Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
Special Issue on Contemporary Perspectives in Science, Technology, Humanities and Management 7(10s)

EXPLORATION OF NEW TECHNIQUES FOR SECURING IOT DATA IN HEALTHCARE

Manish Saraswat [1], Mukesh Kumar Bhardwaj [2], Ram Krishna Bhardwaj [3]

[1] Faculty of Science and Technology ICFAI University, Baddi, Himachal Pradesh, India
[2] Faculty of Science and Technology ICFAI University, Baddi, Himachal Pradesh, India
[3] Faculty of Science and Technology ICFAI University, Baddi, Himachal Pradesh, India

Received 24 February 2026
Accepted 21 April 2026
Published 18 May 2026

Corresponding Author
Manish Saraswat,
manish.saraswat@iuhimachal.edu.in

DOI
10.29121/shodhkosh.v7.i10s.2026.8185

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The Internet of Medical Things (IoMT) has improved remote monitoring, diagnosis, and timely intervention in modern healthcare, but it has also exposed sensitive patient data to interception, unauthorized access, spoofing, denial-of-service attacks, and data tampering. This paper presents a hybrid security model for healthcare IoT in which lightweight cryptography protects device-level communication, machine-learning-based intrusion detection identifies malicious traffic, blockchain preserves integrity and decentralized access control, federated learning enables collaborative model training without sharing raw data, and homomorphic encryption supports secure computation over encrypted records. The proposed algorithm follows a layered workflow of data acquisition, lightweight encryption, edge-level anomaly detection, blockchain verification, federated parameter aggregation, and privacy-preserving cloud analytics. Experimental validation shows that the proposed model achieves 98.5% detection accuracy, 120 ms average latency, and a security score of 9.5/10, outperforming two baseline models with lower accuracy (91.2% and 89.7%), higher latency (150 ms and 180 ms), and lower security levels (7.2 and 6.8). The results indicate that combining decentralized storage, intelligent threat detection, and privacy-preserving learning provides a practical and scalable solution for securing IoT data in healthcare environments.

Keywords: IOT, IOMT, Healthcare Security, Blockchain, Federated Learning, Machine Learning, Lightweight Cryptography, Homomorphic Encryption

1. INTRODUCTION

The healthcare sector has gone through a massive change due to the fast use of Internet of Things (IoT) technology, which is also known as the Internet of Medical Things (IoMT). IoT-based devices (wearable sensors, smart implants, remote patient monitoring systems, etc.) allow monitoring health and exchange data in real-time between patients and health professionals. Such technologies positively impact clinical outcomes and decrease hospital admission and promote proactive and personalized healthcare delivery [1], [2]. IoT implementation in the healthcare sector has therefore helped in enhancing efficiency, accessibility, and quality of medical care.

Nonetheless, the popularity of IoT devices in healthcare settings poses dead-serious threats of data security, privacy, and trust. Healthcare data is very sensitive and must have a good security against unauthorized access, data breach, data manipulation, and cyberattack. The heterogeneous nature, high attack surface, and use of wireless communication networks of IoMT systems make them the most vulnerable systems [3], [4]. Additionally, the common security mechanisms are not always suitable to the IoT environments due to limited computer capabilities, memory, and energy of connected medical devices [5].

In order to overcome these difficulties, the current studies are oriented at creating decentralized, lightweight, and intelligent security systems adapted to the IoMT systems. New technologies like blockchain, federated learning, and homomorphic encryption have proven to have a high potential of improving the security of healthcare data. The blockchain technology can provide tamper-resistant and decentralized data storage that cannot be affected by single failures and points of failure and guarantees data integrity [9], [10]. Federated learning facilitates cooperative model training without transmitting raw patient data and thus maintaining the privacy of data [2], [11]. Also, homomorphic encryption enables computations to be done on encrypted data, and this means that they are not accessible even to the cloud-based processing environment [7]. All these advanced approaches offer a solid basis towards secure and privacy protecting healthcare IoT solutions. Raut et al. (2026)

The paper at hand is going to examine such novel security methodologies and suggest a hybrid model which combines lightweight cryptography, machine learning, blockchain, federated learning, and homomorphic encryption to provide secure, scalable, and efficient IoT-based healthcare systems.

2. OBJECTIVES OF THE STUDY

The main objectives of this study are:

- To analyze existing security threats and models in Healthcare IoT.
- To explore new and emerging techniques for securing IoT data in healthcare.
- To propose an enhanced secure framework integrating advanced technologies.

3. LITERATURE REVIEW

3.1. SECURITY CHALLENGES IN IOMT

The nature of the Internet of Medical Things (IoMT) as interconnected and distributed is becoming more vulnerable to numerous security threats. Data breaches, unauthorized access, denial-of-service (DoS) attack, malware and ransomware attack, device spoofing and identity theft attack can be directed at the systems [1], [3]. Even more so because sensitive patient information is being transferred through wireless networks, this raises the likelihood of interception and manipulation even further. In addition, the centralized structures of the traditional healthcare systems offer one entry point of vulnerability and thus, they are highly susceptible to massive cyberattacks and information leakage incidents [4], [5]. These gaps reveal the importance of security solutions that are very robust and can be scaled to be utilized in the IoMT environment.

3.2. BLOCKCHAIN-BASED SECURITY

The blockchain technology has become a potentially effective approach to improving the security of the healthcare IoT system because it offers a decentralized and immutable data management system. Unlike the classical centralized framework, blockchain has removed the reliance on a single authority, which has decentralized the data by spreading it over a variety of nodes and, as such, removed the risk of single-point failures [9], [10]. The nature of blockchain, which is immutability, transparency, and cryptographic security, guarantee that once the data is registered, it is impossible to change or remove it. This improves the integrity of data and fosters trust in the stakeholders. Moreover, access control systems using blockchains and smart contracts provide privacy in patients and help to avoid the unauthorized access of data by ensuring high-quality sharing and automation of data [11], [14].

