Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 270 (2025) 3668–3677

Procedia Computer Science

www.elsevier.com/locate/procedia

29th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2025)

A Blockchain-Based Security Framework for a Highly Secure and Intelligent Healthcare Ecosystem

Priyanka Verma[a,*], Nitesh Bharot[b], Rutvij H. Jhaveri[c,*], John G. Breslin[b]

[a]*School of Computer Science, University of Galway, Galway, Ireland*
[b]*Data Science Institute, University fo Galway, Galway, Ireland*
[c]*Department of Computer Science and Engineering, Pandit Deendayal Energy University, Gandhinagar, India*

Abstract

The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling real-time patient monitoring, remote diagnostics, and intelligent decision-making. However, IoMT data is prone to unauthorized access, resulting in a significant loss of privacy and security. To address these challenges, we propose a novel security framework which is based on XChaCha20-Encryption fortified with a Role-Based Access Control (RBAC) mechanism and a blockchain-integrated ML model to establish a highly secure and intelligent healthcare ecosystem. The proposed framework employs a Proof of Authority (PoA) consensus mechanism to validate and secure blockchain operations, making it particularly well-suited for real time IoMT applications. The performance of the system is evaluated on the WUSTL-EHMS-2020 dataset, demonstrating superior results over other state-of-the-art approaches. Moreover, the proposed framework achieves remarkable encryption and decryption times of 0.61 and 0.71 seconds, respectively. Along with data privacy proposed framework outperforms other methods and achieves an accuracy of 99.43% for detecting cyber attacks launched against IoMT data.

Keywords: Plaintext; Ciphertext; XChaCha20; Encryption; Decryption; Random Forest; Consensus Mechanism; Blockchain

1. Introduction

The emergence of the Internet of Medical Things (IoMT) has revolutionized healthcare by enabling real-time patient monitoring [1], remote diagnostics, and intelligent decision-making. IoMT devices generate vast amounts of sensitive medical data that, if properly utilized, can enhance patient outcomes and operational efficiency. However, managing and securing this data pose significant challenges, including privacy concerns, cybersecurity threats, and

* Corresponding author.
E-mail address: priyanka.verma@universityofgalway.ie, rutvij.jhaveri@sot.pdpu.ac.in

1877-0509
10.1016/j.procs.2025.09.492

scalability issues [2]. With the rise of data-driven healthcare systems, ensuring the confidentiality and integrity of medical records while minimizing operational overhead has become a primary concern.

Moreover, IoMT ecosystems involve interconnected medical devices that continuously collect and exchange critical health data. Traditional centralized healthcare data systems suffer from inherent vulnerabilities, such as single points of failure, unauthorized access, and large-scale data breaches [3]. While IoT-driven healthcare enables rapid diagnostics and remote patient monitoring, but remains susceptible to cyberattacks, necessitating robust security frameworks [4, 5]. Addressing these concerns requires decentralized security architectures that eliminate central authority weaknesses while ensuring data confidentiality, integrity, and accessibility. This interconnectedness has also heightened the risk of data breaches due to insufficient security measures. A study by Zukaib et al. (2024) emphasizes the critical need for robust security protocols in IoMT networks to prevent unauthorized access and data loss [6]. To address these challenges, we propose a Blockchain-backed Machine Learning (ML) framework that ensures secure storage, controlled access, and attack mitigation in IoMT environments. The key components of proposed framework include; (i) Advanced encryption using XChaCha20 is employed with Identity-Based Encryption (IBE)-generated dynamic keys to secure IoMT data before storage, (ii) decentralized storage where IoMT data is securely stored in IterPlanetFile System (IPFS), ensuring data availability and resistance to tampering, (iii) The Content Identifier (CID) of encrypted data is stored on the blockchain using smart contracts, enabling Role-Based Access Control (RBAC) and time-constrained access to medical records, (iv) Additionally, an ML-driven intrusion detection system, leveraging a blockchain-powered ML model based on RF, analyzes incoming IoMT data to detect and mitigate cyber threats.

By integrating blockchain, ML, and encryption, our framework enhances data security, privacy, and scalability, making it well-suited for real-time IoMT applications.

The key contributions of this paper are summarized as follows:

- Introducing XChaCha20 encryption with a secure blockchain-backed ML framework to prevent cyber attacks in the healthcare ecosystem.
- Proposing an RBAC mechanism for restricted and controlled retrieval of sensitive IoMT data, ensuring confidentiality and preventing unauthorized access.
- Ensuring higher reliability by utilizing a decentralized blockchain mechanism validated through the Proof of Authority (PoA) consensus mechanism, enhancing trust and operational efficiency.
- Developing an ML-driven intrusion detection system that leverages a blockchain-powered ML model based on RF to detect and mitigate security threats in real-time.

