International Journal of Safety and Security Engineering
Vol. 15, No. 10, October, 2025, pp. 2177-2189
Journal homepage: http://iieta.org/journals/ijsse

A Deep Learning and Blockchain-Based Trust Framework for Securing IoMT

Mariem Fourati*, Amel Meddeb-Makhlouf, Ferdaous Kamoun-Abid, Faouzi Zarai

New Technologies and Telecommunications Systems Research Laboratory, National School of Electronics and Telecommunications, Sfax 3018, Tunisia

Corresponding Author Email: mariem.frt@gmail.com

https://doi.org/10.18280/ijsse.151020

Received: 24 September 2025
Revised: 25 October 2025
Accepted: 28 October 2025
Available online: 31 October 2025

Keywords:
blockchain, cybersecurity, deep learning, IoMT, IDS, TMS

ABSTRACT

The adoption of Internet of Things (IoT) technologies in medical supervision enables real-time patient monitoring but also introduces significant security challenges. Traditional approaches rely on Intrusion Detection Systems (IDS) or Trust Management Systems (TMS). Yet, each faces limitations when applied independently. This study proposes an IDS-based trust management framework that integrates both approaches to strengthen Internet of Medical Things (IoMT) security. In the proposed model, trust scores are dynamically assigned to entities according to IDS outcomes, where the IDS employs a deep learning (DL)-based Convolutional Neural Network (CNN) trained on the CIC-IoMT2024 dataset. Blockchain is further incorporated to securely and transparently record trust score updates, ensuring accountability and traceability. Experimental results demonstrate the effectiveness of the framework: CNN achieves over 99% detection accuracy, outperforming existing methods on the same dataset. In addition, blockchain introduces an average latency of only 14 ms, while trust calculation requires approximately 3.6 ms. These findings indicate that the integration of IDS and TMS, supported by blockchain, provides a robust mechanism for accurate attack detection, secure trust evaluation, and immutable recording. The proposed framework, therefore, enhances the overall security posture of IoMT environments.

1. INTRODUCTION

New technologies moving from a physical phase to a digital phase have given rise to a new dimension in the management of patients' medical information. Internet of Things (IoT) systems, cloud, and other technologies aim to facilitate the management of data and services offered for both medical staff and patients. In this area of healthcare, security is a key pillar in terms of ethics and confidentiality. This cutting-edge system offers expanded proficiency and comfort; it also presents critical concerns with respect to framework security and potential vulnerabilities [1]. Actually, as mentioned in the study by Ibrahim et al. [2], more than 280 million individuals were influenced by miscellaneous cyberattacks, highlighting the need for continued monitoring and real-time activities.

To face these challenges, researchers are working on the reliability, accessibility, and confidentiality of medical information to ensure security in the health sector [3, 4]. With the frequency of data breaches and internal attacks existing in this sector, a proposal for a scientific approach is necessary to address internal and external vulnerabilities. At this level, the famous obstacle exists at the level of communication between end-user devices and monitoring devices. Several models have been proposed, based on firewalls, Intrusion Detection Systems (IDS) [5], and blockchain [6]. It is therefore necessary to develop a secure model to protect data in healthcare applications. To address these challenges, there are various approaches [3, 4, 7-9] that implement intrusion detection in the healthcare data transmission, using innovative intelligent techniques.

The most important issue in securing the medical environment is guaranteeing the trust of communications. To cater to those needs, we propose in this paper to assess trust based on several metrics, such as energy consumption and medical state. Nevertheless, computing several metrics is not sufficient when an attack may target the system. Therefore, we propose to implement trust management based on the intrusion detection process. The first step calculates the trust, then the intrusion detection module will implement the trust as a feature. Miscellaneous work relies only on trust assessment, which can be ineffective in the presence of anomalies related to attacks. Therefore, another security level is proposed to detect real-time attacks or abnormal behavior that may not be assessed by the trust score.

Our main motivations in this work are: (i) Merging different metrics types to compute trust level of medical context entities, (ii) Supervising not only the environmental characteristics but also the patients' data, (iii) Using an up-to-date dataset for the intrusion detection process and (iv) Ensuring systems traceability to explore the attackers' behavior and detect newer misbehaviors. These provided details can be used to build reports and move on to the forensics stage.

The remaining part of this paper introduces some related

works building the trust using intrusion detection, artificial intelligence (AI), and blockchain for different environments and especially for the medical environment. Section 3 details our approach and the different components describing the architecture. Section 4 presents the performance study of our approach with a comparative study. Finally, Section 5 concludes the paper with future work.

2. RELATED WORKS

Managed medical information collected from different patient sensors is sensitive and has to be secured against attacks. New technologies such as cloud architecture are used by doctors to guarantee data availability by storing duplicate data continuously. In fact, these new technologies are also subject to attacks targeting the medical sensitive data. Therefore, administrators deploy recent intrusion detection approaches based on deep learning (DL) algorithms that are developed by researchers. In this field, Khatun et al. [7] gave a fundamental overview of IoT in healthcare. They presented privacy and data security challenges associated with machine learning (ML) and healthcare IoT (H-IoT) devices. Moreover, they focused on monitoring IoT layers in this domain, such as network, perception, and cloud. This study examines the key aspects of cybersecurity, big data, e-health, and cloud computing in the context of H-IoT. It explores the application of ML techniques, including anomaly detection, device classification, and their critical and access control.

To trust the deployed system, several security requirements in the medical field have to be ensured, regarding the recorded data in the database and its transfer between patients and medical staff. To meet these challenges, some works [10] propose a reputation system deployment. Other works [11, 12] build trust using AI, whereas other works implemented blockchain-based health data.

2.1 Centralized trust-based approaches

We notice that some researchers focus on the trust of communications in different areas. In fact, Umashankar Ghugar et al. [13] presented an approach called Dual-Layer Trust Based IDS (DLTIDS). It is based on trust to counter Blackhole attacks, where two layers of defense are deployed. The first layer is about the evaluation of the behavior of the nodes thanks to the packet transfer rate, the calculations of trust, and the reliability at the level of communications. The second layer is based on the improvement of security via the indirect measures of trust. Remya et al. [14] developed a system called Trust-Based IDS for RPL (TIDSRPL). They aimed to decrease the risk of resource exhaustion via this strategic transfer that conserves energy, computing resources, and storage at the node level. It uses a hybrid trust model and heartbeat monitoring, offloading complex computations to the root node. It employs Subjective Logic, incorporating trust, distrust, and uncertainty for flexible attack detection. Key parameters include trust propagation and Fault Threshold to reduce false positives. It outperforms the default objective function, Minimum Rank with Hysteresis Objective Function-RPL (MRHOF-RPL), with a 33-45% improvement in energy efficiency and a 20-35% reduction in packet loss. It offers 45% better energy conservation during combined Selective Forwarding and Sinkhole attacks.

These works present IDS implementation, but they consider trust as a metric in the intrusion detection process. Added to that, the proposed system is centralized, so it is exposed to vulnerabilities and integrity attacks.

2.2 Blockchain-based trust approaches

To mitigate the centralization threats, several works adopted the decentralized blockchain technology. Indeed, Yang et al. [10] proposed a secure and efficient blockchain-based data sharing scheme for IoT. This system is based on an off-chain storage strategy and then performs on-chain indexing to meet the storage constraints in the blockchain, and uses a specific smart contract for the purpose of access control, secure querying, and sharing of data in IoT. At the data sharing process level, they incorporate a reputation mechanism. In addition, in this work, the system calculates the reputation of nodes and stores them in the blockchain via a smart contract. Any user announced as malicious is revoked.

To protect the HSN, Mutleg et al. [5] suggested a solution using Hyperledger blockchain to detect compromised Internet of Medical Things (IoMT) nodes and protect sensitive health information. They introduced a Clustered Hierarchical Trust Management System (CHTMS) designed to block malicious nodes. For securing health records, they use an embedded Elliptic Curve Cryptography (ECC), and they are interested in resistance against Denial of Service (DoS) attacks. About evaluation results, they indicate that integrating blockchain into the HSN enhances detection capabilities and outperforms current systems, demonstrating improved security and reliability compared to traditional databases. Bhan et al. [15] propose a Federated Friendly Learning (FCL) platform to ensure privacy in IoMT applications and secure data sharing. This study proposed a secure and collaborative federated Q-learning model, integrating a blockchain-certified trust mechanism, which strengthens data privacy by restricting participation to only authenticated nodes. This architecture is based on a multi-layer model combining (1) a blockchain infrastructure, (2) a dynamic trust mechanism, (3) a federated learning framework and (4) secure communication protocols. Regarding the results of this work, there is an increase in the accuracy levels equal to 94.7% and privacy protection equal to 92.4%.