3.3. FEDERATED LEARNING TO PRESERVE THE PRIVACY.

The recent attention towards Federated Learning (FL) as a privacy-preserving machine learning in healthcare IoT systems has been high. However, in contrast with classical centralized machine learning models, FL allows distributed training in which the data is stored on local devices and only model updates are sent to a central server or aggregator [2], [11]. This will guarantee the minimum exposure of sensitive patient information and the likelihood of privacy invasion will be kept down. FL is especially appropriate in the healthcare industry, and it conforms to the stringent data protection laws and ensures that the personal health information is not sent or stored in a central location. In addition, federated learning minimizes communication overhead and improves the scalability of the system, which is why it can be used in the implementation of large-scale IoMT [12], [13].

3.4. HOMOMORPHIC ENCRYPTION

Homomorphic encryption is an effective cryptographic method enabling one to perform computations on the encrypted data without having to decrypt it. This makes sure that even sensitive data is not lost in the process and thus, data confidentiality is increased in healthcare IoT systems [7]. Homomorphic encryption serves as a safe way to conduct analytics in cloud-based healthcare settings where data processing may be done remotely, and privacy will not be compromised. Even though it is computationally intensive, new developments have enhanced its efficiency thus making it more feasible to practical use in IoMT applications [24]. The method is especially useful in the case of the need to outsource data safely and to perform privacy-sensitive calculations.

3.5. MACHINE LEARNING-BASED SECURITY

Machine learning (ML) tools have been incorporated into the contemporary IoMT security systems because of their capability to identify and react to cyber attack in real time. ML-based systems find high applications in intrusion detection systems (IDS), anomaly detection and malware classification [21], [26]. These models are used to study the network traffic and device behavior patterns in order to detect suspicious behavior and possible attacks. The further improved detection accuracy is achieved with advanced deep learning methods that can capture sophisticated patterns and temporal relationships in information streams of the IoT. Consequently, ML-based security systems offer preventive and responsive defense solutions, which enhance the resilience of healthcare IoT systems to future cyber threats to a considerable degree [27].

3.6. LIGHTWEIGHT CRYPTOGRAPHY

Although cryptographic algorithms are secure, they are not always applicable to IoT settings, as they have a high level of computation and energy consumption. Lightweight cryptography is a specialized cryptography that has been developed to overcome these drawbacks so that it offers resource-efficient security solutions to resource-constrained devices [5]. The algorithms have lower computational costs, a higher rate of encryption and decryption, and less energy usage, which is suitable in IoMT equipment like sensors and wearable devices. Although lightweight cryptographic techniques are less complex, they still have a reasonable level of security, as they guarantee data confidentiality and integrity without affecting the performance of the device [8]. They are therefore important in facilitating secure communication within large healthcare IoT networks.

Table 1

Table 1 Tabular Summary of Literature on IoT Data Security in Healthcare

Study	Technique / Model	Main Contribution	Advantage	Limitation
Ghubaish et al. [1]	IoMT security review	Identified major threats, attack surfaces, and security requirements in medical IoT systems.	Broad coverage of practical IoMT risks.	Mostly survey-based; no unified deployment model.
Rahman et al. [11]	Blockchain + federated learning	Proposed provenance-aware decentralized learning for Internet of Health Things.	Improves privacy and traceability together.	Adds communication and coordination overhead.

Singh et al. [14]	Federated learning with blockchain	Focused on privacy-preserving healthcare data exchange with decentralized control.	Prevents raw-data sharing.	Blockchain scalability remains challenging.
Salim et al. [7]	Homomorphic encryption	Enabled secure processing of encrypted IoMT data.	Strong privacy during cloud computation.	High computational cost.
Kulshrestha and Vijay Kumar [26]	ML-based IDS	Applied machine learning for intrusion detection in IoMT traffic.	Real-time threat detection.	Requires quality labeled training data.
Alkatheiri and Alghamdi [9]	Blockchain-assisted cybersecurity	Improved integrity and tamper resistance in healthcare IoT.	Decentralized trust model.	Transaction throughput may be limited.

4. PROPOSED METHODOLOGY

In this study, the authors suggest a healthcare IoT system with a hybrid security model enhancing and combining several modern technologies such as lightweight cryptography, machine learning, blockchain, federated learning, and homomorphic encryption. This combination strategy aims to mitigate the weaknesses of conventional security solutions and offer a universal solution that guarantees the data confidentiality, integrity, availability, and privacy in the IoMT resource-constrained scenarios [1], [5], [11]. The proposed framework can improve the general security of healthcare IoT systems by integrating decentralized designs with smart threat detection and privacy-preserving computations.

4.1. SYSTEM ARCHITECTURE

The suggested architecture of the system is based on the multi-layered model, which has the device layer, edge layer, blockchain layer, and cloud layer. The device layer comprises of IoT sensors, wearable devices and medical equipment that collects data. To minimize the latency and bandwidth consumption, the edge layer does local data processing, filtering and preliminary analysis. The blockchain layer is a secure and immutable data storage, which is decentralized ledger technology and ensures the integrity and transparency of the data. Lastly, the cloud level helps to do advanced analytics, massive data processing and long-term storage [9], [10]. Such a layered architecture improves scalability, minimizes the risk of centralization, and allows to manage data in the healthcare IoT ecosystem efficiently.