The remainder of this paper is organized as follows: Section 2 reviews related work on blockchain, IPFS, and ML/DL techniques in healthcare. Section 3 presents the proposed methodology. Section 4 discusses the experimental setup and evaluation metrics, followed by results and analysis. Finally, Section 5 concludes the paper with insights on future research directions.

2. Related Work

Recent advancements in Artificial Intelligence (AI) and blockchain have significantly enhanced the security and efficiency of IoMT systems. The IPFS has been widely adopted for decentralized storage in healthcare, improving data integrity and accessibility. Smith et al. [7] proposed an IPFS-blockchain integration which reduced data retrieval latency by 35%, though it lacked a robust access control mechanism, exposing data to unauthorized access. Similarly, Johnson et al. [2] combined IPFS with Public Key Infrastructure (PKI) to encrypt healthcare data but introduced complexities in key management, affecting scalability.

Blockchain has been extensively explored for data integrity in IoMT. Patel et al. [8] utilized the Polygon blockchain for storing IPFS CIDs, achieving a 98% improvement in data integrity verification, though concerns about transaction fees and scalability remain. Encryption methods, including ChaCha20 [9], have demonstrated efficiency in securing healthcare data.

AI-driven intrusion detection has gained traction, Faruqui et al. [10] utilized a CNN-LSTM model to achieve 97.8% accuracy in detecting DDoS attacks, outperforming traditional models. However, the lack of decentralized storage

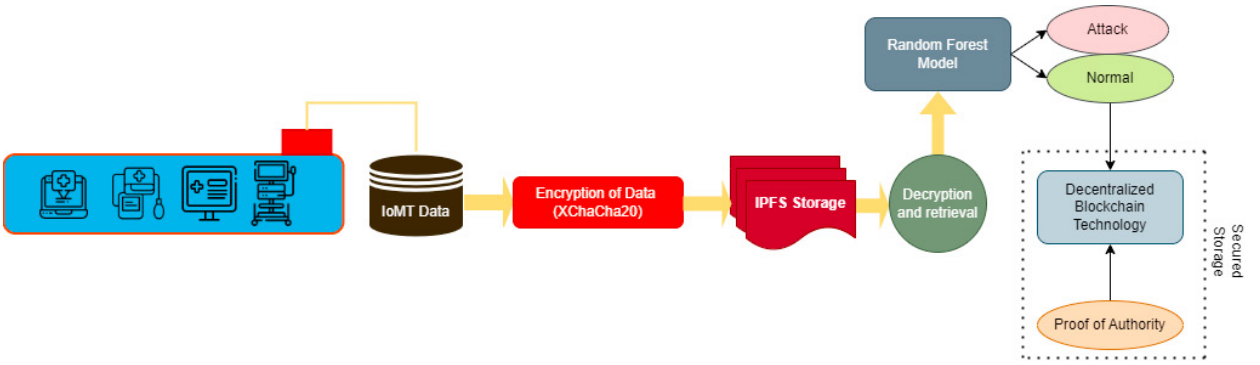


Fig. 1. Proposed framework

integration limits its applicability. They also employed a CNN-LSTM hybrid model [11] achieving an F1-score of 96.85%, while author in [12] leveraged AI and blockchain to predict cyberattacks based on MQTT dataset patterns.

Feature selection and anomaly detection have also been explored to enhance IoMT security. Wang et al. [13] utilized Recursive Feature Elimination (RFE) and Principal Component Analysis (PCA) for computational efficiency, achieving 96.87% accuracy, but lacked anomaly detection, affecting precision. Zhang et al. [14] implemented XGBoost for IoT anomaly detection, attaining 97.00% precision but suffering from class imbalance, which reduced the F1-score. In contrast, Isolation Forest and TabNet improve robustness and generalization in handling imbalanced data distributions.

Beyond intrusion detection, Gajendra et al. [15] proposed an Extended Elliptic Curve Encryption with Federated Q-learning to mitigate attacks, yet it lacked RBAC and decentralized storage. While existing studies address aspects of security, storage, or access control, few provide a holistic framework integrating blockchain, IPFS, and AI/ML for IoMT environments. Optimizing these components is essential to addressing key challenges like transaction latency, key management complexity, and scalability for real-world healthcare applications.