Another use of the blockchain is proposed by Babu et al. [16]. They deploy blockchain technology to protect the confidentiality of patient information and to secure data exchange. Trust is guaranteed by smart contracts based on keys and certificates. The chain codes manage actors' authentication, registration, and verification. This also ensures chain traceability.

2.3 Intrusion detection-based approaches

In the related works on ML-enabled IDS for IoMT, a variety of innovative methodologies have been explored to improve feature selection and classification processes. The work presented by Ibrahim et al. [2] is based on a robust IDS for IoMT networks. It integrates a honeypot to divert attackers from critical systems and uses ML (K-Nearest Neighbor) to improve detection accuracy and resilience against cyberattacks. Researchers evaluated their models by testing two IoMT datasets, containing attacks such as Man-In-The-Middle (MITM), Data Injection, and Distributed Denial of Service (DDoS). The results are 92.5% and 99.54% for accuracy and 96.74% and 99.23% for precision across all

datasets, highlighting the potential of IDS to secure IoMT networks. In the same field, Sudharson et al. [17] implemented ML-IDS to increase the security of smart health applications (medical IoT) and patient information in the interconnected world. They used AdaBoost classifier, giving a recall value of 0.96. Their approach, tested on NSL-KDD dataset, focused on 12 features to achieve high performance in detecting DoS, User-to-Root (U2R), Root-to-Local (R2L), and Probe attacks. This system demonstrated superior accuracy, recall, and precision metrics. The study highlights the effectiveness of using adaptive ML models and optimized feature selection to enhance the security of interconnected medical devices, providing critical insights into the development of robust IoMT security frameworks.

Table 1. Comparison of the studied related work

Ref.	For Medical Environment?	Trust Metrics	Intrusion Detection Method	Deployed AI Algorithm	Evaluation Results of the AI	Deployed Blockchain (Type/ Name)
Trust-based Approaches						
[15]	Yes: IoMT: HSN	Sliding Time Window-based Trust Metrics, Direct and Indirect Trust, Cluster-based Trust	Lightweight SNORT IDS: Communication Component, Traffic Monitor and Blocklist	N.A.	N.A.	*) Private blockchain *) Hyperledger Fabric
[16]	Yes: IoMT	Smart contract-based registration, identification, and authentication	N.A.	N.A.	N.A.	*) Private blockchain *) Hyperledger Fabric
[10]	No: IoT	IoT users Feedback: Negative Ratings (NR) and Positive Ratings (PR)	N.A.	N.A.	N.A.	*) Private blockchain *) Ethereum: Ganache
[13]	No: WSN	Direct Trust and Indirect Trust (Watchdog Metrics)	Dual-Layer Trust-Based IDS for Blackhole Attacks	N.A.	N.A.	N.A.
[14]	No: RPL for LLNs	Subjective Logic (Trust, Distrust, and Uncertainty), Fault Threshold	Trust-Based Hybrid IDS with Heartbeat Monitoring	N.A.	N.A.	N.A.
[17]	Yes: IoMT	Interaction score between devices Penalization for malicious behavior	N.A.	N.A.	N.A.	*) Blockchain type not mentioned
AI-based Intrusion Detection Approaches						
[18]	Yes: IoT-based healthcare system	N.A.	Edge-based IDS with Multi-attack Detection	Dwarf Mongoose Optimized ANN (DMO-ANN)	Accuracy: 97.2%; Recall: 96.15%	*) Blockchain type not mentioned
[19]	Yes: IoMT	N.A.	Attacks Classification (like DoS, R2L, and U2R)	Naïve Bayes KNN AdaBoost	Best results with AdaBoost classifier: Recall = 96% Accuracy = 98.5%	N.A.
[9]	Yes: Medical data transmission	N.A.	weight function: WO-DBN: Weight-Optimized Deep Belief Network	LSTM + DNN	Best Accuracy rate = 98.6%	*) Blockchain + IPFS *) Type not mentioned
[2]	Yes: Smart healthcare systems	N.A.	Anomaly-based detection	Random Forest	92% accuracy in detecting unauthorized data access	N.A.
[20]	Yes: IoMT	N.A.	Attacks' Classification Architecture: The output of Base-learners is served as input to Meta-learner	Base-learners: MLP, CNN, and LSTM Meta-learner: ANN	$Acc_{IoTHealthcare-Security}$ = 99.95% $Acc_{WUSTL-EHMS-2020}$ = 99.65%	N.A.

Tyagi and Manju Bargavi [18] introduced a blockchain-based approach in their study, where they proposed a method called FIDANN, which is an intelligent intrusion detection mechanism. This method protects the confidentiality of medical information using Artificial Neural Networks (ANN) optimized by Dwarf Mongoose and uses a Federated Learning technique. This work used blockchain technology to save the updated model's weights. Thus, they guarantee integrity in a decentralized system. Actually, Kanna et al. [9] proposed an approach based on DL to secure medical information. In this

work, the data acquisition phase is done via online sources and then verified by the weight function (WO-DBN: Weight-Optimized Deep Belief Network). Regarding the security of medical data, the authors base their approach on chaotic map assisted encryption coupled with the optimal key generation of existing images in the database and blockchain technology. The final phase is about disease diagnosis, where the decrypted data are sent to classify the node with or without malicious intrusion. This phase is done via Res-LSTM + DNN: the support of a residual network (Resnet101), Long Short-Term Memory (LSTM), and the Deep Neural Network (DNN). In the validation part of this work, the accuracy rate of the approach is 98.6%. Another approach named SNN-IoMT (Stacked Neural Network Ensemble for IoMT Security) was proposed by Sun et al. [19]. It consists of an AI-based IDS framework designed to secure dynamic IoMT environments. This article is based on a DL architecture of STM, MLP (stacked combining multi-layer perceptron), and Convolutional Neural Network (CNN). It presents a model for optimizing data management and integration while ensuring system scalability and interoperability. The experiments are based on both IoTHealthcare-Security and WUSTL-EHMS-2020 datasets, providing respectively 99.95% and 99.65% accuracy.

Although the trust-based IDS demonstrates robust energy efficiency and enhanced security against various routing attacks, it is not without limitations. One notable challenge is its reliance on offloading computational tasks to the root node in high traffic scenarios. Furthermore, the effectiveness of the system depends on fine-tuning parameters, such as trust thresholds and Fault Threshold values, which may vary across network environments and require context-specific optimization. Moreover, as presented in Table 1, to ensure traceability, blockchain technology is used without focusing on IDS output, which may detect an attack that is not considered in the blockchain update, which is essential in the medical environment using sensitive data.

3. METHODOLOGY

3.1 Trust management

To overcome the limitations of existing trust-related works, we propose in this paper a trust-based management architecture deploying blockchain techniques for the medical environment. Indeed, the former deploys sensitive information, where human lives are impacted if the network is threatened. Thus, our main objective is tracking the user's behavior by monitoring all the components of the architecture. The monitoring consists of a trust-based assessment. However, this can also be attacked and modified. For this reason, we propose to use blockchain technology to guarantee the integrity of the stored information about the monitored component. In fact, to implement our solution, we base our study on a medical-based architecture, depicted in Figure 1.