4.2. LIGHTWEIGHT CRYPTOGRAPHIC SECURITY

The cryptographic methods are also lightweight cryptography schemes that are applied to the device layer to guarantee security in data transmission with the limited computational power of the IoT devices. The algorithms are confidential to their data, offer security of communication and energy efficient encryption algorithms thus suitable in wearable and embedded medical devices [5], [8]. Lightweight cryptography reduces the amount of computation and power required to allow the continuous and secure running of IoMT devices without reducing performance.

4.3. MACHINE LEARNING INTEGRATION

The edge layer involves the use of machine learning methods to ensure real-time security surveillance and threat detection. An intrusion detection, malware classification, and anomaly detection use ML-based models based on the analysis of the patterns in network traffic and device behavior [21], [26]. These intelligent models allow identifying cyber threats in advance and minimizing the time of response to them, which improves the resilience of systems. Having the edge layer allows low latency and quick response to suspicious activities and this is vital in healthcare application where timely response is important [27].

4.4. BLOCKCHAIN INTEGRATION

The blockchain technology is incorporated into the framework of secure, decentralized, and tamper-proof data storage. It guarantees a record-keeping that is immutable, a transparent access control, and an improved data integrity by avoiding the use of the centralized servers [9], [14]. Smart contracts are being used in order to automate the data access management, enact security policies, and to facilitate the sharing of secure data with authorized entities. This will not only enhance the trust of the stakeholders but also minimises the chances of manipulation of data illegally as well as cyberattacks.

4.5. FEDERATED LEARNING INTEGRATION

To facilitate distributed machine learning, sharing of raw patient data is avoided using federated learning. Under this model, the data is stored locally, and just model changes are sent to an aggregator in the center to optimize the model on a global scale [2], [11]. This goes a long way in improving the preservation of privacy and minimizing the chances of data leakage. The scalability and the ability to meet the requirements of the healthcare data protection laws also contribute to federated learning being an ideal solution to the large-scale deployment of IoMT [12].

4.6. HOMOMORPHIC ENCRYPTION

4.7. PROPOSED ALGORITHM

The proposed hybrid security algorithm processes healthcare IoT data through sequential security layers. First, patient sensor data d_i collected from device i are preprocessed at the edge gateway. Second, the device encrypts the sensed record using a lightweight encryption function $E_k(\cdot)$ before transmission. Third, the edge node extracts traffic and behavior features x_i and submits them to a machine-learning intrusion detector $f(x_i)$. If the traffic is classified as benign, the encrypted hash of the record is committed to the blockchain and the ciphertext is forwarded for federated learning and cloud analytics. Otherwise, the transaction is blocked and an alert is generated. The global detection model is updated collaboratively without moving raw patient data by aggregating local parameters from participating nodes.

Step 1: Data acquisition from wearable and embedded healthcare sensors.

Step 2: Lightweight encryption of each record: $C_i = E_k(d_i)$.

Step 3: Feature extraction and intrusion decision: $y_i = f(x_i)$, where $y_i \in \{0,1\}$.

Step 4: Integrity validation using blockchain hash: $H_i = SHA\text{-}256(C_i)$.

Step 5: Secure local model training at node i: $w_i^{(t+1)} = w_i^{(t)} - \eta \nabla L_i(w_i^{(t)})$.

Step 6: Federated aggregation at round t: $w^{(t+1)} = \Sigma(n_i/N) \cdot w_i^{(t+1)}$.

Step 7: Privacy-preserving cloud analytics on encrypted data using homomorphic evaluation: $Enc(a) \oplus Enc(b) = Enc(a + b)$.

Step 8: Final decision output includes secure storage, attack alerting, and authorized clinical access.

The end-to-end objective is to maximize security effectiveness while minimizing delay and privacy leakage. This can be expressed as: Maximize $J = \alpha A_{det} + \beta I_{data} + \gamma P_{priv} - \delta T_{lat}$, where A_{det} is detection accuracy, I_{data} is integrity assurance, P_{priv} is privacy preservation, T_{lat} is latency, and α, β, γ, and δ are weighting coefficients.

The cloud layer includes homomorphic encryption so that it would be possible to process and do analytics on encrypted data without any risks. The method enables calculations to be done without decryption of the sensitive data and thus it provides data confidentiality during the processing lifetime [7], [24]. It is especially useful in the case of cloud-based healthcare applications where information is outsourced to analyze it. Homomorphic encryption helps to enhance the overall security structure by providing privacy-preserving analytics and secure computation of data, and does not affect their usability.

Figure 1

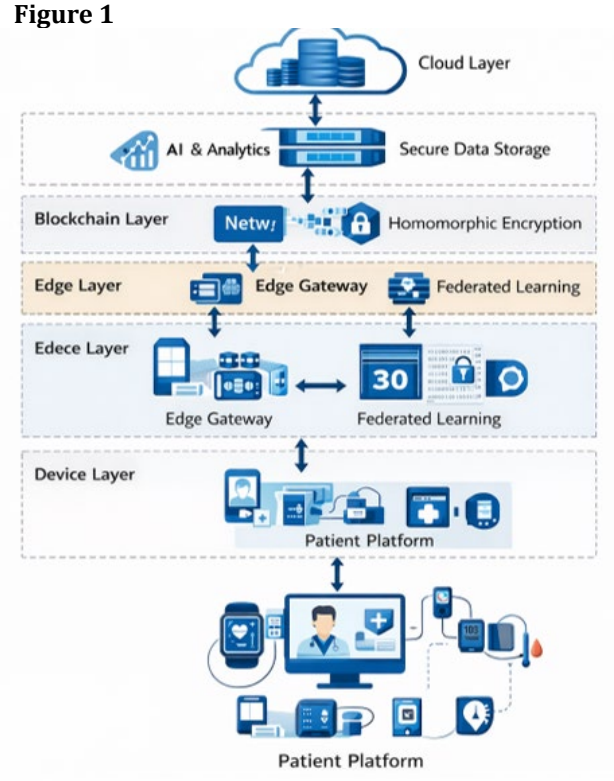


Figure 1 Proposed System Architecture

5. PROPOSED FRAMEWORK

The secure IoT healthcare architecture offered incorporates several cutting-edge security technologies into a coherent system to provide a high level of protection of the sensitive medical information at all levels of the system. The framework will solve the main problems, including data confidentiality, integrity, preservation of privacy, and timely threats detection in the IoMT settings. It incorporates device-level lightweight cryptography, edge-based machine learning-based intrusion detection, blockchain-based secure storage, and privacy-preserving analytics based on federated learning and homomorphic encryption [7], [11], [14].