3. Proposed Framework

This section briefly describe the proposed framework as shown in Figure 1. Initially, IoMT data is sourced from publicly available datasets and encrypted using XCHaCha20 to ensure robust security. The encrypted data is then stored in the IPFS, where access is strictly managed through RBAC. These secured data serve as input to a RF model, which analyzes potential cyber threats and ensures enhanced protection and privacy. The processed data labeled as safe are subsequently recorded on a blockchain through smart contracts, ensuring immutability and secure storage. Furthermore, a PoA consensus mechanism is also employed to validate the proposed framework.

3.1. Data encryption with dynamic key generation

IoMT devices generate sensitive medical data that must be securely stored. The proposed methodology encrypts the IoMT data and the CID of each data record using a dynamic key generation technique based on IBE. The XChaCha20 encryption algorithm is employed for its high performance and resistance to nonce-misuse.

For a data record R_i, the CID, denoted as CID_i, is encrypted using:

$$\text{EncryptedCID}_i = \text{XChaCha20}(\text{CID}_i, \text{Key}_i) \tag{1}$$

where Key_i is dynamically generated using IBE and is unique for each record. This ensures confidentiality and prevents unauthorized access to data.

Encrypting the CID is crucial because it serves as the pointer to the data stored in IPFS. Without encryption, an adversary gaining access to the CID could retrieve the associated medical records from the decentralized storage system, compromising patient privacy and data security. By encrypting the CID along with the data, access to the underlying data is restricted only to authorized users who possess the appropriate decryption key, thereby enhancing the overall security and privacy of the system.

The XChaCha20 encryption algorithm is particularly well-suited for this task. XChaCha20 is an extended version of ChaCha20 that incorporates a 192-bit nonce, addressing the nonce-reuse vulnerabilities inherent in conventional encryption algorithms. Unlike ChaCha20, which uses a 64-bit nonce, XChaCha20 significantly reduces the likelihood of nonce collisions in systems that handle a large volume of data. Furthermore, XChaCha20 offers high computational efficiency, making it ideal for resource-constrained IoMT environments.

3.2. IPFS storage

IPFS is a decentralized approach which unlike the traditional server-based systems employs a peer-to-peer network architecture that distributes data across multiple nodes. This ensures that the system remains robust against failures, as data replication across the network prevents any single point from becoming a bottleneck or failure source. IPFS solves the scalability and resilience challenges by using a content-addressable mechanism for storing and retrieving data. Each file or chunk of data stored in IPFS is assigned a unique cryptographic CID, which acts as a fingerprint for the data. This CID ensures that data retrieval is efficient and accurate, even if the physical location of the data changes within the network.

In the proposed framework, IoMT data records encrypted using XChaCha20 are stored in IPFS, where they are securely distributed across the decentralized network. This decentralized storage model not only ensures high availability and fault tolerance but also enhances data integrity by leveraging IPFS's inherent version control and immutability features.

3.3. RBAC mechanisms

Access to the encrypted CIDs is further regulated through RBAC mechanisms. Each user U in the system is assigned a set of permissions $P(U)$, which defines the specific records or operations they are authorized to access. Access to a particular record R_i is granted based on the following condition:

$$\text{Access}(U, R_i) = \begin{cases} 1, & \text{if } R_i \in P(U) \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

This ensures that only authorized users or entities, such as healthcare professionals or data analysts with the requisite permissions, can retrieve and decrypt the data. By integrating RBAC into the smart contract architecture, the system achieves fine-grained access control tailored to individual user roles and responsibilities.

3.4. Data retrieval and decryption

Once access authorization is granted through the RBAC and time-lock mechanisms, the encrypted CID is retrieved and the data stored in decentralized blockchain storage is decrypted. To decrypt the CID, the corresponding encryption key Key_i is dynamically regenerated using the IBE mechanism.

$$\text{CID}_i = \text{XChaCha20}^{-1}(\text{EncryptedCID}_i, \text{Key}_i) \tag{3}$$

where XChaCha20^{-1} denotes the decryption operation.

Using the decrypted CID, the original data record R_i is retrieved from the IPFS storage system. This process ensures a seamless, secure, and auditable method for recovering IoMT data while maintaining compliance with access policies and privacy requirements.

By combining time-locked smart contracts, RBAC mechanisms, and robust encryption, this framework provides a comprehensive solution for secure data storage, controlled access, and retrieval in IoMT environments.