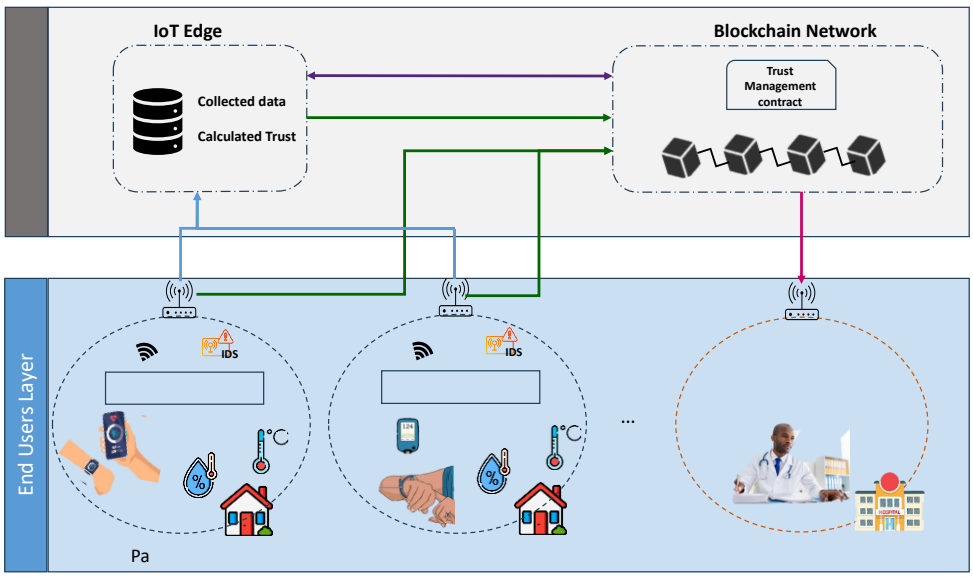


Figure 1. Proposed architecture based on blockchain

In fact, two actors are presented in the system: the medical staff and the patient. Trust ensures that the medical system accesses the data only if the environment is announced as trusted. The patient is surrounded by different sensors collecting miscellaneous data. It can be either a medical or an environmental sensor. Those sensors send periodically data to the Treatment Unit (TU) periodically, which in turn sends the processed data to the gateway. It also handles the needed calculations. Moreover, an IDS is installed in the environment to supervise the network.

The TMS proceeds through different stages to perform trust calculation and storage [20]. The first step is data collection, where different metrics are stored. After that, the collected data is used to calculate the trust before the propagation of this new trust.

In this proposed process, following the flowchart of Figure 2, the following steps are executed:

Step 1: User U requests a connection to the network to have remote medical control.

Step 2: The gateway activates continuous monitoring (Intrusion detection process and trust-related data storage), and it processes immediately to the trust calculation using a set of parameters and the output of the IDS.

Step 3: If the trust calculation procedure is done, the gateway checks if the device is always allowed. In parallel, we should launch the write action in the blockchain to ensure traceability. This action is a transaction that generates a transaction hash. This hash will be the link between trust and

the related transaction.

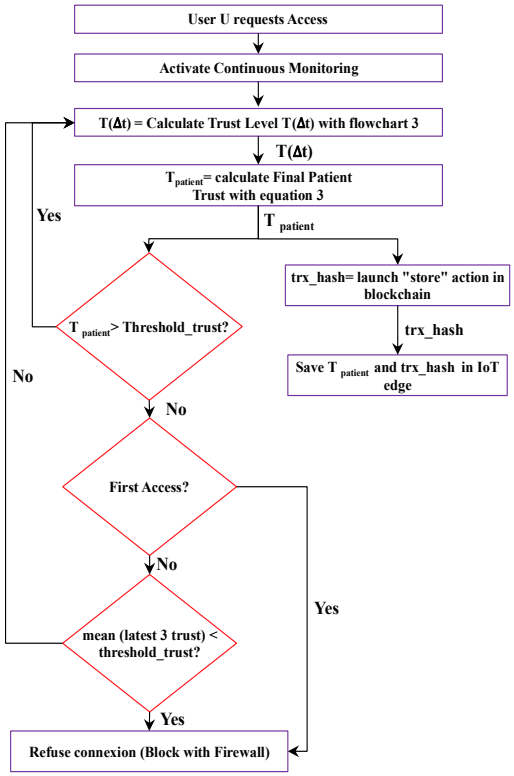


Figure 2. System's general algorithm

Step 4: If the obtained trust is higher than the trust threshold, then

Step 4.1: The user, either a new patient or an old one, is allowed to access the system and we continue the monitoring and the calculation.

Step 5: Otherwise,

Step 5.1: if it is his first access, then it is rejected and reported as a non-trustworthy entity.

Step 5.2: If not, then the gateway checks the average of the last three trust scores. The objective here is to check whether the trust score dropped out for just one instance, or the behavior is degrading.

Step 5.2.1: If the behavior persists and the average does not attain the threshold, then the user is refused and added to the firewall's blacklist.

Step 5.2.2: Else, the user is kept in the system, and the gateway continues the trust calculation process.

We detail in the following the main modules in the considered architecture of Figure 1.

3.1.1 Data collection

In our network, there are environmental sensors and medical sensors, capturing different types of data. Since we aim to ensure more trust, we monitor each sensor to obtain our trust metrics.

For continuous monitoring, at each time interval, the gateway receives information from both sensors and IDS. Then, the CIC-flow meter will be applied to the data to get statistical output. Next, our DL model is applied to obtained output to get the attack probability. Added to that, the collected values from medical sensors are supervised with the energy consumption rate and the Packet Delivery Ratio (PDR). Thus, we have all the needed information to perform trust calculation. The IoT edge computing will take the computation task. Once trust is calculated, it will be stored in the blockchain network and on the IoT edge.

3.1.2 Trust calculation

After data collection by the gateway, trust metrics are pretreated and then used in the trust calculation process. Data treatment and the trust calculation are executed as described in the published articles [21, 22]. The used metrics are direct observations obtained in our network. In fact, each device reports the energy consumption e and eventually medical data to the gateway. Medical data is one of the trust indicators associated with the trust value T_{med}. T_{med} represents an indication of anomalies in the medical data. Moreover, energy consumption is another indicator supervising if there is any suspicious behavior depleting resources. It reflects the energy consumption rate of all existing sensors. This metric is selected to tackle attacks like DoS in the physical layer.

Also, we calculate the ratio between received packets and total sent packets, called PDR. Then, the gateway calculates trust based on energy consumption e, PDR, and medical data trust T_{med} as proposed in the paper [21]. It is important to highlight that each feature is bounded between 0 and 1. To increase the precision of the trust level, we propose adding the IDS decision as a trust feature, as described in Figure 3.

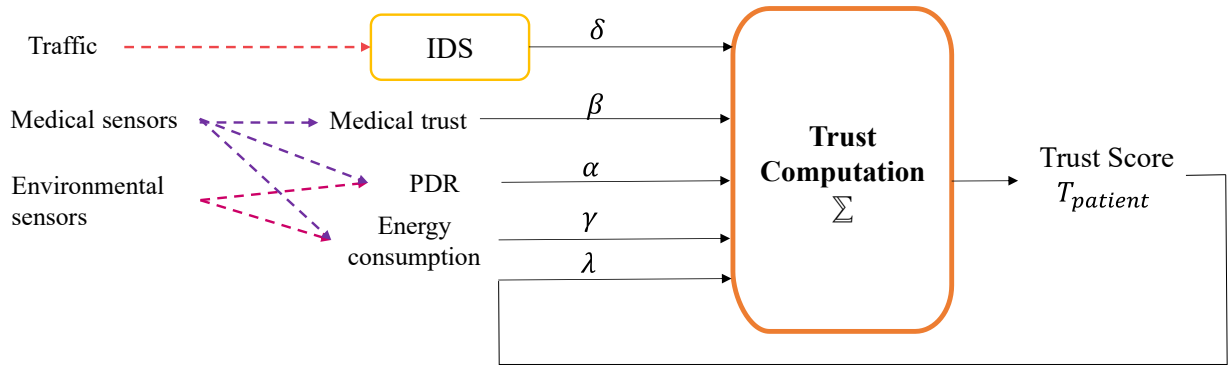


Figure 3. Trust calculation

The proposed intrusion detection mechanism is based on AI by training the model. The output of the model is the attack probability p. If the probability is high (upper than a threshold defined by the administrator), it reflects a danger to our system. So, the related attribute should reflect the non-trust, as considered in Eq. (1).

$$T_{IDS} = 1 - p \quad (1)$$

3.1.3 Trust update

At each time interval Δt, the gateway calculates the trust for this current interval Δt. The obtained trust will not be the adopted trust for the network. Otherwise, it will be integrated into a weighted sum to bring attention to the old trust, since we assume that the node's behavior cannot vary suddenly. Each interval Δt, a trust calculation is proceeded. The gateway collects data and calculates current trust using Eq. (2).

