are long short-term memory and decision tree algorithms respectively. D. Javeed et al [24] adopts hybrid deep learning algorithm such as long short term memory and gate recurrent unit algorithms for designing intrusion detection system. Further, the black box nature of the deep learning algorithms was resolved by including explainable nature named shapely adaptive explanations. Binbusayyis, A et al [25] conducts comparative study on the different machine learning algorithm towards intrusion detection system in IoMT environment. The notable machine learning algorithms utilized were k-nearest neighbours, support vector machine, decision tree, Navies Bayes, and artificial neural networks. M. Kumar et al [26] provides end-to-end security to the IoMT environment by performing privacy preservation, data analysis, and secure data uploading using k-anonymity algorithm, optimized Elman neural network, and Rooted Elliptic Curve Cryptography with Vigenère Cipher respectively. S. Rahmadika et al [27] amalgamates blockchain technology and deep learning algorithm for designing misbehaviour detection model for IoMT environment. The deep learning algorithm utilized named bi-directional long short-term memory and also utilized Ethereum blockchain technology with smart contract technology. Gupta, K et al [28] designs an intrusion detection model based on decision tree algorithms. Besides, this work also performs dimensionality reduction on input to improve the detection accuracy. P. Radoglou-Grammatikis et al [29] presents both the intrusion detection and prevention system for IoMT environment using self-learning approach. Specifically, this work provides security to the TCP and HTTP protocols respectively. Khan, I et al [30] also adopts explainable AI algorithm for enabling threat detection in IoMT environment. For the skipped recurrent units, the explainable model is applied to justify the detection accuracy.

Y. K. Saheed et al [31] combines deep learning, machine learning, and optimization algorithm for detecting the cyber threats in IoMT environment. The deep recurrent neural network was amalgamated with conventional machine learning algorithm for intrusion detection. Further, the particle swarm optimization was used to parameter optimization. Y. Gao et al [32] exploits blockchain technology to the edge enabled medical environment along with safe guard extension method. More specifically, the authentication was enabled by blockchain and integrity of data assessment was enabled by safe guard extension method. V. Ravi et al [33] utilized attention based deep learning algorithm for IDS in IoMT environment. The attention layers in the deep learning algorithm firmly analyses the temporal and spatial features to enhance the learning accuracy. D. C. Nguyen et al [34] performs access control, offloading, and privacy using smart contract authentication, edge computing entrenched offloading, and blockchain technology respectively. P. Singh et al [35] utilized deep learning and hierarchical federated learning for detecting threats in IoMT environment. Here, the deep learning algorithm utilized named hierarchical long short-term memory. V. Kotiyal et al [36] also utilized federated Siamese network for detecting the outlier in IoMT environment. The accuracy achieved by this work was amplified than the state-of-the-art works. A. Lakhan et al [37] utilized blockchain and federated learning technology for securing the IoMT environment. Utilizing both the federated learning and blockchain technology, the tasks from the IoMT devices were scheduled. Different from the aforementioned work the R. Guo et al [38] secures the IoMT data by performing encryption scheme based on attributes in cloud entrenched IoMT environment. The encryption model designed by this work was provably resisted against collision and highly secure. M. Adil et al [39] performs authentication and AI technology for securing the IoMT environment. The AI algorithm utilized was supervised machine learning and cryptographic parameter entrenched decryption and encryption respectively. J. Zhang et al [40] secure the IoMT data by adopting paring independent signcryption system for resisting the attacks in IoMT environment. The designed signcryption scheme reduce the computation cost and amplify the security.

## III. Background

This section explains the preliminary knowledge of the methods/algorithms used in the proposed work. In this section, we explain the exploited message hashing algorithm and blockchain technology respectively as follows.

### *A. Hash based Block Cipher-256 (HBC-256)*

In our work, the messages are hashed using HBC-256. The general format of hashing the message is denoted as $\mathrm{Me}(\mathrm{Me}^0, \mathrm{Me}^1, \dots, \mathrm{Me}^{h-1})$ at $u = 3$ in which the u denotes the parts in the message, $\mathrm{Me}^p(\mathrm{Me}^0, \mathrm{Me}^1, \dots, \mathrm{Me}^{u-1})$ denotes the block of message Me that composed of bits $128 \times u$, $p = 0,1, \dots, h-1$. The HBC-256 utilized principal key of $pu_0^i$ from the $\mathrm{Me}^p$ of Me. The successive mediator hash is denoted as $ha_{i-1}^i, i = 0, \dots, u-1$. During the initial stage of message hashing $\mathrm{Me}(\mathrm{Me}^0, \mathrm{Me}^1, \dots, \mathrm{Me}^{h-1})$, the primary value of hash is acquired as $ha_0^i = 0^{128}$. Entrenched on the number of blocks in message $\mathrm{Me}^p$, key rounds $pu_j^i, j = 1,2, \dots, \mathrm{Ro}_1$ in which the Ro is denoted as number of hashing rounds in $\mathrm{Me}^p$ message block.

Utilizing compression function, the HBC-256 is performed. The compression function composed of dual inputs such as round key of 128 bit $pu_j^i$, mediator hash value of 128 bit $ha_j^i$, and 128-bit input message $ha_{j-1}^i$. The non-linearity of the inputs is determined by adopting S-box method. For the u-times, the hashing is performed to provide the complete message hash.

## IV. Proposed Model

In this research, we mainly focus on providing security in an IoMT environment by performing intrusion detection. The blockchain-based authentication is proposed to achieve better security and privacy preservation. The proposed work utilized Blockchain technology with Delegated Proof of Accessibility (DPoA) algorithm for validation. Furthermore, we have also utilized Artificial Intelligence (AI) algorithm for Intrusion Detection System (IDS). In addition to that, we have adopted 6G communication technology for enabling ultra-fast communication with no communication overhead. The entities involved in this work such as Smart IoMT device, distributed edge servers, Trusted Authority (TA), cloud assisted blockchain, and end users. Fig 1 represents the simplified architecture of the proposed work. The brief explanation of the entities involved are described below,

- ***Smart IoMT Device:*** The Smart IoMT device involved of body sensors, medical equipment, and medical vehicles respectively. Those devices and sensors are responsible continuously monitoring and reporting the patient health status.
- ***Distributed Edge Servers (DEdS):*** The DEdS is responsible for optimal channel selection and IDS respectively. By exploiting the

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

edge servers in distributed manner, the problem of single point of failure will be reduced.

- ***Trusted Authority (TA):*** For authenticating both the smart IoMT devices, and end users the TA is utilized. The functionalities of TA are juxtaposed with blockchain to enhance the legitimacy verification.
- ***End Users:*** The End users includes patients, doctors, and medical assistants whom are used dedicated applications to view, and analyse their health status. It is noted that, in our work we have enabled separate access rules of end users based on their roles.
- ***Cloud assisted Blockchain:*** The blockchain technology is utilized for amplifying the privacy measures in the IoMT environment. Along with that, we have also exploited DPoA consensus to the blockchain to enable better and secure storage.