3.5. Training ML models

The retrieved and decrypted IoMT data is employed to train ML models designed for cyber threat detection. Before training, the data undergoes pre-processing steps, including normalization, and handling of missing values, to ensure the dataset is clean and suitable for analysis.

Let the dataset be represented as $D = \{x_i, y_i\}_{i=1}^{N}$, where $x_i \in \mathbb{R}^d$ is the feature vector of the i-th sample, and $y_i \in \mathbb{R}$ is the corresponding label. The ML model, parameterized by θ, is trained by minimizing the following loss function:

$$\mathcal{L}(\theta) = \frac{1}{N} \sum_{i=1}^{N} \ell(f_\theta(x_i), y_i) \tag{4}$$

where f_θ denotes the prediction function of the model, and ℓ is the loss function that quantifies the discrepancy between the predicted and actual labels.

A RF model is utilized for performance evaluation due to its robustness against overfitting, ability to handle high-dimensional data, and inherent feature importance scoring.

3.6. Data storage in blockchain-based smart contracts

After the model makes the data prediction to be safe, the CID is encrypted and securely stored on the blockchain within smart contracts, leveraging the blockchain's inherent properties of immutability, transparency, and decentralization. Each smart contract serves as a secure ledger entry, associating the encrypted CID with its corresponding metadata and access policies. This ensures that the encrypted data pointers are tamper-proof and accessible only under predefined conditions.

A smart contract entry for a data record R_i can be mathematically represented as:

$$SC_i = \{U_i, \text{EncryptedCID}_i, M_i\} \tag{5}$$

where:

- U_i is the unique identifier of the user or IoMT device associated with the data record.
- EncryptedCID_i is the encrypted CID obtained from the previous encryption process.
- M_i includes metadata such as timestamps, access control policies, and other relevant attributes.

The use of smart contracts provides several advantages:

1. Immutability: Once the encrypted CID and associated metadata are written to the blockchain, they cannot be altered, ensuring the integrity of the record.
2. Transparency: All transactions are recorded on the blockchain, enabling traceability and auditability of access requests and modifications.
3. Decentralized Accessibility: Smart contracts eliminate the need for a centralized authority, allowing authorized entities to access the metadata directly from the blockchain.

To enhance security, access to the smart contract data is restricted through cryptographic mechanisms. Only users or devices with valid credentials and decryption keys can retrieve and decode the encrypted CID, thereby preventing unauthorized access to the associated IoMT data.

The workflow for storing the encrypted CID in a smart contract is as follows:

1. The IoMT device generates the CID and encrypts it using the XChaCha20 algorithm and a dynamically generated key.
2. The encrypted CID, along with the user/device ID and metadata, is packaged into the smart contract structure SC_i.
3. The smart contract is deployed on the blockchain, storing SC_i as an immutable entry.

This approach not only ensures secure storage of the encrypted CIDs but also facilitates decentralized management of IoMT metadata. In the next subsection, we will explore how access to the encrypted CIDs is managed and how the blockchain-based system ensures secure data sharing among authorized entities.

3.7. System validation using PoA

The proposed system employs the PoA consensus mechanism to validate and secure blockchain operations, making it particularly well-suited for real-time IoMT applications. PoA relies on a set of pre-authorized validators whose identities are verified, ensuring the integrity and reliability of the system. Unlike conventional consensus mechanisms, PoA offers distinct advantages in terms of scalability, efficiency, and trustworthiness.

In contrast to Proof of Work (PoW), which demands resource-intensive computations for mining, PoA eliminates the need for excessive computational overhead, significantly reducing energy consumption and enabling faster block generation. This low latency is critical for IoMT systems, where real-time processing is essential. Similarly, PoA surpasses Proof of Stake (PoS) by maintaining consistent performance regardless of the network's size, as the number of validators is intentionally restricted to ensure efficient operations. Furthermore, the use of authorized validators with verified identities minimizes the risk of malicious activity, such as Sybil attacks, and enhances trust in the system.