$$T(\Delta t) = \alpha * PDR + \beta * T_{med} + \gamma * e + \delta * T_{IDS} \quad (2)$$

The network trust follows Eq. (3) by taking into consideration that the weights $\lambda < \mu$, $\lambda + \mu = 1$ and $\lambda <= 0.4$, as we aim to prioritize the new trust value.

$$T_{patient} = \lambda T(\Delta(t-1)) * \mu T(\Delta t) \quad (3)$$

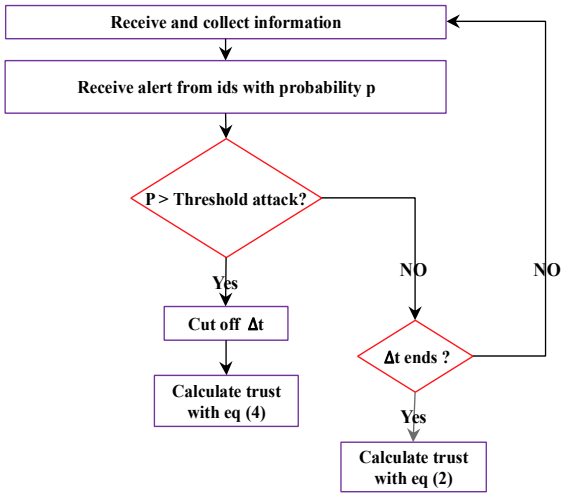


Figure 4. Trust update further to attack detection

If an intrusion alert is generated during the time interval, the gateway instantly calculates a new trust, as explained in Figure 4. This calculation is based on the attacks' probability. In fact, if we get a probability of attack p more than a predefined threshold, the current trust is updated as indicated in Eq. (4). The new trust will be recalculated according to Eq. (3). The thresholds in our system are defined and fitted by the network administrator.

$$T(\Delta t) = T_{IDS} \quad (4)$$

3.1.4 Trust propagation

To share the trust score between entities, we used the blockchain network. The node connected to the blockchain can execute two different functions: the "set" function to change the ledger and the "get" function to retrieve the trust value. Thus, to preserve the new score, the gateway will invoke the update function with the new score and features.

To ensure more access speed, we propose having a database storage on the IoT Computing edge. At each time interval, Δt, the information will be stored in the database. If the trust value is deemed significant—such as a notable increase or decrease, or a value exceeding a predefined trust threshold—it will also be recorded on the blockchain. This update will be associated with the corresponding transaction hash for traceability data stored on the edge, which will be verified periodically to ensure information integrity and conformity to the blockchain to avoid or detect alteration.

3.2 Blockchain-based trust

To ensure more security and traceability, we opted for a blockchain network to store trust variations. We choose a private blockchain to guarantee the privacy of the medical environment. To access the blockchain, every entity should be connected to a blockchain node as described in Figure 5.

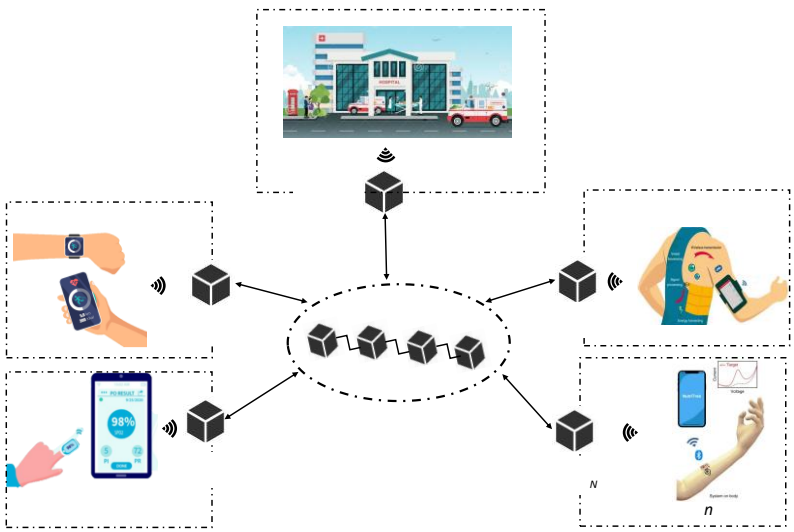


Figure 5. Blockchain architecture

In our architecture, every node is the member's gateway. The member is either a patient or a medical institution. If an entity does not have a node in the blockchain, a new node is created. The used blockchain will be a private blockchain since we are dealing with a medical context.

To manage the trust updates, a smart contract is used. Every operation is traced in the blockchain via this smart contract. This smart contract will allow every node to either update or retrieve the appropriate trust score. The update function allows every patient side to update the trust value, and the retrieve function permits both the edge and the medical side to get the trust value assigned to the patient.

The distributed ledger will track down every transaction which will be structured in blocks approved by the validators. Each block can contain one or more transactions. The transaction includes many fields indicating information relative to the update trust function. In fact, each transaction is defined by a "transaction hash". The sender is defined by the gateway aiming to upload the new trust value. It is presented by the patient's address account. The destination field will contain, in our case, the contract address since we are invoking methods from it. Regarding the data, it englobes the encoded form of the invoked function and the given parameters.

3.3 Detection module

The IDS accepts analyzed traffic and detects if there are any intrusions that may cause instability in the system. The anomaly-based IDS aims to detect suspicious behavior based on ML. In fact, the IDS is trained on the network normal behavior. A deviation from the normal baseline is accounted as an attack. Indeed, learning-based IDS tailored for medical settings is proposed to enhance security by identifying threats while minimizing disruptions. Continuous monitoring and real-time intrusion detection have to be ensured because of the sensitivity of medical data. It is also designed to detect abnormal behavior of the user and the device, as well as unauthorized access to the medical records by patients and medical staff.

Table 2. CNN parameters

Parameters	Value
Convolutional layers number	3
Activation function	ReLU
First dropout layer rate	0.2
Second dropout layer rate	0.3

For that, we propose applying DL, where we go through four phases: data preprocessing, building the proposed model, applying the model on training and validation data, and finally applying the model on the test data. Data preprocessing consists of 1) selecting and building the dataset, 2) selecting pertinent features, 3) One Hot encoding and 4) features scaling.

When the data is ready, we focus on building a CNN model. This model consists of both Convolutional layers and fully connected layers. Also, it englobes 3 Batch normalization layers. Added to that, we introduced 2 dropout layers to avoid overfitting and pooling layers, helping to minimize the computational complexity. The output layer uses the activation function sigmoid since we are performing binary classification. The used parameters are explained in Table 2.

4. RESULTS AND DISCUSSION

The simulation environment is a Virtual machine with the operating system Ubuntu 20.04. The virtual material of the virtual machine is: 8 vCPU and 16 GB of RAM. In the following, we will describe the evaluation of each part of our system.

4.1 AI-based IDS

4.1.1 Dataset description

We trained and tested our model on the CIC-IoMT2024 dataset [23]. This dataset is produced in a real environment with a miscellaneous type of sensors (healthcare sensors, home devices…) established by the Canadian Institute for Cybersecurity. Also, different protocols are used in the collected data, such as Bluetooth and Wi-Fi. The collected traffic contains benign and malicious flows. Malicious traffic contains mainly five attack families: recon, spoofing, DoS, DDoS, and malformed data.

We propose to deploy our IDS on this dataset. We have chosen to perform different classifications as Table 3 details. The benign and the recon traffic contain varied protocols. The Denial-of-Service Traffic was parsed into either MQTT or TCP/IP protocol.