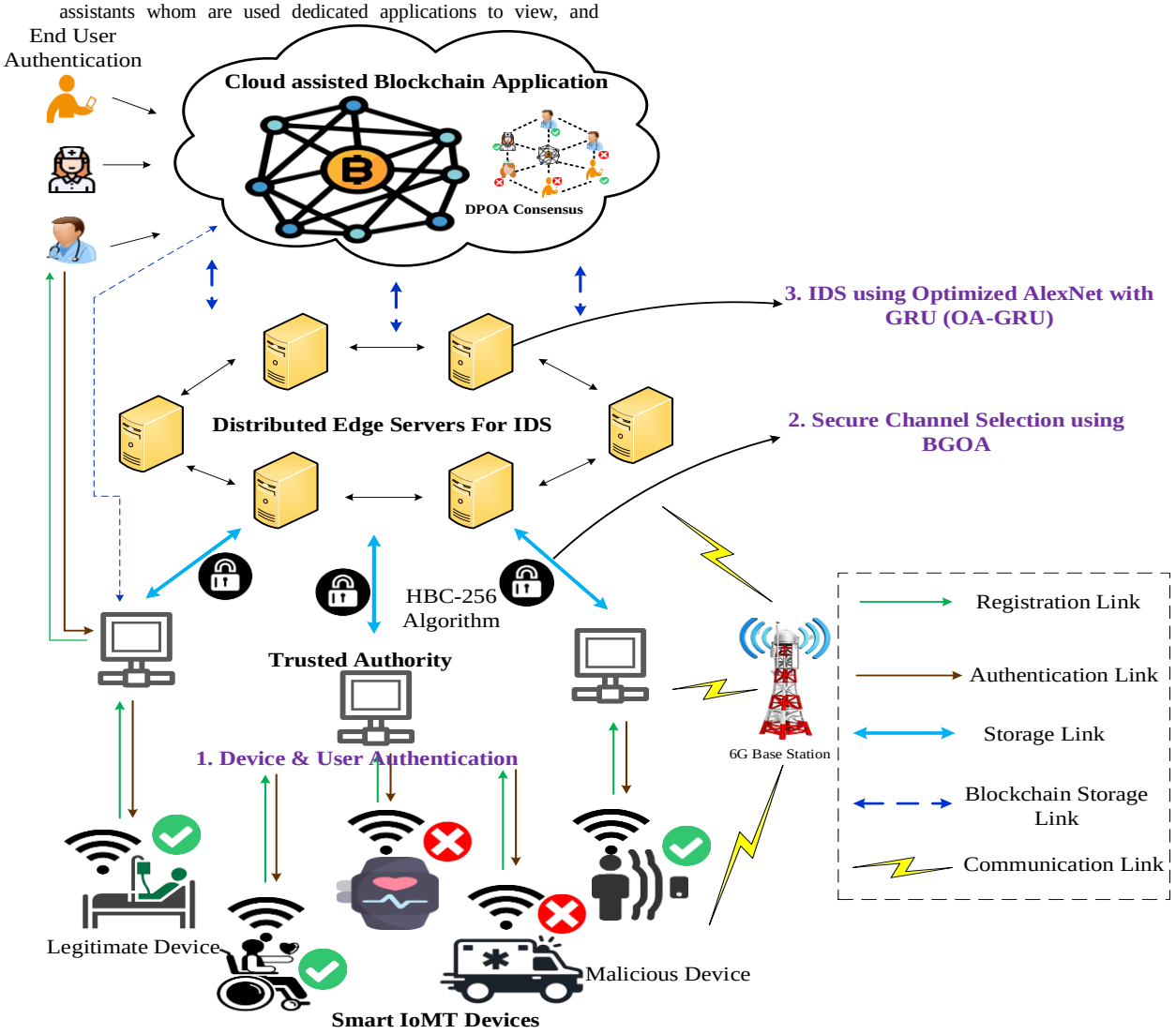


Fig. 1 Simplified Architecture of the Proposed Opti-IntrusionNet

### A. *User & IoMT Device Authentication*

Initially, the users and devices are confirming their legitimacy to the blockchain through TA. The users in the proposed environment such as patients, doctors, and medical assistants utilize their User ID (U_ID), password, and biometrics for ensuring their legitimacy. Whereas, the remote IoMT devices utilize Device_ID (D_ID), location, and Medium Access Control (MAC) address for authenticity verification. Once the entities are authenticated, the information/message sent by them are hashed using Hash based on Block Cipher (HBC-256) hashing algorithm which effectively balances computational speed and protects against preimage attacks. The detailed mathematical explanation of HBC-256 is shown in section III. In addition to that, we have implemented smart contract-based verification of security key is implemented to allow the device to access network. By performing authentication, the malicious device attacks are resisted. The steps involved authentication are described below,

*(i) Registration Phase*

At first, the users and smart IoMT devices are registered to TA by sending the registration request. Upon receiving the registration request, the TA asks the sender to create them with newer login ID and password respectively. The mathematical representation of those processes are mentioned below,

$$\mathrm{Reg}_{\mathrm{req}}[\mathrm{U}^{\mathrm{IoMT}}, \mathrm{SD}^{\mathrm{IoMT}}] \rightarrow \mathrm{TA} \quad (1)$$

$$\mathrm{TA}\left(\mathrm{Reg}_{\mathrm{req}}[\mathrm{U}^{\mathrm{IoMT}}, \mathrm{SD}^{\mathrm{IoMT}}]\right) \rightarrow \mathrm{Rep}[\mathrm{credentials}] \quad (2)$$

$$\begin{cases} \mathrm{U}^{\mathrm{IoMT}}[\mathrm{U_{ID}}, \mathrm{Pass}, \mathrm{BIO}] \\ \mathrm{SD}^{\mathrm{IoMT}}[\mathrm{D_{ID}}, \mathrm{Loc}, \mathrm{MAC}] \end{cases} \rightarrow \mathrm{TA} \quad (3)$$

The above equation (1), (2), and (3) represents the registration request to TA, registration request reply by acquiring the private credentials respectively. The obtained credentials are then stored in TA itself and also forwarded to the blockchain to ensure legitimacy. Once the credentials are stored, the TA provides the Permanent Authentication Token (PAT) along with their created password and biometrics for their authentication. The PAT is utilized to ensure the user/device presence time in the environment. It is noted that, for the IoMT device the PAT has higher presence time whereas for the users the PAT time is

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

minimal. The mathematical representation of those processes is mentioned below,

$$\mathrm{TA} \rightarrow \begin{cases} \mathrm{TA(dat)} \rightarrow [\mathrm{U^{IoMT}}, \mathrm{SD^{IoMT}}] \\ \mathrm{BL(dat)} \rightarrow [\mathrm{U^{IoMT}}, \mathrm{SD^{IoMT}}] \end{cases} \quad (4)$$

$$\mathrm{TA} \begin{cases} \mathrm{PAT, BIO, Pass, U\_ID} \\ \mathrm{PAT, Pass, D\_ID} \end{cases} \rightarrow \mathrm{U^{IoMT}}, \mathrm{SD^{IoMT}} \quad (5)$$

Where, the equations (4), and (5) denotes the credential storage in TA & blockchain, and login credential creation respectively.

*(ii) Authentication Phase*

During authentication, the entities sends an authentication request to the TA. Once the request has been received, the TA also makes request to the blockchain to share the original proof of the requestors. The detailed mathematical explanations are provided below,

$$\mathrm{Auth_{req}}[\mathrm{U^{IoMT}}, \mathrm{SD^{IoMT}}] \rightarrow \mathrm{TA} \quad (6)$$

$$\mathrm{TA} \rightarrow \mathrm{BL(credentials\ \&\ PAT)} \quad (7)$$

Upon acquiring the already stored credentials from blockchain, and PAT. It initially checks the originality of the legitimacy by verifying with current and previously stored credentials. The formulation of authenticity verification is presented as,

$$\mathrm{TA} \rightarrow \begin{cases} \mathrm{Reg^{cren}} = \mathrm{Auth^{cren}}, & \text{Legitimate} \\ \mathrm{Reg^{cren}} \neq \mathrm{Auth^{cren}}, & \text{Illegtimate} \end{cases} \quad (8)$$

Where, $\mathrm{Reg^{cren}}$ and $\mathrm{Auth^{cren}}$ denotes the registration and authentication credentials respectively. If both are same, then the particular entity is authenticated and considered as legitimate otherwise discarded from the network. In addition to that, the TA also closely watched the PAT once the entity get authenticated. If the PAT time for the corresponding entity increased to their limit the login session is expired and they must re-login again. Along with time, their activities also monitored to strongly ensure their legitimacy.