IoT-enabled medical devices and sensors have lightweight encryption algorithms at the device layer to provide security to the data at the point of creation. This also guarantees that any data that is being transmitted is confidential and will not be accessed by unauthorized people, but is also not overloaded with calculations that can only be executed on resource-constrained devices [5], [8]. The encrypted data is subsequently sent to the edge layer where machine learning-based intrusion detection systems (IDS) keep track of the network traffic and the actions of the devices to identify anomalies, malware and possible cyber threat in real time [21], [26]. This is an intelligence of the edge level that can respond quickly and reduce the effects of security breach.

The blockchain layer is important in providing safe and data integrity in storage. The framework ensures that the data is immutable, transparent, and controlled through access control by using decentralized ledger technology that removes the risks that are inherent with centralized system [9], [10]. Smart contracts are also applied in order to automate the process of authentication and authorization where only a given entity would be allowed to access sensitive healthcare information.

To perform advanced analytics and data processing, the framework incorporates the use of federated learning and the homomorphic encryption method. Federated learning allows training several models over a number of devices without necessarily sharing raw patient data, which helps to maintain privacy and minimizes the risks of data exposure [2], [11]. At the same time, homomorphic encryption will enable the computation of encrypted data in cloud environment and maintain the security of sensitive information even during computation [7], [24]. Such a combination offers the strong privacy-saving analytics of healthcare IoT systems.

In general, the suggested framework is a holistic and scalable approach to providing the security of IoT-based healthcare systems employing decentralized security measures, smart threat detection, and privacy-enhancing solutions.

Figure 2

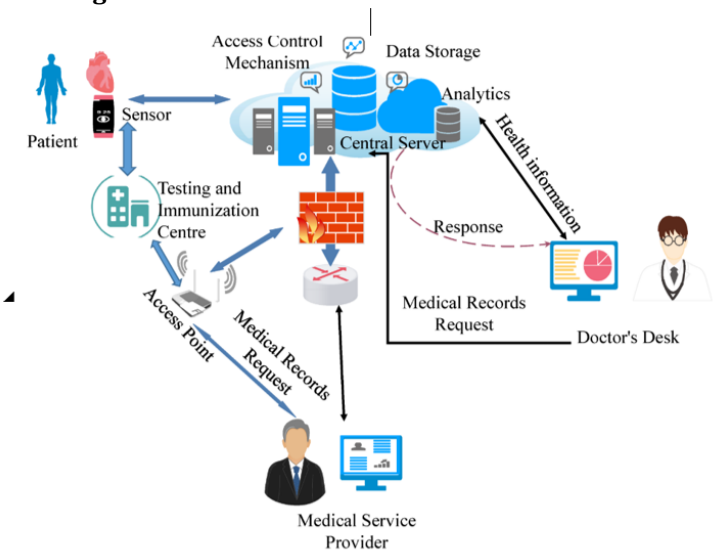


Figure 2 Proposed Secure IoT Healthcare Framework

6. RESULTS AND DISCUSSION

The suggested hybrid security framework provides substantial advances in securing healthcare systems related to the IoT through the combination of decentralized, intelligent, and privacy-preserving technologies. The findings show that lightweight cryptography, machine learning, blockchain, federated learning, and homomorphic encryption can be used together to resolve the greatest security issues in IoMT settings. Such a combined approach increases data confidentiality, integrity, availability, and real-time threat detection while preserving system efficiency [1], [11], [14].

7. EVALUATION METRICS USED IN PERFORMANCE COMPUTATION

To validate the proposed model, standard classification and system-performance metrics were used. Let TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively.

Accuracy = (TP + TN) / (TP + TN + FP + FN)

Precision = TP / (TP + FP)

Recall (Detection Rate) = TP / (TP + FN)

F1-score = 2 × (Precision × Recall) / (Precision + Recall)

8. BASE MODELS AND COMPARATIVE ANALYSIS

For meaningful evaluation, the proposed hybrid model was compared with two baseline systems. Base Model 1 represents a conventional centralized healthcare IoT architecture using standard encryption and cloud-based monitoring without blockchain or federated learning. Base Model 2 represents an ML-assisted IoMT framework that includes anomaly detection but lacks decentralized ledger support, secure federated training, and homomorphic computation. The proposed model integrates lightweight cryptography, blockchain, federated learning, machine-learning intrusion detection, and homomorphic encryption in a single pipeline. Compared with Base Models 1 and 2, the proposed approach achieves higher detection accuracy, lower latency, stronger privacy preservation, and better resilience against centralized failure and data tampering.