Table 3. Selected dataset description

Attack	Protocol		
Benign		Any	
Spoofing		ARP	
Recon		Any	
DoS	MQTT	TCP/IP:	ICMP TCP/SYN UDP
DDoS	MQTT	TCP/IP:	ICMP TCP/SYN UDP

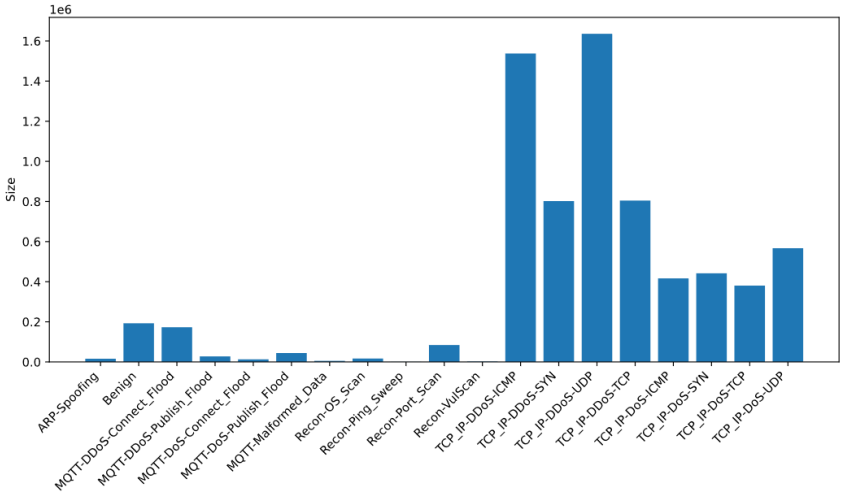


Figure 6. Class distribution in training dataset

The proposed dataset separates training data from test data. Thus, we trained our model on the training dataset, and then the test phase uses the provided test dataset. Our model is executed on the train files provided by the Canadian Institute for Cybersecurity. We split the file into 70% train and 30% validation. Then, to evaluate our model, we test it on the offered test files. The distribution of different classes' instances in the provided train data is illustrated in Figure 6.

4.1.2 Evaluation metrics

To evaluate a model, numerous metrics exist apart from accuracy. To extend our approach study, we focus on: confusion matrix (CM), precision, recall, and F1-score [24, 25].

Confusion matrix (CM): In the CM: Rows, reflect actual classes marked True and False. As for columns, they present predicted values. If the prediction is correct, it is considered Positive. Otherwise, it is Negative. This matrix is summarized in Eq. (5).

$$\mathrm{CM} = \begin{matrix} TP & FP \\ FN & TN \end{matrix} \tag{5}$$

where,

TP: True Positive: information correctly detected as attack.

FP: False Positive: incorrectly detected benign as attack.

FN: False Negative: incorrectly classified attacks as benign.

TN: True Negative: benign information correctly classified.

Accuracy (ACC): The Accuracy metric is measured by the proportion of correctly classified observations (both TP and TN) out of the total observations. This metric is represented by Eq. (6).

$$ACC = \frac{(TN + TP)}{(TN + TP + FP + FN)} \tag{6}$$

Precision: This metric considers the samples classified as positive. It presents the correctly classified positive samples percentage to both TP and FP. This metric is presented by Eq. (7).

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

Recall: It evaluates the effectiveness of a model to correctly identify all labels. It is presented by Eq. (8).

$$Recall = \frac{TP}{TP + FN} \tag{8}$$

F1-score: The F1-score is the average of the precision presented by Eq. (7) and the recall obtained by Eq. (8). This parameter provides a balance between recall and precision. It is detailed in Eq. (9).

$$F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{9}$$

4.1.3 Model results

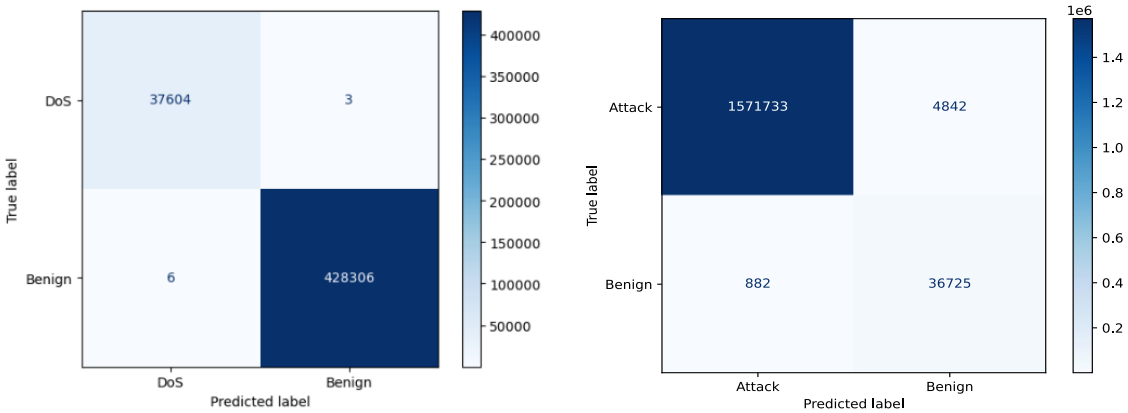
After selecting the dataset, we initiated the learning process through creating the DL model described earlier, based on CNN. We trained and tested the model using three different class distributions, detailed in Figure 7 alongside other existing distributions. The first distribution is Boolean, classifying traffic as either benign or DoS. The second includes an additional attack type: reconnaissance (recon). The third distribution treats each category separately, encompassing 19 classes in total—benign plus 18 distinct attack types. Due to the large size of the dataset and limitations of our hardware, we reduced the amount of data related to DoS and DDoS attacks during training.

Category	Attack	Classes distribution				
		2 classes	2 classes ours	6 classes	3 classes ours	19 classes
Benign	-	BENIGN	BENIGN	BENIGN	BENIGN	BENIGN
Spoofing	ARP Spoofing	ATTACK	-	SPOOFING	-	ARP SPOOFING
Recon	Ping sweep		-	RECON	RECON	Ping sweep
	Recon VulScan		-			Recon VulScan
	OS scan		-			OS scan
	Port scan		-			Port scan
MQTT	Malformed data		-	DDOS	-	Malformed data
	DoS connect flood		DOS		DOS	DoS connect flood
	DoS publish flood					DoS publish flood
	DDoS publish flood		-		-	DDoS publish flood
	DDoS connect flood		-		-	DDoS connect flood
DoS	DoS ICMP		DOS	DOS	DOS	DoS ICMP
	DoS UDP					DoS UDP
	DoS TCP					DoS TCP
	DoS SYN					DoS SYN
DDoS	DDoS ICMP		-	MQTT	-	DDoS ICMP
	DDoS UDP		-		-	DDoS UDP
	DDoS TCP		-		-	DDoS TCP
	DDoS SYN		-		-	DDoS SYN

Figure 7. Different proposed distributions

In the 2-class and 3-class classification scenarios, accuracy exceeds 99%, achieving 99.6% and 99%, respectively. However, in the 19-class classification, accuracy drops to 73%. To better understand these results, we analyzed the confusion matrices shown in Figures 8, 9 and 10. In the binary classification, the number of false positives (FP) and false negatives (FN) remain very low relative to the overall traffic.

In the multi-class setting, confusion occurs primarily between benign traffic and both ARP spoofing and reconnaissance attacks. This is due to certain features that are not sufficiently discriminative for these classes but are important for distinguishing DoS attacks. Moreover, these types of attacks do not alter the system's state, making them harder to detect [25]. Additional confusion is observed within the DoS traffic, particularly between TCP-IP and MQTT traffic, as they exhibit similar behaviors.