*B. Optimal Channel Selection*

After performing successful authentication, the optimal channel selection was executed to perform the communication securely and precisely. The Binary Grasshopper Optimization Algorithm (BGOA) was utilized for optimal channel selection by considering occupancy of channel, Signal to noise ratio (SNR), information capacity of channel, channel angle, channel height, bit rate, channel state information (CSI), QoS and feedback. After each communication, the feedback was collected from the users and stored in the blockchain to improve the channel selection. By executing the communication optimally and securely channel-based attacks are mitigated. In our work, we consider the optimal solution as an optimal channel for communication whereas the information passes are considered as the grasshoppers. At first, the population of the channels and grasshoppers are initialized. To be more specific, the swarm of grasshopper is initialized as $\mathrm{Y_j} = (\mathrm{j} = 1,2,..,\mathrm{M})$ in which the M is denoted as size of swarm (i.e. Channel). For every channel, a binary value is assigned as '0' and '1' respectively with the probability of 0.5 as,

$$\mathrm{Y_j^i}(0) = \begin{cases} 0, \text{if } \mathrm{RAN()} > 0.5 \\ 1, \text{otherwise} \end{cases} \quad (9)$$

From the above equation, $\mathrm{Y_j^i}$ denotes the i-th dimension of the j-th channel whereas the RAN provides the binary values among 0 and 1 respectively.

At that time of searching, the grasshoppers tried to find the optimal channel in the swarm based on the population level and channel characteristics mentioned above. More clearly, the grasshoppers continuously updating its search position that can be formulated as,

$$\mathrm{d} = \mathrm{D_{maxi}} - \mathrm{ct^{iter}} \frac{\mathrm{D_{maxi}} - \mathrm{D_{mini}}}{\mathrm{max^{iter}}} \quad (10)$$

From the above equation, $\mathrm{D_{mini}}$ represents the minimal position value (worst channel characteristics during search) and $\mathrm{D_{maxi}}$ represents the maximal position value (best channel characteristics during search). Whereas the $\mathrm{max^{iter}}$, and $\mathrm{ct^{iter}}$ denotes the maximum and current iteration respectively. For the binary phase the position updation of the grasshopper for finding the best channel can be formulated as,

$$\mathrm{Y_{jc}} - \mathrm{tar_c} = \mathrm{d}\left(\sum_{\mathrm{i}=1, \mathrm{i}\neq 1}^{\mathrm{M}} \mathrm{d} \frac{\mathrm{UB^c} - \mathrm{LB^c}}{2} \mathrm{STR}\left(\left|\mathrm{Y_i^c} - \mathrm{Y_j^c}\right|\right) \frac{\mathrm{Y_i} - \mathrm{Y_j}}{\mathrm{c_{ij}}}\right) \quad (11)$$

Where, $\mathrm{tar_c}$ denotes the target in c-th dimension, $\mathrm{LB^c}$ and $\mathrm{UB^c}$ denotes the lower and upper bound in c-th dimension respectively, STR denotes the channel capacity based on its characteristics. Overall the above equation (10) presents the distance among the $\mathrm{Y_{jc}}$ and $\mathrm{tar_c}$. For computing distance among them, hamming distance measure is utilized. Based on the two strings and channel features in the grasshopper, the hamming distance measure is computed as,

$$\left|\mathrm{Y_i} - \mathrm{Y_j}\right| = \mathrm{Hamm^{dis}}\left(\mathrm{Y_i}, \mathrm{Y_j}\right) = \sum_{\mathrm{b}=1}^{\mathrm{U}} \left[\mathrm{Y_{ib}} \neq \mathrm{Y_{jb}}\right] \quad (12)$$

From the above equation, $\mathrm{Hamm^{dis}}()$ denotes the hamming distance measure which must be lies among [0,1] , and b denotes the feature index that can be varied among 1 to U. At that case of one bit, the formulation of hamming distance can be provided as,

$$\mathrm{Hamm^{dis}}\left(\mathrm{Y_{ic}}, \mathrm{Y_{jc}}\right) = \begin{cases} 1, \text{if } \mathrm{Y_{ic}} = \mathrm{Y_{jc}} \\ 0, \text{if } \mathrm{Y_{ic}} \neq \mathrm{Y_{jc}} \end{cases} \quad (13)$$

The $\mathrm{Hamm^{dis}}()$ provides the binary digit in which we use transformation function Tr(dis) to transmute into real numbers. Henceforth, the equation $(\mathrm{Y_{jc}} - \mathrm{tar_c})$ can be rewritten again as,

$$\left|\mathrm{Y_{jc}} - \mathrm{tar_c}\right| = \mathrm{Tr(dis)} \quad (14)$$

From which, the $\left|\mathrm{Y_{jc}} - \mathrm{tar_c}\right| = \mathrm{Hamm^{dis}}(\mathrm{Y_{ic}}, \mathrm{tar_c})$ denotes the hamming distance among $\mathrm{tar_c}$ and $\mathrm{Y_{jc}}$ respectively. Henceforth, the function dis can be computed as,

$$\mathrm{dis} = \mathrm{d}\left(\sum_{\mathrm{i}=1, \mathrm{i}\neq 1}^{\mathrm{M}} \mathrm{d} \frac{\mathrm{UB^c} - \mathrm{LB^c}}{2} \mathrm{STR}\left(\left|\mathrm{Y_i^c} - \mathrm{Y_j^c}\right|\right) \frac{\mathrm{Y_i} - \mathrm{Y_j}}{\mathrm{c_{ij}}}\right) \quad (15)$$

For the binary search process, the value of $\mathrm{LB^c}$ is 0 whereas the value of $\mathrm{UB^c}$ is 1. Substuting the value, we get $\frac{1-0}{2} = 0.5$. On the whole, the Tr(dis) is responsible for channel selection based on $\lfloor \mathrm{maxi(dis)}, \mathrm{mini(dis)} \rfloor$ . The $\lfloor \mathrm{maxi(dis)}, \mathrm{mini(dis)} \rfloor$ are computed based on the channel characteristics in which when the channel characteristics possess maxi(dis) it is selected as an optimal channel for communication otherwise not selected. The formulation of Tr(dis) is provided as follows,

$$\mathrm{Tr(dis^c)} = \begin{cases} 0, \text{if } \mathrm{dis^c} > \frac{\mathrm{maxi(dis^c)} - \mathrm{mini(dis^c)}}{2} \\ 1, \text{if } \mathrm{dis^c} > \frac{\mathrm{maxi(dis^c)} - \mathrm{mini(dis^c)}}{2} \\ \text{Else} \begin{cases} 1, \text{if } \mathrm{RAN()} < 0.5 \\ 0, \text{Otherwise} \end{cases} \end{cases} \quad (16)$$

From the above equation, $\mathrm{mini(dis^c)} = 0$ whereas the $\mathrm{maxi(dis^c)} = 2 * \frac{\mathrm{d_{maxi}}}{\mathrm{dim}}$, The RAN() can be drawn randomly from the available channels from the uniform distribution [0,1]. The updation of successive searches can be formulated as,

$$\mathrm{Y_{jc}} = \begin{cases} |1 - \mathrm{Tr(dis)_c}|, \text{otherwise} \\ \mathrm{Tr(dis)_c}, \text{if } \mathrm{Tr(dis^c)} = 0 \end{cases} \quad (17)$$

From the above equation the target in c-th dimension is denoted as $\mathrm{Tr(dis)_c}$ whereas the $\mathrm{Tr(dis)_c}$ is computed in equation (16). The fitness function of solutions can be formulated as,

$$\mathrm{Fit} = ב * \mathrm{ER} + (1 - ב) * \frac{\mathrm{Sel\_Ch}}{\mathrm{Tot\_Ch}} \quad (18)$$