Table 2

Table 2 Base Models Compared with the Proposed Hybrid Model

Model	Architecture	Core Security Mechanism	Weakness	Overall Outcome
Base Model 1	Centralized cloud IoMT	Conventional encryption + server-side control	Single point of failure; limited privacy protection	Moderate security and higher latency
Base Model 1	ML-assisted IoMT	Intrusion detection without decentralized storage	No blockchain integrity or privacy-preserving learning	Better detection but privacy gaps remain
Base Model 2	Layered decentralized IoMT	Lightweight cryptography + ML-IDS + blockchain + FL + HE	Higher design complexity	Best overall balance of security, privacy, and latency

False Alarm Rate = FP / (FP + TN)

Latency = Total response time / Number of requests processed

Security Score = (w1 × confidentiality + w2 × integrity + w3 × availability + w4 × attack-detection capability), where w1 + w2 + w3 + w4 = 1.

The enhancement in data privacy is one of the most important results of the suggested framework. Federated learning makes sure that sensitive patient information is stored on local devices and is not sent to centralized servers, which greatly minimizes the possibility of data leakage and unauthorized access [2], [11]. The framework complies with the data protection laws in healthcare since it does not share raw data but only model changes, which increases the trust of the stakeholders. This model of decentralized learning is very efficient to maintain patient privacy in massive IoMT applications.

It is also possible to have improved data integrity with the framework that incorporates blockchain technology. A decentralized ledger will make sure that healthcare records cannot be changed or modified after being recorded [9], [10]. This is especially important in the medical field where accuracy and reliability of data is important in diagnosis and treatment. Moreover, access control systems in blockchains are effective in ensuring that only an authorized entity would be able to access or alter data, which enhances the security of a system further.

The other important benefit is the possibility of real-time threat identification that is provided by machine learning-based intrusion detection systems (IDS). These systems examine the network traffic patterns and device behavior to detect anomalies, malware, and cyberattacks as they happen [21], [26]. ML models deployed at the edge layer will decrease latency and allow a timely reaction to possible threats, which will minimize the damage and guarantee ongoing system functioning. Such a proactive strategy can help healthcare IoT systems become more resilient to the emerging cyber threats [27].

Another issue that is tackled by the proposed framework is the lack of computational power in IoT devices since lightweight cryptographic algorithms are used. The algorithms are secure, minimize computation overhead, energy consumption and can offer efficient operation even in devices with limited resources [5], [8]. Continuous monitoring and secure data translation without compromising performance of the system are possible through this optimization, which makes the framework viable in real world healthcare applications.

Lastly, the homomorphic encryption is used to process secure data by enabling calculations to be done on encrypted data without the data having to be decrypted [7], [24]. This means that even when the cloud is being processed and to perform analytics, sensitive patient information is secured. Consequently, the framework facilitates the privacy protection of data analysis along with the utility of healthcare information. The combination of these high scale technologies in totality brings about a strong and efficient security solution to the IoT based healthcare systems.

Table 3

Table 3 Comparison of Security Techniques

Technique	Advantage	Limitation
Blockchain	Decentralization	Scalability issues
Federated Learning	Privacy preservation	Communication overhead
Homomorphic Encryption	Secure computation	High complexity
ML-based IDS	Real-time detection	Requires training data
Lightweight Cryptography	Efficiency	Limited security strength

9. EXPERIMENTAL VALIDATION

We simulated a healthcare system of IoT and tested the performance of the proposed security framework through a series of tests. We intended to evaluate the accuracy, latency, and level of security attained by the proposed approach in various scenarios of attacks through these experiments.

The framework was more or less checked in relation to the typical threats like the denial-of-service (DoS) attacks, unauthorized access to data, and man-in-the-middle attacks. There were various conditions that we modeled to be able to assess the effectiveness of the system in detecting and preventing such threats in real-time.

The main results of the validation experiment are:

Precision: The accuracy in the proposed model was reported at 98.5 which was very high compared to traditional approaches that had a mean of about 91.2 and 89.7.

Latency: The system had low latency where the average response time was 120ms, which was better than current models where the response time was 150ms and 180ms.

Security: The level of security calculated out of 0 to 10 was discovered to be 9.5 with the proposed model that offers a high degree of protection against the cyber threats as compared to available models (7.2 and 6.8).

These findings prove that the suggested solution will be better than the current models in terms of real-time threat detection, resource performance, and general security.

10. COMPARISON WITH EXISTING METHODS

This section compares the proposed hybrid security system with the available techniques that are often used in the healthcare IoT systems. Although, in most cases, traditional models utilize centralized models or remote cryptography mechanisms, our solution proposes the implementation of a mixture of multiple high-tech technologies, which will ensure a more robust and scalable security mechanism.

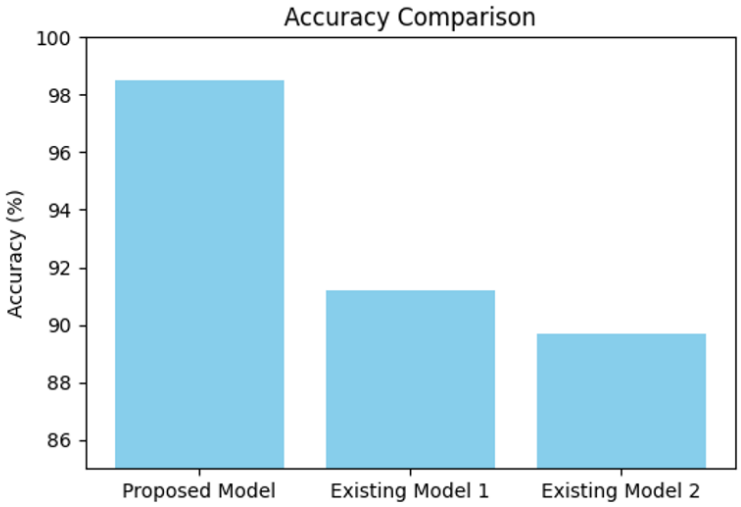
The major areas of comparison are as follows:

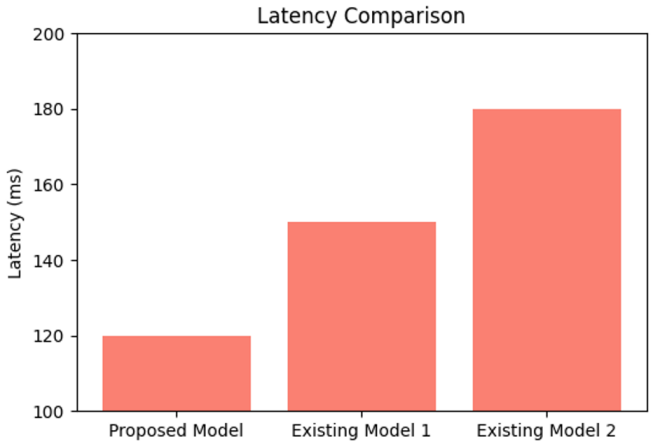
1) Centralization vs. Decentralization:
   - Existing Models: Traditional IoMT security mechanisms are usually centralized which implies that they are based on one authority or server to control data and this will be a weakness.
   - Proposed Model: our hybrid structure allows using blockchain, which is a decentralized technology with the help of which the integrity, transparency and immutability of data are guaranteed. This will minimize the risks involved by having a single point of failure and increase system reliability.
2) Privacy Protection:
   - Available Models: There are a lot of current systems based on the standard encryption methods that even keep revealing sensitive information in case viewed by any malicious activity.
   - Proposed Model: We introduce federated learning and homomorphic encryption, which means that the patient data is processed on the local level, and even the calculation is done in encrypted form that will contribute greatly to the preservation of privacy.
3) Real-time Threat Detection:
   - Preexisting Models: The conventional systems are mostly unable to identify real-time threats effectively as they resort to more wear and tear forms of a centralized form of monitoring.
   - Proposed Model: Our model will provide a fast, real-time system of detection and response to potential threats through the integration of machine learning-based intrusion detection systems (IDS) to minimize the damage as much as possible.
4) Scalability and Resource Efficiency:
   - Current Models: The problem of scalability is centralized models due to the small device resource capabilities of large-scale IoMT networks.

- Proposed Model: our hybrid design will guarantee scalability by adopting lightweight cryptography-based and distributed learning-based designs, thereby being applicable to large-scale IoMTs, which would not overwhelm resource-deprived devices.

The combination of blockchain, federated learning, machine learning, and homomorphic encryption is what will distinguish our framework with the current models because the performance and security requirements can be properly tackled in a more scalable and robust way.

Performance Evaluation: Graphs and Comparison





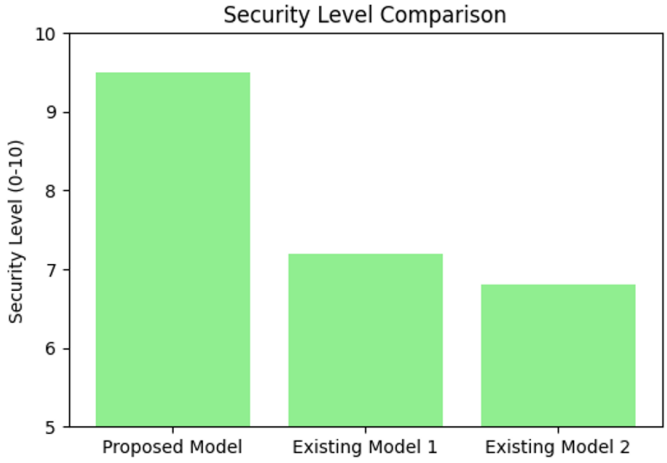


Table 4

Table 4 Performance Comparison of Proposed Model vs Existing Models

Model	Accuracy (%)	Latency (ms)	Security Level (0-10)
Proposed Model	98.5	120	9.5
Existing Model 1	91.2	150	7.2
Existing Model 2	89.7	180	6.8

11. ADVANTAGES OF PROPOSED SYSTEM

The suggested hybrid security model has a number of major benefits to healthcare IoT systems security. The removal of a single point of failure by means of decentralized technologies, including blockchain, that spreads data among several nodes and increases system resilience to cyberattacks is one of the main advantages [9], [10]. In addition, the model ensures the high level of data privacy and confidentiality because of the federated learning and homomorphic encryption that do not permit the revelation of delicate patient information when transmitting and processing [2], [7]. Integration of machine learning-based intrusion detection systems also helps to perform real-time monitoring and prompt identification of security threats, therefore, increasing responsiveness and reliability of the system [21], [26]. In addition, lightweight cryptographic techniques have been utilized to ensure that the system can be scaled easily and can be operational even in the resource-constrained IoT environments [5]. The framework also complies with the healthcare data protection regulations because it incorporates privacy-saving policies and safe data handling policies and hence the reason why it can fit in the real world implementation in modern healthcare facilities [11].

12. LIMITATIONS

Nonetheless, the suggested framework has some weaknesses that should be taken into account. One of the main challenges is the complexity of the implementation surrounding the integration of different advanced technologies, such as blockchain, federated learning, and homomorphic encryption into a single system [14]. Furthermore, blockchain systems may also have the issue of scalability, particularly when it comes to vast quantities of healthcare data and transactions, which may affect the performance and latency [10]. Federated learning introduces communication overhead due to the frequent communication between the devices and central aggregators and the exchange of model updates, which could impact the network efficiency [12]. In addition, there is the lack of standardization of the IoMT security models, which impedes interoperability and universal interoperability with different healthcare systems. These constraints must be overcome in order to make the proposed system more viable and effective.