(a) Benign and DoS (b) Benign and attack

Figure 8. 2 Classes' confusion matrix

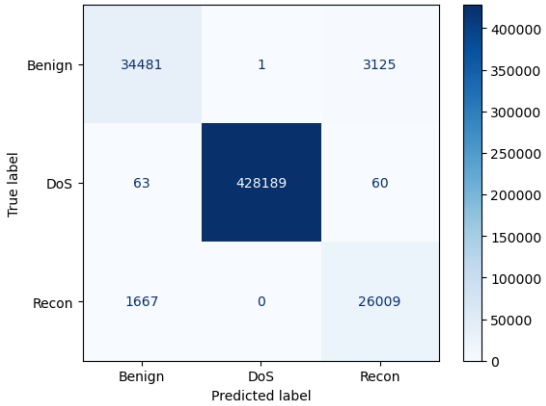


Figure 9. Confusion matrix for 3 classes' classification

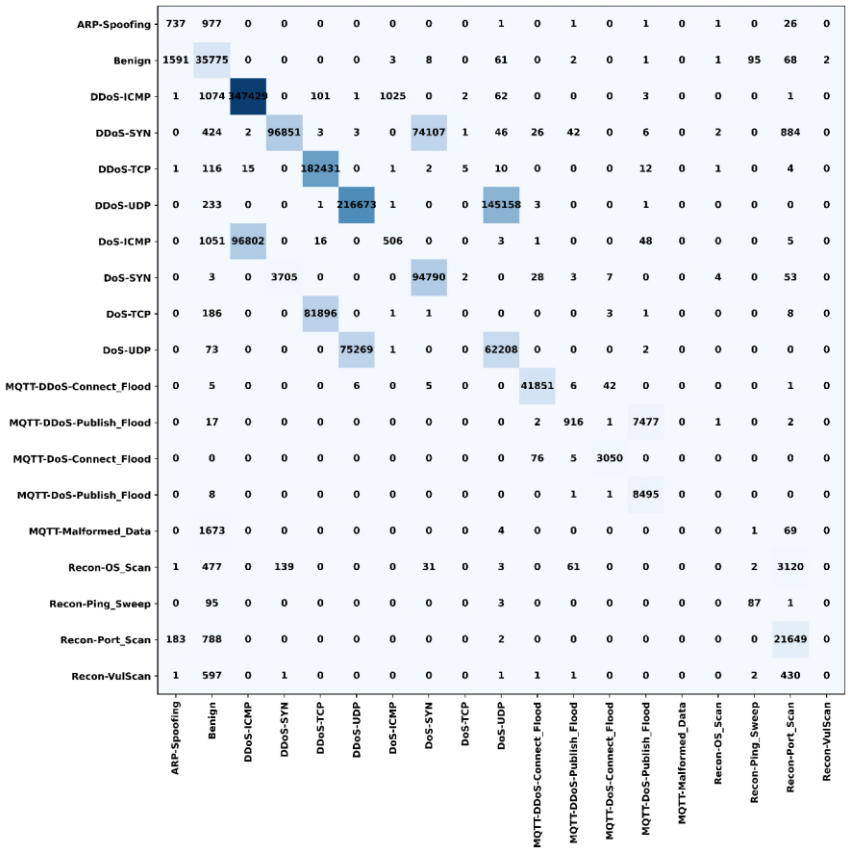


Figure 10. Confusion matrix for 19 classes

4.1.4 Comparison of classification results

Table 4 summarizes classification results across different studies, which mainly follow two common class distributions. The first is a binary classification setting, where [21, 26, 27] categorize data into benign and attack classes, achieving accuracies of 99.6%, 97%, and 99.92%, respectively. Our model outperforms accuracies reported in the previous studies [21, 26], while remaining consistent with the study by Hafid et al. [27]. The second setting involves a 19-class distribution, used in the previous studies [21, 26], where they achieved accuracies of 73.3% and 87.96%, respectively. Our model attains comparable accuracy to the study by Fourati et al. [21]; however, Mezina et al. [26] reported superior results due to their use of a hybrid model that incorporates deeper and more complex learning architectures. In contrast, we introduced a novel 3-class distribution with a different class split. Using our CNN model under this setup, we achieved an accuracy of 99%, a Recall of 95.21%, a Precision of 94.77%, and an F1-score of 94.77%. The relatively lower F1-score can be attributed to class imbalance within the training dataset.

Table 4. Comparative results

Classes Number	Classes	Ref.	Algorithm	Accuracy (%)	Recall (%)	Precision (%)	F1-Score (%)
2	Benign, Attack	[23]	RF	99.6	95.1	97.1	96.1
			AdaBoost	99.6	96.1	95.9	95.9
		[26]	DNN	99.6	94.8	95.6	95.2
			UNet++ +LSTM	99.92	99.84	99.99	99.92
		[27]	XGBoost	97	100	96	98
		Ours	CNN	99.64	98.67	94.14	96.29
3	Benign, DoS	Ours	CNN	99.99	99.99	99.99	99.99
	Benign, Recon, DoS	Ours	CNN	99	95.21	94.77	94.95
6	Benign, Recon, spoofing, DDoS, DOS, MQTT	[23]	RF	73.5	71.3	73.5	67.6
			Logistic regression	72.9	71.2	74.8	69.4
19	Each attack separately	[23]	RF	73.3	57.7	69.1	55.1
		[26]	UNet++ +LSTM	87.96	93.31	94.55	86.47
		Ours	CNN	73.59	51.85	56	48.34

4.2 Blockchain configuration

The chosen blockchain network is the permissioned blockchain GoQuorum. It represents an open-source Ethereum-based blockchain. This blockchain is a real blockchain that can be implemented in a production environment. It proposes different consensus algorithms: Raft, IBFT, and QBFT. The selected consensus algorithm is RAFT, as it offers rapidity. After the installation of Geth (Go Ethereum) proposed by GoQuorum, we proceeded with the creation of the blockchain network, specifying the initial node's number and the consensus algorithm. Our GoQuorum blockchain network is formed by 5 nodes using the Raft consensus algorithm. A node is defined by an IP address and a port where the service is running.

We prepared the script of our smart contract and then compiled it. As a result, we have the ABI and the bytecode distinguishing the contract. We then deployed our smart contract to the blockchain network using the Ethereum library web3 via the Application Programming Interface (API) JSON-RPC [28]. This API allows our program to make calls with the Ethereum client. Once the contract is deployed, a contract address is generated to identify our contract and make interaction with it possible. This is a primordial action so that our nodes update the trust level. After accomplishing these requirements, every node can establish the actions' call.

4.3 Delay-based evaluation

Our system contains different computational operations: prediction operation, trust calculation, and transaction publishing in a blockchain network. We propose to study the computational time of those main operations in Table 5.

In the gateway, when the system is about to update the trust, we have two main operations namely prediction and the update. The old trust recuperation is from the IoT edge and not from the blockchain. Thus, the trust calculation will be equal to 0.0036 seconds. Compared to prediction and trust calculation, the process, including blockchain communication, is higher. However, it does not affect our system performance since it does not depend on direct communication with the blockchain but rather on the IoT edge. Additionally, trust modification will only be triggered when a notable change in the trust score is detected. Minor variations or unchanged trust levels will not be recorded on the blockchain in order to minimize processing time.

Table 5. Time-based evaluation

Operation		Time (s)
Prediction		0.1117
Trust calculation		0.0036
Blockchain operations	Store	1.04
	Retrieve	1.03
	Contract deployment	1.05

4.4 Comparative study

In this section, a comparative study is established between our work and Yang et al's work [10]. They present an approach in an IoT environment with the deployment of trust based on blockchain. Table 6 details the simulation environments.

First, we tried to compare the reputation evolution. The authors presented the effect of the NR and PR decrease on their reputation score. We will present our reputation progress with values variating in PDR, Energy consumption, and medical trust, and with modifying in each time period the attack probability. We fitted updated weights as follows: $\lambda = 0.3$ and $\mu = 0.7$. Regarding weights of metrics: α, β, and γ equal 0.2 while $\delta = 0.4$.

The first curve in Figure 11, having PR equal to 5 with no NR, is increasing. Our approach has different attributes and uses the IDS decision in calculating trust. We obtain a decrease in trust when the attack probability increases. In fact, the

probability p starts with a value of 1 in instant $\Delta t = 0$, but when it becomes p = 0, we find that the trust value is under the trust threshold fixed by Yang et al. [10]. Added to that, the last three occurrences in the curve have values inferior to the threshold. As a result, following our proposed algorithm, this node is rejected from the network.