Where, the ER represents the error rate during channel selection process, ב denotes the channel selection co-efficient to control the local minima trap, Sel_Ch and Tot_Ch denotes the selected and total channels respectively. The pseudocode for BGOA based channel selection is provided below,

**BGOA based Channel Selection**

**Input:** Number of channels (Ch), $\mathrm{max^{iter}}$, $\mathrm{d_{mini}}$ and $\mathrm{d_{maxi}}$
**Output:** Optimal Channel (Sel_Ch)
**Set** Population of grasshopper's position $\mathrm{Y_j} = (\mathrm{j} = 1,2,..,\mathrm{M})$ at [0,1]
  Computed Fit of every grasshopper
  Computed best Ch from the Fit
  $\mathrm{ct^{iter}}$=0
  **While** ($\mathrm{ct^{iter}} < \mathrm{max^{iter}}$)
    Apprise d from equation (10)
    **Fo**r every grasshopper (info) do
      Regularize the search space [2,4]
      Compute Tr(dis) from equation (15) and (16)
      Position updation using (17)
    **End For**
      Target updation towards best channel
      $\mathrm{ct^{iter}} = \mathrm{ct^{iter}} + 1$
  **End While**
  Return Tr
**End**

*C. Hybrid DL Model for Intrusion Detection*

Once the optimal channel is selected and secure communication is successfully initiated. The network traffics from the IoMT devices are provided to the distributed and decentralized edge servers for intrusion detection. In our work, we utilize hybrid DL algorithm for designing IDS. The hybrid DL algorithm utilized named Optimized AlexNet with Gated Recurrent Unit (OA-GRU). Wholly, the designed OA-GRU is named as Optimized Intrusion

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

Detection Network (Opti-IntrusionNet). Fig 2 represents the proposed IDS using OA-GRU. The detailed explanation of Opti-IntrusionNet is explained as follows,

*(i) Optimized AlexNet*

The secured information in form of packets/flows are initially provided to the Optimized AlexNet model. More specially, the designed model analyses the network statistical and temporal features respectively. As the name suggested that optimized AlexNet, we optimize the conventional AlexNet model in terms of optimizing the size of convolutional kernels. More clearly, we increase the maxpooling (max_po) and convolutional (conv) layers whereas the output convolutional layers sizes are reduced. In addition to that, we have also removed the regularized local response layers in the optimized AlexNet. As we said earlier, the max_po is increased to 5 and the conv layer is increased to 8. The size of step is 1 and the convolutional kernel is $5 \times 5$. The output nodes numbers of the 8-conv layer are 128, 192, 256,192,128,48, and 48. Furthermore, the Fully Connected Layer (FCL) and Final Layer (FL) had 65 and 28 output nodes respectively. The major advantage of Optimized AlexNet is that it amplifies the speed of convergence by enhancing the training ability. The structure of Optimized AlexNet is shown in fig. The mathematical model of proposed model is provided as follows.

The convolutional layers with filters in the optimized AlexNet are utilized for feature extraction. It is assumed that a-th of layer e is denoted by $x_a^e$ and the i-th layer e-1 is denoted as $x_a^{e-1}$. The $x_a^e$ is computed as,

$$x_a^e = \sum_{i \in qa} z_{ai}^e * x_i^{e-1} + h_a^e \quad (19)$$

From the above equation, at the layer e the mapping of features is denoted as |q|, the prejudiced term is denoted as $h_a^e$ for all the connections to a-th feature map. Whereas for the layer e-1 the feature subset is denoted as $q_a$ at the layer a. Here, the activation function used is ReLU function for the layer a(x) can be formulated as,

$$a(x) = \max(0, x) \quad (20)$$

From the above equation, the activation function values range from 0 to x. Furthermore, the max_po can be formulated as,

$$x_{a(e+1),}, i^{e+1}, t = \max_{0 \le a < W, 0 \le i < A} y_{a^{e+1}}^e * W + j, i^{e+1} * N + I \quad (21)$$

Where,

$$0 \le f^{e+1} < w^{e+1}, 0 \le i^{e+1} < N^{e+1}, 0 \le e < E^{e+1} = E^e \quad (22)$$

The convolutional neural network with forward pass can be formulated as,

$$a^1 \to e^1 \to a^1 \to \cdots a^{z-1} \to e^{z-1} \to a^z \to e^z \to F \quad (23)$$

From the above equation, the $a^1$, $a^{z-1}$, and $a^z$ denotes the convolutional neural network, $a^1$, $e^{z-1}$, $e^z$ represents the processing of layers. The cost function of layer processing can be formulated as,

$$Cf = \frac{1}{2} \|i - a^Z\|^2 \quad (24)$$

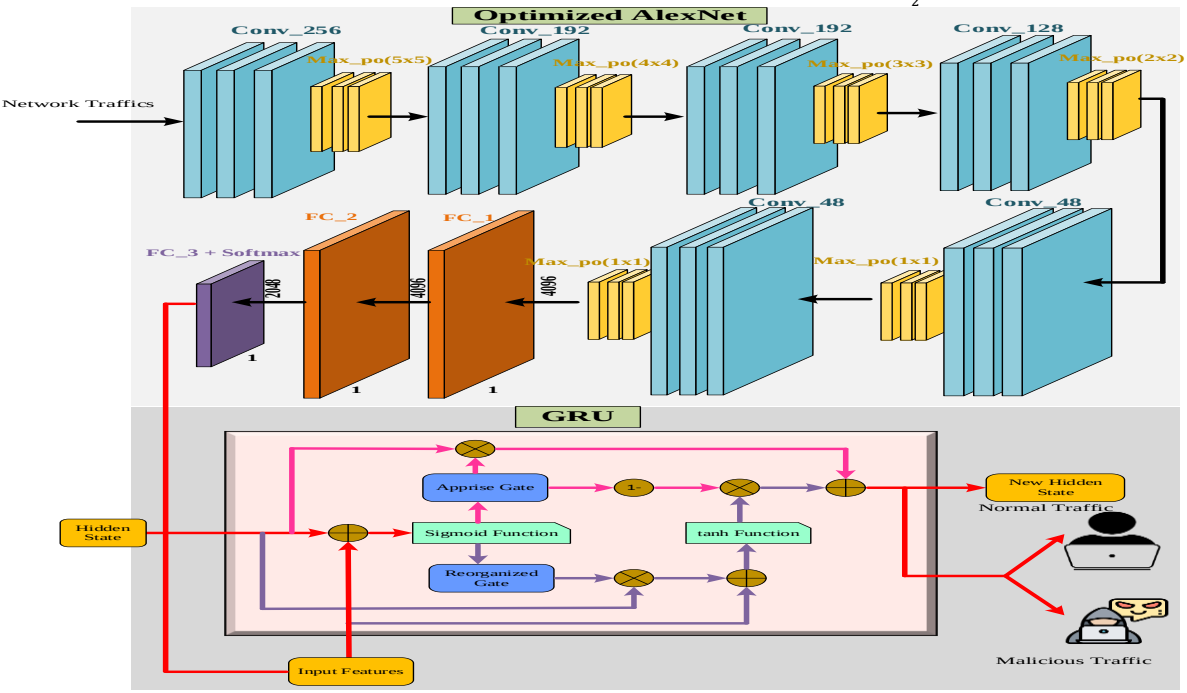


Fig 2. Proposed IDS using Hybrid DL (OA-GRU)

*(ii) Gated Recurrent Unit (GRU)*

Once the network features are processed in optimized AlexNet, it is then provided to GRU to resolve the gradient problems in the features. There are three gates in the GRU and interior cell state. The apprise gate ($\varepsilon$) is provided to process the backward and forward information. The past knowledge is provided in the reorganized gate ($\beta$). The mathematical formulation of GRU can be formulated as,

$$\beta_t = \propto \left(Y_t . We_{y\beta} + Hid_t . We_{h\beta} + p_\beta\right) \quad (25)$$

$$\varepsilon_t = \propto \left(Y_t . We_{y\varepsilon} + Hid_{t-1} . We_{h\varepsilon} + p_\varepsilon\right) \quad (26)$$

From the above equation, $p_\beta$ and $p_\varepsilon$ denotes the bias function respectively whereas the $We_{y\beta}$ and $We_{y\varepsilon}$ represents the parameters of weights respectively. Once the features are again processed with the GRU, the features are then passed to dual FCL and softmax layer to detect the intrusions.