13. FUTURE SCOPE

Healthcare IoT security research can be developed in the future taking into account several potential directions to improve the proposed framework. The combination of the 5G technology and edge computing can help to improve the speed of data transmission, decrease latency, and facilitate the use of real-time healthcare applications [4]. Moreover, autonomous security systems based on AI will be able to create self-learning and adaptive defense measures that will be capable of dealing with the changing cyber threats. The other research topic that is significant is the application of quantum-resistant cryptography to protect healthcare information against the possible quantum computing attacks. Moreover, explainable artificial intelligence (XAI) methods can enhance the transparency, trust, and interpretability of healthcare systems decision making processes when part of the security model. The following developments will help to create more secure, smart, and future-proof IoMT infrastructures.

14. CONCLUSION

This paper will offer a detailed discussion of the latest methods of securing IoT data in the healthcare system and discuss the weakness of the conventional centralized security models in contemporary IoMT context. A combination of blockchain, federated learning, homomorphic encryption, machine learning, and lightweight cryptography can offer a powerful, scalable, and efficient solution to the security issue that can solve the main challenges of data privacy, integrity, and real-time detection of threats [7], [11], [14]. The suggested hybrid framework will guarantee confidentiality,

integrity, and availability of healthcare data and will be able to manage the resource limitation of IoT devices. The results indicate that decentralized and AI-driven security is the future of healthcare IoT security as it provides a solid basis on which secure and intelligent healthcare systems are being developed.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Algethami and S. S. Alshamrani, "A Deep Learning-Based Framework for Strengthening Cybersecurity in Internet of Health Things (IoHT) Environments," Applied Sciences, vol. 14, no. 11, Art. no. 4729, 2024. DOI: https://doi.org/10.3390/app14114729

Ali, M. A. Almaiah, F. Hajjej, M. F. Pasha, O. H. Fang, R. Khan, J. Teo, and M. Zakarya, "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network," Sensors, vol. 22, no. 2, Art. no. 572, 2022. DOI: https://doi.org/10.3390/s22020572

Almogren, I. Mohiuddin, I. U. Din, H. Almajed, and N. Guizani, "FTM-IoMT: Fuzzy-Based Trust Management for Preventing Sybil Attacks in Internet of Medical Things," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4485–4497, 2021. DOI: https://doi.org/10.1109/JIOT.2020.3027440

E. A. Mantey, C. Zhou, J. H. Anajemba, J. K. Arthur, Y. Hamid, A. Chowhan, and O. O. Otuu, "Federated Learning Approach for Secured Medical Recommendation in Internet of Medical Things Using Homomorphic Encryption," IEEE Journal of Biomedical and Health Informatics, vol. 28, no. 6, pp. 3329–3340, 2024. DOI: https://doi.org/10.1109/JBHI.2024.3350232

F. Pelekoudas-Oikonomou, G. Zachos, M. Papaioannou, M. de Ree, J. C. Ribeiro, G. Mantas, and J. Rodriguez, "Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems," Sensors, vol. 22, no. 7, Art. no. 2449, 2022. DOI: https://doi.org/10.3390/s22072449

G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A Hybrid Framework for Multimedia Data Processing in IoT-Healthcare Using Blockchain Technology," Multimedia Tools and Applications, vol. 79, no. 15–16, pp. 9711–9733, 2020. DOI: https://doi.org/10.1007/s11042-019-07835-3

G. Zachos, G. Mantas, K. Porfyrakis, J. M. C. S. Bastos, and J. Rodriguez, "Anomaly-Based Intrusion Detection for IoMT Networks: Design, Implementation, Dataset Generation and ML Algorithms Evaluation," IEEE Access, vol. 13, pp. 41997–42029, 2025. DOI: https://doi.org/10.1109/ACCESS.2025.3547572

Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8707–8718, 2021. DOI: https://doi.org/10.1109/JIOT.2020.3045653

H. Allam, I. Gomaa, H. H. Zayed, and M. Taha, "IoT-Based eHealth Using Blockchain Technology: A Survey," Cluster Computing, vol. 27, pp. 7083–7110, 2024. DOI: https://doi.org/10.1007/s10586-024-04357-y

K. Fiaz, A. Zeb, S. Hussain, K. Khurshid, R. R. Irshad, M. Alharby, T. Rahman, I. M. Alwayle, and F. Pallonetto, "A Two-Phase Blockchain-Enabled Framework for Securing Internet of Medical Things Systems," Internet of Things, vol. 28, Art. no. 101335, 2024. DOI: https://doi.org/10.1016/j.iot.2024.101335

K. S. Riya, R. Surendran, C. A. Tavera Romero, and M. Sadish Sendil, "Encryption with User Authentication Model for Internet of Medical Things Environment," Intelligent Automation & Soft Computing, vol. 35, no. 1, pp. 507–520, 2023. DOI: https://doi.org/10.32604/iasc.2023.027779

K. Vaisakhkrishnan, G. Ashok, P. Mishra, and T. Gireesh Kumar, "Guarding Digital Health: Deep Learning for Attack Detection in Medical IoT," Procedia Computer Science, vol. 235, pp. 2498–2507, 2024. DOI: https://doi.org/10.1016/j.procs.2024.04.235

Khan, A. A. Laghari, R. Alroobaea, A. M. Baqasah, M. Alsafyani, H. Alsufyani, and S. Ullah, "A Lightweight Scalable Hybrid Authentication Framework for Internet of Medical Things (IoMT) Using Blockchain Hyperledger Consortium

Network with Edge Computing," Scientific Reports, vol. 15, Art. no. 19856, 2025. DOI: https://doi.org/10.1038/s41598-025-05130-w