Table 6. Test environment comparison

Parameters	Ref. [10]	Ours
Trust metrics	NR: negative ratings number PR: positive ratings number	PDR, Energy, Medical-related trust, and Attack probability
Used blockchain	Ganache (Ethereum)	GoQuorum (Ethereum-based)
Web3 library	Web3.py	Web3.js
Environment	Virtual machine: Ubuntu	
VM configuration	RAM: 4 GB 8 vCPU 2.30GHZ	RAM: 16 GB 8 vCPU 2.99 GHZ

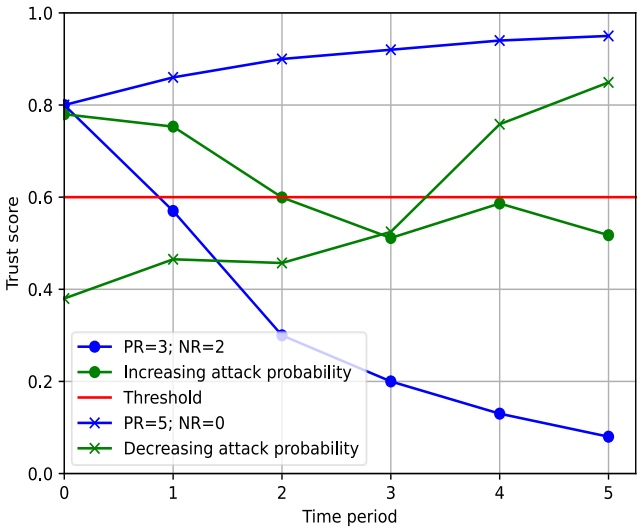


Figure 11. Trust score variation

Second, we moved forward to the blockchain evaluation. We tested the write transaction latency, where we tested the different delays when the transaction number per second varies. The work by Yang et al. [10] used ganache in simulation, representing one node (defined by an IP address and a port). To get a fair comparison, we fix our test on one node in the GoQuorum blockchain. The latency chart in Figure 12 shows that our blockchain network returns an increasing latency value proportionally to the transaction rate as proposed in the paper. Compared to other processes in our approach, the latency value remains acceptable and ensures the rapidity of the transaction process.

Added to that, we evaluated the trust update throughput values as illustrated in Figure 13. In Figure 13(a), we represented the throughput of our blockchain. Throughput, expressed in Transaction Per Second (TPS), is defined as the average number of correctly handled transactions according to received transaction flow per second [28].

In fact, as the number of transactions increases, the throughput rises accordingly. For comparison purposes, we selected a specific window from our performance curve to use in the comparison analysis with the Yang et al's [10] throughput values in Figure 13(b). The Value remains acceptable since it does not exceed 30 TPS.

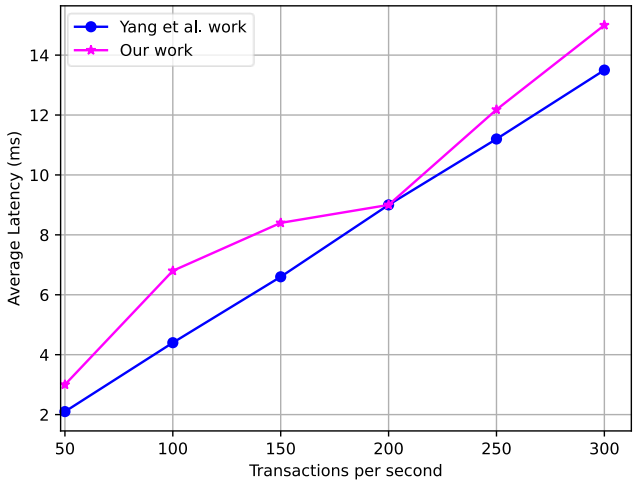
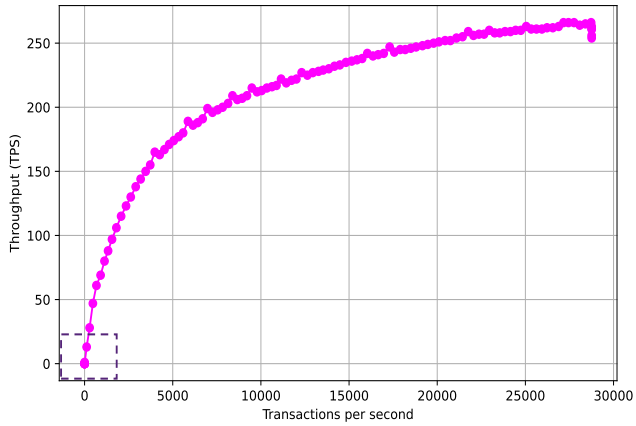
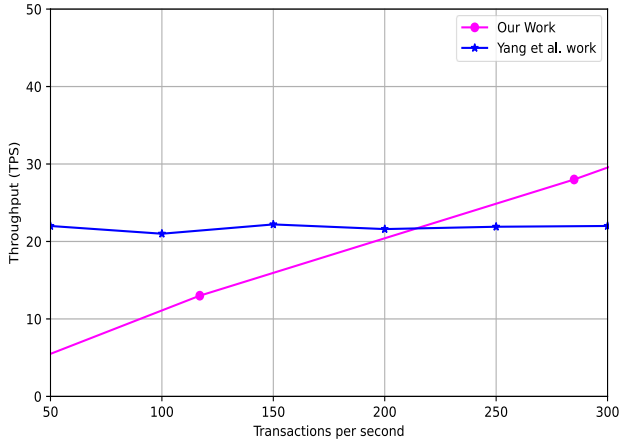


Figure 12. Write transactions latency



(a) Our system's throughput



(b) Throughput comparison

Figure 13. Throughput comparison for updating trust

To evaluate blockchain throughput, we conducted multiple tests, each varying the number of threads. In this context, a thread represents a user interacting with the blockchain. As the number of threads increases, the volume of transactions rises proportionally. As illustrated in Figure 14, the throughput curves exhibit an upward trend, indicating that the throughput improves with higher transaction rates. This demonstrates GoQuorum's capability to efficiently handle a high volume of transactions. For instance, with three concurrent users, the throughput peaks at a maximum of 480 TPS.

To summarize, our trust model maintains a level of security

since it always controls the network, and the trust score reflects the degree of network reliability. Moreover, the permissioned blockchain network is a real network that can be upgraded to a production environment. It offers an average latency of 9.06 ms and a throughput attaining 260 TPS for a high transaction volume.

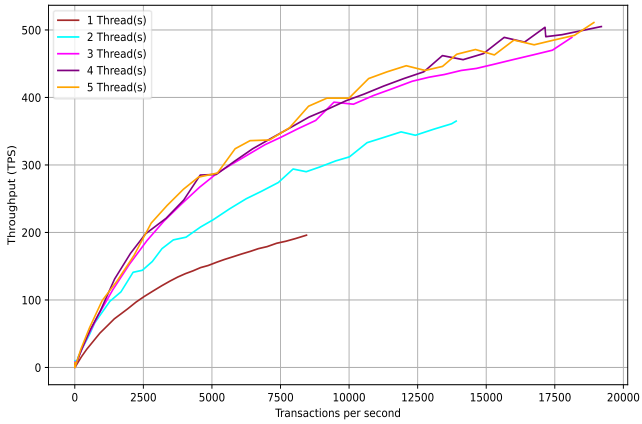


Figure 14. Throughput variation

5. CONCLUSIONS

This study presents a trust architecture for the IoMT, designed to enhance security, reliability, and traceability in medical IoT environments. The proposed framework integrates an IDS with a TMS, where each entity in the network is assigned a dynamic trust score reflecting its behavior and reliability. To ensure secure and tamper-proof record keeping, blockchain technology is employed, providing transparency, accountability, and immutable traceability of all trust-related operations.

The evaluation of the trust computation demonstrates that the proposed system efficiently reflects the reliability of entities, with minimal computation time. Any decline in performance metrics or anomalies detected by the IDS yields a proportional decrease in trust score, ensuring that the system accurately represents entity behavior over time. The IDS is implemented using a CNN trained on CIC-IoMT 2024 dataset. It achieves classification accuracy exceeding 99% in binary tasks, outperforming existing methods and demonstrating the effectiveness of DL for real-time attack detection.

Blockchain integration was evaluated in a realistic deployment using GoQuorum, showing low latency (14 ms for 300 TPS) and the ability to handle high transaction rates from multiple users, confirming the practical applicability of the system in production environments.

Overall, this research demonstrates that combining IDS-based trust management with blockchain technology provides a comprehensive and effective approach to foster the security posture of medical IoT networks.

At this stage of analysis, we would assert that this research can be regarded as valuable and promising in terms of laying the ground for fruitful lines of investigation and paving the way for new research directions. Indeed, further research is needed to focus on boosting blockchain capabilities, particularly through smart contracts to automate key security functions such as access control and authentication. Additionally, full-scale deployment in a real IoMT environment is planned to further assess system robustness, scalability, and resilience against sophisticated attacks.