## V. Experimental Evaluation

This section emphases and analyze the performance of the proposed Opti-IntrusionNet. The designed model accuracy and performance is scrutinized using Root Mean Square Error (RMSE). On the other hand, the IDS detector and classifier performance are examined using performance metrics such as detection accuracy, precision, recall, and F-measure. In this experiment, the system and simulation setup are configured robustly. To be clearer, the proposed work tunes the system configuration of windows 11 with AMD Ryzen 5 5600H with Radeon Graphics 3.30 GHz for distributed edge servers and blockchain setup respectively. Furthermore, we have simulated 7 IoMT devices with one 6G base station on the 8G RAM system. For compiling the proposed work, we utilize python 3.11.4 with two libraries such as pandas 1.4.0 and NumPy 1.19.5 respectively. As we designed machine learning model for IDS, the machine learning libraries used in our proposed work are Keras 2.3.0, TensorFlow 2.10, and Scikit-Learn 1.0 respectively.

The RMSE is responsible for computing the total IDS error from the actual IDS errors respectively. The formulation of RMSE is computed below,

$$RMSE = \sqrt{\frac{1}{m} \sum_{j=1}^{m} (Det^{IDS} - Act^{IDS})^2} \quad (27)$$

Furthermore, the performance of the proposed model are also indicated using key performance indicators such as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) respectively. The accuracy defines the performance of the intrusion detection model in terms of normal and malicious traffic respectively. Besides, the precision, recall, and F-measure analyze the classification performance towards malicious traffics. To be more

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

specific, the recall rate analyzes malicious events classification performance of classifier, precision rate analyzes the reliability of designed IDS model, and F-measure amalgamates both the precision and recall in single picture. Table 1 denotes the hyperparameters of the proposed algorithms. The mathematical equations of the performance metrics are provided below,

$$Acc = \frac{TP+TN}{TP+TN+FP+FN} \quad (28)$$

$$Pre = \frac{TP}{TP+TN} \quad (29)$$

$$Rec = \frac{TP}{TP+FN} \quad (30)$$

$$F-Score = 2 \times \frac{Pre \times Rec}{Pre+Rec} \quad (31)$$

Table 1
Hyperparameters of Proposed Algorithm

| Algorithms | Hyperparameter | Values |
|---|---|---|
| Optimized AlexNet | Maximum Epochs | 5 |
| | Batch Size Rate | 10 |
| | Learning Rate | 0.0005 |
| | Frequency of Validation | 4 |
| | Rate of Dropout | 0.6 |
| | Rate of momentum | 0.7 |
| | Optimizer | Stochastic Gradient Descent (SGD) |
| GRU | Dropout Rate | [1.5,0.5,0.7] |
| | No. of Hidden Layers | [1,2,3,4,5] |
| | Activation units | [Nadam, RMSprop] |
| | Loss | MSE |
| | No. of nodes among layer | [6,12,18,24,30] |
| | No. of Time Steps | 15 |
| | Activation at output | Linear |

*(i) Comparative Analysis*

The performance of the proposed Opti-IntrusionNet is examined by comparing the proposed with existing works such as LightGBM-IoMT [22], MisBlock-IoMT [27], Self-IDS [29], DewCloud-IoMT [35], and BlockFL-IoMT [37]. The LightGBM-IoMT utilized machine model named light gradient boosting machine for cyber-attack detection.

The MisBlock-IoMT work utilized BiLSTM along with smart contract based Ethereum blockchain. The Self-IDS utilized self-learning approach detecting IDS in healthcare systems. The DewCloud-IoMT designed Hierarchical federated learning with LSTM for IDS in IoMT environment. The BlockFL-IoMT designed smart scheduling framework for health care systems using blockchain consensus algorithm. The graphical comparison of proposed Vs existing works in terms of performance metrics are shown in fig 3 (a) - (d), whereas the 3 (e) & (f) denotes provides ROC curve and classification loss for the proposed work.

From the graphical analysis, it is clear that when the rate of IoMT devices/traffics increases to its maximum the performance metrics also increases. Among that, our proposed work achieves better performance than the existing works. The reason for achieving higher accuracy of the proposed work than the existing work is that, we exploit hybrid deep learning algorithm named Optimized AlexNet-GRU that reduced the unwanted layers thereby increasing the accuracy. To be clearer, the accuracy metrics analyze the end-to-end performance of the proposed model. The precision, recall, and F-measure rate of the proposed work is increased due to adoption of authentication, access control, channel selection, and blockchain techniques respectively. Those processes are robustly block and defend against malicious traffics thereby increased in precision, recall, and F-measure than the existing works. On the other hand, the mentioned existing works lacks in designing end-to-end intrusion detection framework for IoMT environment thereby achieving poor results during comparative analysis. For better understanding, we have also provided the numerical results and its difference in table 2 below.