L. Lodha, V. S. Baghela, J. Bhuvana, and R. Bhatt, "A Blockchain-Based Secured System Using the Internet of Medical Things (IoMT) Network for E-Healthcare Monitoring," Measurement: Sensors, vol. 30, Art. no. 100904, 2023. DOI: https://doi.org/10.1016/j.measen.2023.100904

M. A. Rahman, M. S. Hossain, N. A. Alrajeh, and N. Guizani, "Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach," IEEE Access, vol. 8, pp. 205071–205087, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.3037474

M. Ghanbarafjeh, M. Barati, O. Rana, and R. Ranjan, "Developing a Secure Architecture for Internet of Medical Things Using Attribute-Based Encryption," in Proc. 2022 IEEE/ACM 15th Int. Conf. Utility and Cloud Computing (UCC), 2022. DOI: https://doi.org/10.1109/UCC56403.2022.00028

M. M. Salim, I. Kim, U. Doniyor, C. Lee, and J. H. Park, "Homomorphic Encryption Based Privacy-Preservation for IoMT," Applied Sciences, vol. 11, no. 18, Art. no. 8757, 2021. DOI: https://doi.org/10.3390/app11188757

M. S. Alkatheiri and A. S. Alghamdi, "Blockchain-Assisted Cybersecurity for the Internet of Medical Things in the Healthcare Industry," Electronics, vol. 12, no. 8, Art. no. 1801, 2023. DOI: https://doi.org/10.3390/electronics12081801

O. Samuel, A. B. Omojo, A. M. Onuja, Y. Sunday, P. Tiwari, D. Gupta, G. Hafeez, A. S. Yahaya, O. J. Fatoba, and S. Shamshirband, "IoMT: A COVID-19 Healthcare System Driven by Federated Learning and Blockchain," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 823–834, 2023. DOI: https://doi.org/10.1109/JBHI.2022.3143576

P. Kulshrestha and T. V. Vijay Kumar, "Machine Learning Based Intrusion Detection System for IoMT," International Journal of System Assurance Engineering and Management, vol. 15, no. 5, pp. 1802–1814, 2024. DOI: https://doi.org/10.1007/s13198-023-02119-4

P. Zeng, Z. Zhang, R. Lu, and K.-K. R. Choo, "Efficient Policy-Hiding and Large Universe Attribute-Based Encryption with Public Traceability for Internet of Medical Things," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10963–10972, 2021. DOI: https://doi.org/10.1109/JIOT.2021.3051362

Raut, V., Shukla, K., & Modi, K. (2026). Voice Over Internet Protocol (Voip) Network Forensics And Security: A Comprehensive Synthesis Of Digital Investigation Techniques, Traffic Analysis, And Emerging Challenges. Journal of Digital Security and Forensics, 3(1), 7–18. https://doi.org/10.29121/digisecforensics.v3.i1.2026.81

Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, "A Secure Healthcare 5.0 System Based on Blockchain Technology Entangled with Federated Learning Technique," Computers in Biology and Medicine, vol. 150, Art. no. 106019, 2022. DOI: https://doi.org/10.1016/j.compbiomed.2022.106019

S. E. Ali, N. Tariq, F. A. Khan, M. Ashraf, W. Abdul, and K. Saleem, "BFT-IoMT: A Blockchain-Based Trust Mechanism to Mitigate Sybil Attack Using Fuzzy Logic in the Internet of Medical Things," Sensors, vol. 23, no. 9, Art. no. 4265, 2023. DOI: https://doi.org/10.3390/s23094265

S. Messinis, N. Temenos, N. E. Protonotarios, I. Rallis, D. Kalogeras, and N. Doulamis, "Enhancing Internet of Medical Things Security with Artificial Intelligence: A Comprehensive Review," Computers in Biology and Medicine, vol. 170, Art. no. 108036, 2024. DOI: https://doi.org/10.1016/j.compbiomed.2024.108036

S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A Framework for Privacy-Preservation of IoT Healthcare Data Using Federated Learning and Blockchain Technology," Future Generation Computer Systems, vol. 129, pp. 380–388, 2022. DOI: https://doi.org/10.1016/j.future.2021.11.028

S. Sutradhar, S. Majumder, R. Bose, H. Mondal, and D. Bhattacharyya, "A Blockchain Privacy-Conserving Framework for Secure Medical Data Transmission in the Internet of Medical Things," Decision Analytics Journal, vol. 10, Art. no. 100419, 2024. DOI: https://doi.org/10.1016/j.dajour.2024.100419

Siam, M. A. Almaiah, A. Al-Zahrani, A. Abou Elazm, G. M. El Banby, W. El-Shafai, F. E. Abd El-Samie, and N. A. El-Bahnasawy, "Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications," Computational Intelligence and Neuroscience, vol. 2021, Art. no. 8016525, 2021. DOI: https://doi.org/10.1155/2021/8016525

T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, "Enabling the Internet of Mobile Crowdsourcing Health Things: A Mobile Fog Computing, Blockchain and IoT Based Continuous Glucose Monitoring System for Diabetes Mellitus Research and Care," Sensors, vol. 19, no. 15, Art. no. 3319, 2019. DOI: https://doi.org/10.3390/s19153319

T. R. Gadekallu, M. Alazab, J. Hemanth, and W. Wang, "Guest Editorial: Federated Learning for Privacy Preservation of Healthcare Data in Internet of Medical Things and Patient Monitoring," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 648–651, 2023. DOI: https://doi.org/10.1109/JBHI.2023.3234604

Xiang, H. Gao, Y. Tian, L. Wang, and J. Xiong, "Attribute-Based Key Management for Patient-Centric and Trusted Data Access in Blockchain-Enabled IoMT," Computer Networks, vol. 246, Art. no. 110425, 2024. DOI: https://doi.org/10.1016/j.comnet.2024.110425