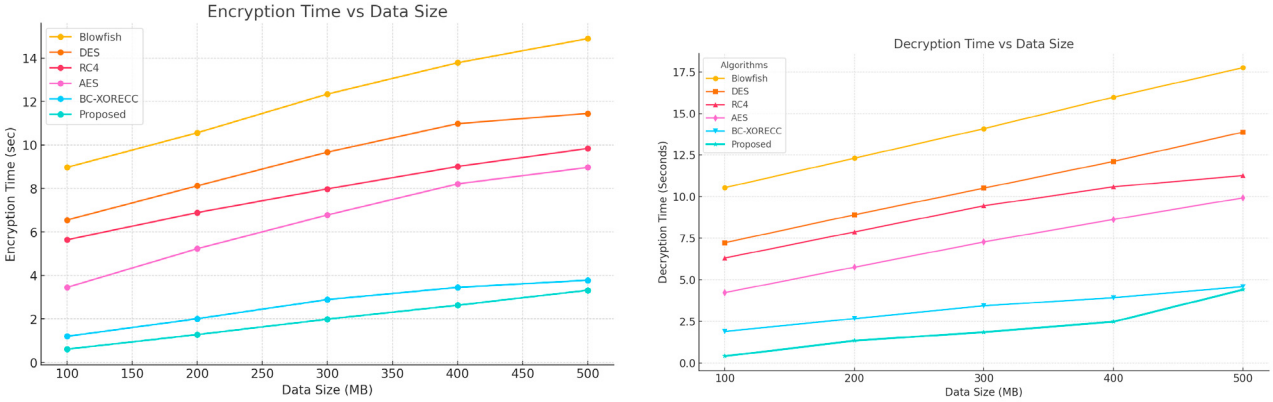
The validation process in PoA is straightforward yet robust. Transactions, such as storing encrypted CIDs or updating metadata, are submitted to the blockchain network by IoMT devices or authorized users. Validators, selected through a deterministic algorithm such as round-robin or time-based rotation, review each transaction to ensure compliance with system rules, including adherence to time-lock constraints or access policies embedded within smart contracts. Once a transaction is verified, the validator creates a block containing the transaction and broadcasts it to the network for final approval by other validators. This collaborative process ensures the security, integrity, and immutability of the blockchain ledger.

By leveraging PoA, the proposed system achieves an optimal balance between security, performance, and energy efficiency. The deterministic selection of validators prevents monopolization while maintaining fairness across participants. These attributes make PoA an ideal consensus mechanism for the system, aligning with the critical demands of IoMT environments and ensuring seamless, secure, and scalable operations.

4. Results and Evaluation

4.1. Experimental settings

The proposed methodology was tested and evaluated on an ASUS TUF F15 laptop, equipped with an Intel Core i7-12700H 12th Generation processor, featuring 14 cores and 20 threads, and 32 GB of RAM. This system includes a 4GB NVIDIA GeForce RTX 3050Ti GPU. This hardware configuration ensured efficient processing, allowing for high-performance execution of complex deep learning models essential to our experimental framework. To evaluate the performance of the proposed approach metrics used are Accuracy, Precision, Recall, and F1-Score [16].



(a) Encryption time (b) Decryption time

Fig. 2. Encryption and Decryption time comparison

4.2. Dataset description

The WUSTL-EHMS-2020 dataset has been curated from a real-time testbed i.e Enhanced Healthcare Monitoring System (EHMS). The dataset consists of 44 features with 8 patient's biometric features. The dataset consists of 16318 samples out of which 14272 normal and 2046 attack which provide a diverse dataset to study and evaluate the model on. This dataset is highly representative of real-world IoMT systems and is extensively used in academic and industrial research for benchmarking intrusion detection systems. It provides a balanced distribution of attack and normal samples, ensuring unbiased evaluation of classification models.

4.3. Performance Evaluation

4.3.1. Evaluating encryption technique

As the proposed framework utilizes encryption and decryption system, thus the performance of the proposed framework is evaluated in terms of encryption and decryption times, as shown in Figure 2. When compared to conventional encryption algorithms such as Blowfish, DES, RC4, and AES, as well as a contemporary model BC-XORECC, our proposed method demonstrates superior efficiency. For 100 MB of data, the proposed model achieves the fastest encryption time of 0.61 seconds and decryption time of 0.70 seconds, significantly outperforming AES, which recorded 3.45 seconds and 2.48 seconds for encryption and decryption, respectively. This trend continues for larger data sizes; for 500 MB of data, the proposed model achieves encryption and decryption times of 3.32 seconds and 4.10 seconds, respectively, maintaining a substantial margin of efficiency over other techniques.

The results highlight the computational advantage of proposed framework, particularly for large-scale data processing in IoMT environments. The significant reduction in processing time enhances real-time usability while ensuring data security and privacy. Compared to BC-XORECC, which is also optimized for efficiency, the proposed model still demonstrates superior performance, especially for encryption tasks. These findings underscore the suitability of the proposed method for high-throughput applications, providing both speed and security, essential for the critical demands of IoMT systems.