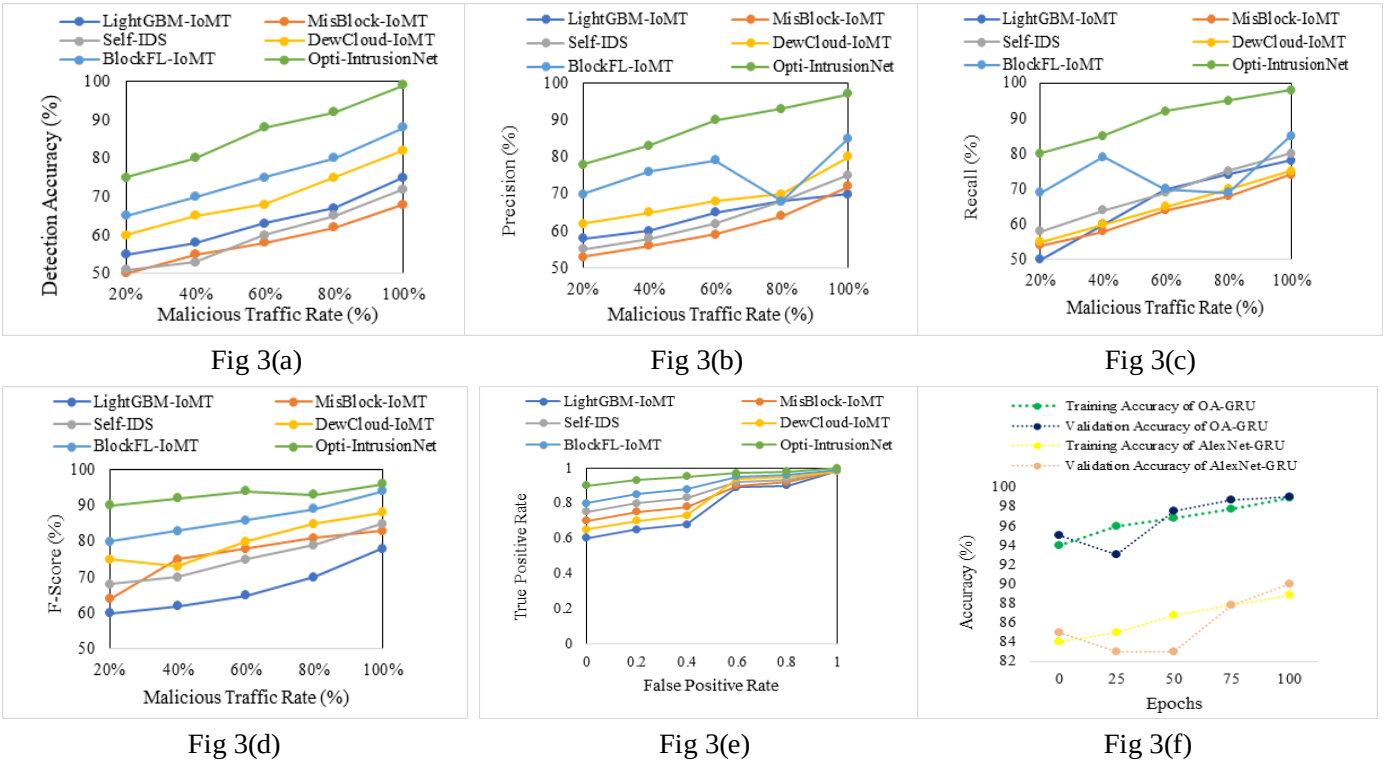


Fig 3(a) Fig 3(b) Fig 3(c)

Fig 3(d) Fig 3(e) Fig 3(f)

Fig. 3 (a)-(d) Performance of Proposed Opti-IntrusionNet on Real Time Malicious Traffic in IoMT Environment, 3 (e) ROC-AUC Curve Comparison of Opti-IntrusionNet Vs Existing Works, and 3 (f) Comparison of Training and Validation Accuracy of Proposed OA-GRU to conventional AlexNet-GRU

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

Table 2
Average Comparative Results Comparison of Proposed Vs Existing Works

| Performance Metrics | LightGBM-IoMT [22] | MisBlock-IoMT [27] | Self-IDS [29] | DewCloud-IoMT [35] | BlockFL-IoMT [37] | Opti-IntrusionNet | Difference |
|---|---|---|---|---|---|---|---|
| Accuracy | 63.6% | 58.6% | 60.2% | 70% | 75.6% | 86.8% | 11.2%-28.2% Higher |
| Precision | 64.2% | 60.8% | 63.6% | 69% | 75.6% | 88.2% | 12.6%-27.4% Higher |
| Recall | 66.4% | 63.6% | 69.2% | 65% | 74.4% | 90% | 15.6%-26.4% Higher |
| F-Measure | 67% | 76.2% | 75.4% | 80.2% | 86.4% | 93% | 6.6%-26% Higher |
| ROC-AUC Curve | 0.78435 | 0.83933 | 0.870333 | 0.825 | 0.9048833 | 0.9594983 | 0.054615-0.175233 Higher |

*(ii) IDS & Blockchain Performance Analysis*

The fig 4 (a)-(c) below shows the performance analysis of proposed IDS on various metrics. The proposed IDS is compared with various metrics such as energy consumption, and detection delay respectively. Those performance are analyzed based of extracted features during network traffic analysis. The table 3 and 4 represents the average numerical results comparison of proposed and existing works. The feature extracted by the proposed work are listed below in table 5,

Table 3
Comparison of IDS Analysis of Proposed Vs Existing Works

| Performance Metrics | | LightGBM-IoMT [22] | Self-IDS [29] | DewCloud-IoMT [35] | Opti-IntrusionNet | Difference |
|---|---|---|---|---|---|---|
| No. of IoMT Traffic | Energy Consumption | 48W | 44.1W | 30.8W | 22.1W | 8.7W-26W |
| | Model Training Delay | 68.3s | 54.6s | 50.9s | 30.4s | 13.7s-20.5s |
| | Model Testing Delay | 71.3s | 57.1s | 53.3s | 33.7s | 19.6s-37.6s |

Table 4
Comparison of Blockchain Performance Analysis of Proposed Vs Existing Works

| Performance Metrics | | MisBlock-IoMT [37] | BlockFL-IoMT [37] | Opti-IntrusionNet | Difference |
|---|---|---|---|---|---|
| No. of Storage Request | Blockchain Energy Consumption | 79.6W | 73.8W | 49.2W | 24.6W-30.4W |
| No. of Blocks | Block Creation Delay | 106.6s | 97.8s | 83.5s | 14.3s-22.5s |
| No. of Blockchain Nodes | Blockchain Scalability | 61.3% | 77.9% | 93.1% | 15.2%-31.8% |

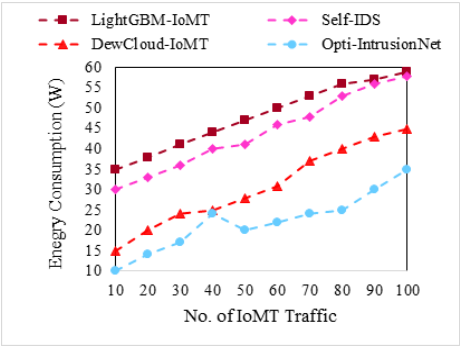


Fig 4(a)

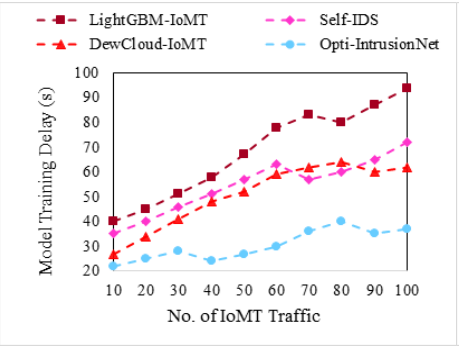


Fig 4(b)

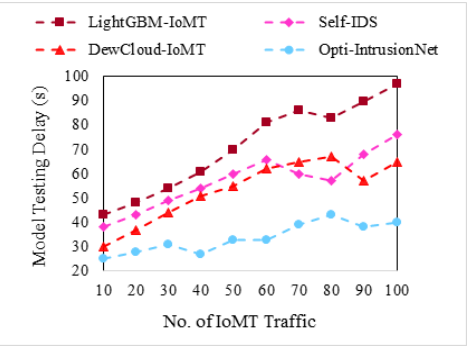


Fig 4(c)

Fig.4 (a)-(c) Energy Consumption Analysis , Model Training Delay Analysis, and Model Testing Delay Analysis of Proposed Opti-IntrusionNet vs Existing Works

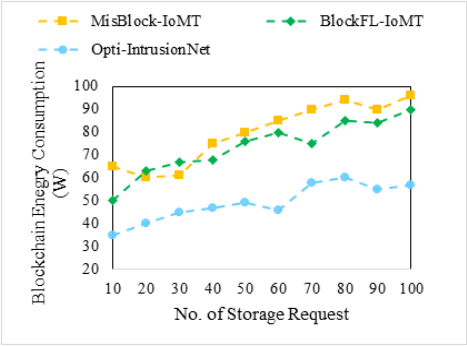


Fig 5(a)

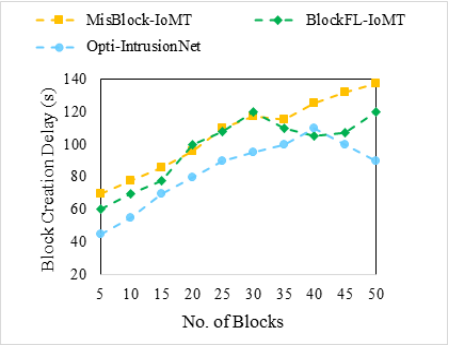


Fig 5(b)