REFERENCES

[1] Mutleg, M.L., Mahmood, A.M., Al-Nayar, M.M.J. (2024). A comprehensive review of cyber-attacks targeting IoT systems and their security measures. International Journal of Safety and Security Engineering, 14(4): 1073-1086. https://doi.org/10.18280/ijsse.140406

[2] Ibrahim, M., Al-Wadi, A., Elhafiz, R. (2024). Security analysis for smart healthcare systems. Sensors, 24(11): 3375. https://doi.org/10.3390/s24113375

[3] Kaliappan, C.P., Palaniappan, K., Ananthavadivel, D., Subramanian, U. (2024). Advancing IoT security: A comprehensive AI-based trust framework for intrusion detection. Peer-to-Peer Networking and Applications, 17(5): 2737-2757. https://doi.org/10.1007/s12083-024-01684-0

[4] Anand, M., Kumar, S.P., Selvi, M., Kumar SVN, S., Ram, G.D., Kannan, A. (2023). Deep learning model based IDS for detecting cyber attacks in IoT based smart vehicle network. In 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, pp. 281-286. https://doi.org/10.1109/icscds56580.2023.10104996

[5] Mutleg, M.L., Mahmood, A.M., Al-Nayar, M.M.J. (2024). Deep learning based intrusion detection system of IoT technology: Accuracy versus computational complexity. International Journal of Safety and Security Engineering, 14(5): 1547-1558. https://doi.org/10.18280/ijsse.140522

[6] Kumarswamy, S., Sampigerayappa, P.A. (2024). A review of blockchain applications and healthcare informatics. International Journal of Safety and Security Engineering, 14(1): 267-287. https://doi.org/10.18280/ijsse.140127

[7] Khatun, M.A., Memon, S.F., Eising, C., Dhirani, L.L. (2023). Machine learning for healthcare-IoT security: A review and risk mitigation. IEEE Access, 11: 145869-145896. https://doi.org/10.1109/access.2023.3346320

[8] Edo, O.C., Ang, D., Billakota, P., Ho, J.C. (2023). A zero trust architecture for health information systems. Health and Technology, 14(1): 189-199. https://doi.org/10.1007/s12553-023-00809-4

[9] Kanna, S.K.R., Murthy, M.Y.B., Gawali, M.B., Rubai, S.M., Reddy, N.S., Brammya, G., Preetha, N.S.N. (2024). A deep learning-based disease diagnosis with intrusion detection for a secured healthcare system. Knowledge and Information Systems, 66(9): 5669-5707. https://doi.org/10.1007/s10115-023-02030-1

[10] Yang, W., Hou, C., Zhang, Z., Wang, X., Chen, S. (2024). Secure and efficient data sharing for IoT based on blockchain and reputation mechanism. IEEE Internet of Things Journal, 11(11): 20631-20647. https://doi.org/10.1109/jiot.2024.3371063

[11] Bajpayi, P., Sharma, S., Gaur, M.S. (2024). AI driven IoT healthcare devices security vulnerability management. In 2024 2nd International Conference on Disruptive Technologies (ICDT), Greater Noida, India, pp. 366-373. https://doi.org/10.1109/icdt61202.2024.10488939

[12] Perivolaris, A., Adams-McGavin, C., Madan, Y., Kishibe, T., Antoniou, T., Mamdani, M., Jung, J.J. (2024). Quality of interaction between clinicians and artificial intelligence systems. A systematic review. Future Healthcare Journal, 11(3): 100172.

https://doi.org/10.1016/j.fhj.2024.100172
[13] Ghugar, U., Dash, S., Jena, S., Swain, N.K., Brahma, B., Sahoo, S.K. (2024). DLTIDS: A dual-layer trust-based intrusion detection system for blackhole attacks in wireless sensor networks. Nanotechnology Perceptions. Advance online publication. https://doi.org/10.62441/nano-ntp.vi.996
[14] Remya, S., Pillai, M.J., Arjun, C., Ramasubbareddy, S., Cho, Y. (2024). Enhancing security in LLNs using a hybrid trust-based intrusion detection system for RPL. IEEE Access, 12: 58836-58850. https://doi.org/10.1109/access.2024.3391918
[15] Bhan, R., Pamula, R., Faruki, P., Gajrani, J. (2023). Blockchain-enabled secure and efficient data sharing scheme for trust management in healthcare smartphone network. The Journal of Supercomputing, 79(14): 16233-16274. https://doi.org/10.1007/s11227-023-05272-6
[16] Babu, E.S., Yadav, B.V.R.N., Nikhath, A.K., Nayak, S.R., Alnumay, W. (2022). MediBlocks: Secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. Cluster Computing, 26(4): 2217-2244. https://doi.org/10.1007/s10586-022-03652-w
[17] Sudharson, K., Babu, G., Santhiya, R., Anita, C.S. (2025). Enhanced privacy-preserving federated convivial learning for Internet of Medical Things (IoMT) through blockchain-enabled trust Q-learning. Journal of the National Science Foundation of Sri Lanka, 52(4): 501-514. https://doi.org/10.4038/jnsfsr.v52i4.11923
[18] Tyagi, P., Manju Bargavi, S.K. (2023). Using federated artificial intelligence system of intrusion detection for IoT healthcare system based on blockchain. International Journal of Data Informatics and Intelligent Computing, 2(1): 1-10. https://doi.org/10.59461/ijdiic.v2i1.42
[19] Sun, Z., An, G., Yang, Y., Liu, Y. (2024). Optimized machine learning enabled intrusion detection system for internet of Medical Things. Franklin Open, 6: 100056. https://doi.org/10.1016/j.fraope.2023.100056
[20] Benmalek, M., Seddiki, A., Haouam, K.D. (2025). SNN-IoMT: A novel AI-driven model for intrusion detection in Internet of Medical Things. Computer Modeling in Engineering & Sciences, 143(1): 1157-1184. https://doi.org/10.32604/cmes.2025.062841
[21] Fourati, M., Meddeb-Makhlouf, A., Zarai, F. (2023). Blockchain-based trust management for IoMT environment. In Lecture Notes in Computer Science (pp. 149-162). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-49737-7_11
[22] Fourati, M., Meddeb-Makhlouf, A., Zarai, F. (2025). Access control based on trust and blockchain for IoMT. Procedia Computer Science, 270: 3934-3942. https://doi.org/10.1016/j.procs.2025.09.518
[23] Dadkhah, S., Neto, E.C.P., Ferreira, R., Molokwu, R.C., Sadeghi, S., Ghorbani, A.A. (2024). CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT. Internet of Things, 28: 101351. https://doi.org/10.1016/j.iot.2024.101351
[24] Sokolova, M., Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. Information Processing & Management, 45(4): 427-437. https://doi.org/10.1016/j.ipm.2009.03.002
[25] Kamoun-Abid, F., Frikha, H., Meddeb-Makhoulf, A., Zarai, F. (2024). Automating cloud virtual machines allocation via machine learning. Indonesian Journal of Electrical Engineering and Computer Science, 35(1): 191-202. https://doi.org/10.11591/ijeecs.v35.i1.pp191-202
[26] Mezina, A., Nurmi, J., Ometov, A. (2025). Novel hybrid UNet++ and LSTM model for enhanced attack detection and classification in IoMT traffic. IEEE Access, 13: 57589-57603. https://doi.org/10.1109/access.2025.3553966
[27] Hafid, A., Rahouti, M., Aledhari, M. (2025). Optimizing intrusion detection in IoMT networks through interpretable and cost-aware machine learning. Mathematics, 13(10): 1574. https://doi.org/10.3390/math13101574
[28] Taherpour, A., Wang, X. (2025). A high-throughput and secure coded blockchain for IoT. IEEE Transactions on Dependable and Secure Computing, 22(4): 3561-3579. https://doi.org/10.1109/tdsc.2025.3532850

NOMENCLATURE

e	associated trust to the sensors' energy consumption
PDR	Packet Delivery Ratio
T_{med}	trust related to medical signal
Δt	time interval (window)
p	attack probability issued from the deep learning model
T_{IDS}	IDS trust
$T(\Delta t)$	current trust value calculated for the Δt interval
$T(\Delta(t-1))$	old trust
$T_{patient}$	final trust value

Greek symbols

α	PDR weight in current trust
β	medical trust weight in current trust
γ	energy weight in current trust
δ	IDS decision weight in current trust
λ	weight of old trust
μ	weight of new trust