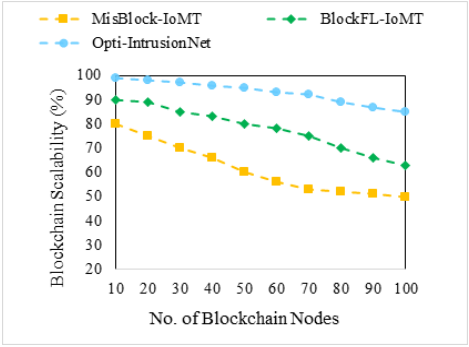


Fig 5(c)

Fig.5 (a)-(c) Blockchain Energy Consumption Analysis , Block Creation Delay Analysis, and Blockchain Scalability Analysis of Proposed Opti-IntrusionNet vs Existing Works

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

Table 5
Features Extracted by the Proposed work

| Feature | Feature Explanation |
|---|---|
| Num_Pkts_SRC_DST | Packets flown from source to destination |
| Num_Pkts_DST_SRC | Packets flown from destination to source |
| Fra_Num | Number of the frame |
| Fra_Len | Length of the frame |
| POR_DST | Destination port |
| POR_SRC | Source port |
| IP_DST | IP address of destination |
| IP_SRC | IP address of source |
| Fra_CNT_SRC | Frames received by the same source |
| Fra_CNT_DST | Frames received by the same destination |

In addition to that, the fig 5 (a)-(c) shows the performance of proposed blockchain with existing blockchain methods such as MisBlock-IoMT [27], and BlockFL-IoMT [37]. The performance of the blockchain is analyzed using metrics such as energy consumption, delay, and scalability respectively.

## VI. Discussion

From the experimental results, it is clear that the proposed work results towards the performance metrics are very promising. The numerical results achieved by the proposed work are very satisfactory in terms of comparative analysis, IDS analysis, and blockchain analysis respectively. The numerical results of comparative results shows that, when the malicious traffic rate increases to maximum from fig ()-(), the accuracy, precision, recall, F-score, and ROC-AUC achieves near to 100% such as 99%, 97%, 98%, 96%, and 0.9999 respectively whereas the state of the art works gains lesser than the existing work. Besides, the training and validation accuracy of the proposed optimized AlexNet-GRU and conventional AlexNet-GRU also compared in fig () which also shows that the proposed work achieves training and validation accuracy when the epochs is at maximized value of 100 are 98.9% and 99% respectively. Furthermore, the numerical results of IDS performance analysis from fig () - () shows that, when the number of IoMT traffic reaches it maximized rate of 100 the energy consumption rate, model training and testing delay achieved by the proposed work are 35W, 37s, and 40s respectively. In addition to that, the blockchain performance of the proposed work is shown from fig ()-(). The blockchain energy consumption rate when the storage request increased to 100 is 57W. The block creation delay when the number of blocks increase to 50 is 90s, and the blockchain scalability % when the number of blockchain nodes increases to 100 is 85%. The table 6 below represents the comparison of proposed and existing works.

Table 6
Comparison of Proposed Vs Existing Works

| Reference | Objective | Algorithms/Methods Utilized | Detection Accuracy |
|---|---|---|---|
| [22] | To secure the IoMT medical devices in independent manner using optimized ML algorithm | Light Gradient Boosting Machine algorithm | 75% |
| [27] | To detect the misbehaviors and improve the privacy rate using blockchain technology for IoMT | Bidirectional Long Short-Term Memory | 68% |
| [29] | To design an intrusion detection and prevention system for healthcare environment | Self-learning approach | 72% |
| [35] | To design an IDS for IoMT environment using cloud and federated learning methodology | Hierarchical Long Short-Term Memory | 82% |
| [37] | Utilizing blockchain and federated learning for IoMT environment to enhance the privacy preservation | FL based secure task scheduling | 88% |
| Proposed Work | To design an end-to-end IDS framework for IoMT environment using blockchain and edge computing | Optimized AlexNet-GRU (OA-GRU) | 99% |

Overall, the major strength of our proposed Opti-IntrusionNet over existing works is that we have designed an complete End-to-End IDS model along with utilizing edge computing, blockchain, and 6G technology respectively. The end-to-end model works on stage by stage to resist the cyber threats such as malicious traffic control, secure data transmission distributed IDS, and privacy aware data storage respectively.

## VII. Conclusion

Poor security, increased malicious traffic, and conventional ML and DL approaches are the major issues in edge based IoMT environment. The problems are resolved by adopting AI and blockchain technologies for IDS framework design named Opti-IntrusionNet. The entities involved in the proposed work such as smart IoMT devices, patients, doctors & medical assistants, distributed edge sever, and cloud assisted blockchain. Initially, this work performs authentication to both the IoMT devices and users to the blockchain assisted TA by considering several metrics using HBC-256 algorithm. The authentication restricts the unwanted malicious traffic thereby safe guard the environment from primary vulnerability threats. Followed by we perform channel selection for the authenticated and hashed data to ensure the privacy in IoMT environment. For that, we adopts optimization algorithm BGOA based on metrics such as occupancy of channel, Signal to noise ratio (SNR), information capacity of channel, channel angle, channel height, bit rate, channel state information (CSI), QoS and feedback. Finally, the secure data traffics are then provided to the distributed edge servers where the traffics are subjected to IDS using OA-GRU algorithm. The proposed OA-GRU algorithms classifies the traffic into two classes such as normal and malicious traffic respectively. At last, all the data including authentication data, and IDS data are stored in DPOS based blockchain as transaction which ensures the privacy. The implementation of the proposed work is carried out using python 3.11.4 along with python and machine learning libraries. The results show that the proposed work achieves better results than the existing works.

## Reference

[1] Nguyen, T.N., Ngo, Q., Nguyen, H., & Nguyen, G.L. (2022). An Advanced Computing Approach for IoT-Botnet Detection in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics, 18*, 8298-8306.

[2] Zhou, X., Xu, X., Liang, W., Zeng, Z., & Yan, Z. (2021). Deep-Learning-Enhanced Multitarget Detection for End–Edge–Cloud Surveillance in Smart IoT. *IEEE Internet of Things Journal, 8*, 12588-12596.

[3] Zhang, L., Wu, Y., Chen, L., Fan, L., & Nallanathan, A. (2023). Scoring Aided Federated Learning on Long-tailed Data for Wireless IoMT based Healthcare System. *IEEE journal of biomedical and health informatics, PP*.

[4] Ghazal, T.M., Abbas, S., Ahmad, M., & Aftab, S. (2022). An IoMT based Ensemble Classification Framework to Predict Treatment Response in Hepatitis C Patients. *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, 1-4.

[5] Alexan, W., Ashraf, A., Mamdouh, E., Mohamed, S., & Moustafa, M. (2021). IoMT Security: SHA3-512, AES-256, RSA and LSB Steganography. *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, 177-181.

[6] Wazid, M., Singh, J., Das, A.K., Shetty, S., Khan, M.K., & Rodrigues, J.J. (2022). ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things. *IEEE Access, 10*, 57990-58004.

[7] Tikkha, R., & Sharma, S. (2022). Cryptographic Measures in IoMT: Security Threats and Measurement. *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1-8.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6831-6839

[8] Sharma, I., & Sharma, S. (2022). Blockchain Enabled Biometric Security in Intemet-of-Medical-Things (IoMT) Devices. *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 971-979.

[9] Khowaja, S.A., Lee, I.H., Dev, K., Jarwar, M.A., & Qureshi, N.M. (2022). Get Your Foes Fooled: Proximal Gradient Split Learning for Defense Against Model Inversion Attacks on IoMT Data. *IEEE Transactions on Network Science and Engineering*.

[10] Gupta, D., Gupta, M., Bhatt, S., & Tosun, A.S. (2021). Detecting Anomalous User Behavior in Remote Patient Monitoring. *2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI)*, 33-40.

[11] Sharma, I., & Sharma, S. (2022). Blockchain Enabled Biometric Security in Intemet-of-Medical-Things (IoMT) Devices. *2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 971-979.

[12] Aggarwal, S., & Sharma, S. (2022). Voice Based Secured Smart Lock Design for Internet of Medical Things: An Artificial Intelligence Approach. *2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, 1-7.

[13] Sivakumar, P., Rathnam, B.R., Divakar, S., Teja, M.A., & Prasad, R.R. (2021). A Secure and Compact Multimodal Biometric Authentication Scheme using Deep Hashing. *2021 IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT)*, 27-31.

[14] Kaur, K., & Yadav, A. (2022). Physically Unclonable Function for Authentication of IoMT Systems using Hybrid Cryptography. *2022 International Conference on Futuristic Technologies (INCOFT)*, 1-6.

[15] T. Ahmed Alhaj *et al*., "A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT)," in *IEEE Access*, vol. 10, pp. 124777-124791, 2022, doi: 10.1109/ACCESS.2022.3225038

[16] F. Z. Belgrana, N. Benamrane, M. A. Hamaida, A. Mohamed Chaabani and A. Taleb-Ahmed, "Network Intrusion Detection System Using Neural Network and Condensed Nearest Neighbors with Selection of NSL-KDD Influencing Features," *2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, BALI, Indonesia, 2021, pp. 23-29, doi: 10.1109/IoTaIS50849.2021.9359689.

[17] O. Almomani, M. A. Almaiah, A. Alsaaidah, S. Smadi, A. H. Mohammad and A. Althunibat, "Machine Learning Classifiers for Network Intrusion Detection System: Comparative Study," *2021 International Conference on Information Technology (ICIT)*, Amman, Jordan, 2021, pp. 440-445, doi: 10.1109/ICIT52682.2021.9491770.

[18] A. Shukla, S. Ahamad, G. N. Rao, A. J. Al-Asadi, A. Gupta and M. Kumbhkar, "Artificial Intelligence Assisted IoT Data Intrusion Detection," *2021 4th International Conference on Computing and Communications Technologies (ICCCT)*, Chennai, India, 2021, pp. 330-335, doi: 10.1109/ICCCT53315.2021.9711795.

[19] M. M. Islam, M. K. Islam, M. Shahjalal, M. Z. Chowdhury and Y. M. Jang, "A Low-Cost Cross-Border Payment System Based on Auditable Cryptocurrency With Consortium Blockchain: Joint Digital Currency," in *IEEE Transactions on Services Computing*, vol. 16, no. 3, pp. 1616-1629, 1 May-June 2023, doi: 10.1109/TSC.2022.3207224.

[20] F. Béres, I. A. Seres, A. A. Benczúr and M. Quintyne-Collins, "Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users," *2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, United Kingdom, 2021, pp. 69-78, doi: 10.1109/DAPPS52256.2021.00013.

[21] Nandy, S., Adhikari, M., Khan, M.A., Menon, V.G., & Verma, S. (2021). An Intrusion Detection Mechanism for Secured IoMT Framework Based on Swarm-Neural Network. *IEEE Journal of Biomedical and Health Informatics, 26*, 1969-1976.

[22] Ghourabi, A. (2022). A security model based on LightGBM and Transformer to protect healthcare systems from cyberattacks. *IEEE Access, PP*, 1-1.

[23] Khan, F., Jan, M.A., Alturki, R., Alshehri, M.D., Shah, S.T., & Rehman, A.U. (2023). A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT. *IEEE Transactions on Industrial Informatics, 19*, 10125-10132.

[24] Javeed, D., Gao, T., Kumar, P., & Jolfaei, A. (2023). An Explainable and Resilient Intrusion Detection System for Industry 5.0. *IEEE Transactions on Consumer Electronics*.

[25] Binbusayyis, A., Alaskar, H., Vaiyapuri, T., & Dinesh, M. (2022). An investigation and comparison of machine learning approaches for intrusion detection in IoMT network. *The Journal of Supercomputing, 78*, 17403 - 17422.

[26] Kumar, M., Kavita, Verma, S., Kumar, A., Ijaz, M.F., & Rawat, D.B. (2022). ANAF-IoMT: A Novel Architectural Framework for IoMT-Enabled Smart Healthcare System by Enhancing Security Based on RECC-VC. *IEEE Transactions on Industrial Informatics, 18*, 8936-8943.

[27] Rahmadika, S., Astillo, P.V., Choudhary, G., Duguma, D.G., Sharma, V., & You, I. (2022). Blockchain-Based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices. *IEEE Journal of Biomedical and Health Informatics, 27*, 710-721.

[28] Gupta, K., Sharma, D.K., Datta Gupta, K., & Kumar, A.D. (2022). A tree classifier based network intrusion detection model for Internet of Medical Things. *Comput. Electr. Eng., 102*, 108158.

[29] Radoglou-Grammatikis, P.I., Sarigiannidis, P.G., Efstathopoulos, G., Lagkas, T.D., Fragulis, G.F., & Sarigiannidis, A. (2021). A Self-Learning Approach for Detecting Intrusions in Healthcare Systems. *ICC 2021 - IEEE International Conference on Communications*, 1-6.

[30] Khan, I.A., Moustafa, N., Razzak, I., Tanveer, M., Pi, D., Pan, Y., & Ali, B.S. (2022). XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks. *Future Generation Computer Systems*.

[31] Saheed, Y.K., & Arowolo, M.O. (2021). Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms. *IEEE Access, 9*, 161546-161554.

[32] Gao, Y., Lin, H., Chen, Y., & Liu, Y. (2021). Blockchain and SGX-Enabled Edge-Computing-Empowered Secure IoMT Data Analysis. *IEEE Internet of Things Journal, 8*, 15785-15795.

[33] Ravi, V., Pham, T.D., & Alazab, M. (2023). Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things. *IEEE Internet of Things Magazine, 6*, 50-54.

[34] Nguyen, D.C., Pathirana, P.N., Ding, M., & Seneviratne, A.P. (2021). BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain. *IEEE Internet of Things Journal, 8*, 11743-11757.

[35] Singh, P., Gaba, G.S., Kaur, A., Hedabou, M., & Gurtov, A.V. (2022). Dew-Cloud-Based Hierarchical Federated Learning for Intrusion Detection in IoMT. *IEEE Journal of Biomedical and Health Informatics, 27*, 722-731.

[36] Kotiyal, V., Gupta, A., Deb, P.K., Misra, S.C., Das, D., & Udutalapally, V. (2023). Skipper: A Federated Siamese Network-Based Group Activity Segregator for IoMT Systems. *IEEE Transactions on Computational Social Systems, 10*, 1770-1779.

[37] Lakhan, A., Mohammed, M.A., Nedoma, J., Martínek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A., & Wang, W. (2022). Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare. *IEEE Journal of Biomedical and Health Informatics, 27*, 664-672.

[38] Guo, R., Yang, G., Shi, H., Zhang, Y., & Zheng, D. (2021). O3-R-CP-ABE: An Efficient and Revocable Attribute-Based Encryption Scheme in the Cloud-Assisted IoMT System. *IEEE Internet of Things Journal, 8*, 8949-8963.

[39] Adil, M.N., Khurram Khan, M., Jadoon, M.M., Attique, M., Song, H.H., & Farouk, A. (2022). An AI-enabled Hybrid lightweight Authentication Scheme for Intelligent IoMT based Cyber-Physical Systems. *IEEE Transactions on Network Science and Engineering*.

[40] Zhang, J., Dong, C., & Liu, Y. (2023). Efficient Pairing-Free Certificateless Signcryption Scheme for Secure Data Transmission in IoMT. *IEEE Internet of Things Journal*.