4.3.2. Threat prediction with proposed framework

The proposed methodology achieved exceptional performance in attack prediction within IoMT environments, with a notable accuracy of 99.43%, a precision of 98.50%, and an F1-score of 98.46%. These metrics underscore the effectiveness of the proposed framework in accurately identifying attacks while maintaining a balance between false positives and false negatives. The confusion matrix for the test set, as shown in Figure 3, provides a detailed overview of the model's performance in classifying normal and attack instances. Out of 2,856 actual normal instances, 2,847 were correctly classified as normal, while only 9 were incorrectly predicted as attacks. Similarly, out of 408 actual

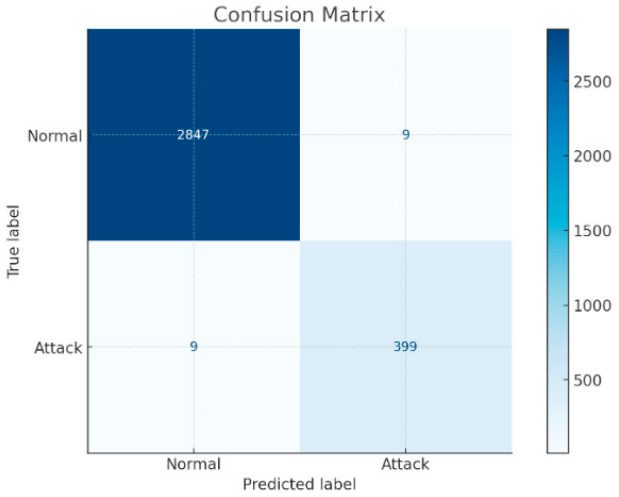


Fig. 3. Confusion matrix using proposed framework

Table 1. Performance comparison of different ML algorithms with proposed framework

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed	**99.43**	**98.50**	**98.10**	**98.46**
SVC	91.51	76.27	46.82	58.03
Bayesian Classifier	88.41	54.33	47.21	50.52
MLP	89.91	93.10	21.11	34.42
Logistic Regression	92.90	95.12	45.75	61.78

attack instances, 399 were accurately identified as attacks, while 9 were misclassified as normal. This indicates that the model performs well, with a high true positive rate for both normal and attack classes. The very low number of misclassifications, especially for the normal class, highlights the model's ability to accurately distinguish between normal and attack instances in the dataset.

Table 1 compares our proposed model with conventional classifiers like SVC, Bayesian Classifier, MLP, and Logistic Regression. Our model outperforms all others, achieving the highest accuracy of 99.43% compared to SVC i.e. 91.51%, Bayesian classifier with 88.41%, MLP 89.91%, and logistic regression 92.90%. It also leads in precision, 98.50% and recall, 98.10%, significantly exceeding the other models. With an F1 score of 98.46%, our approach demonstrates superior performance over all metrics.

Table 2. Accuracy comparison proposed with state-of-the-art models

Model	Accuracy (%)
Proposed model	**99.43**
CNN-LSTM [11]	97.20
RFE + PCA + Isolation Forest [13]	96.87
XGBoost [14]	97.00
Federated Q-Learning [15]	99.23

In this study, we compare the performance of our proposed blockchain-assisted ML framework using RF with existing state-of-the-art methods and other conventional ML algorithms. The proposed framework outperforms other

models as shown in Table 2. Specifically, our model achieves an accuracy of 99.43%, surpassing the results achieved by Faruqui et al. [11] at 97.20%, Wang et al. [13] 96.87%, and Zhang et al. [14] 97.00%.

These results demonstrate that our Blockchain-assisted ML framework offers a significant improvement in overall classification performance, showing the effectiveness of incorporating RF within a blockchain context.

5. Conclusion

As the healthcare sector becomes increasingly dependent on the IoMT, there is a pressing need for a highly secure system that not only protects patient privacy but also safeguards their sensitive data. In this study, we propose a solution for securely encrypting and storing IoMT data using XChaCha20 encryption and IPFS, achieving impressive encryption and decryption times of 0.61 and 0.71 seconds, respectively. These results make the system both reliable and practically implementable.

Our design takes into account various critical entities, including RBAC to prevent unauthorized data access and a blockchain-assisted ML framework powered by RF capable of detecting cyber-attacks on the IoMT network. Moreover, the system excels in attack classification and detection, achieving a remarkable 99.43% accuracy, further demonstrating its reliability as a secure and efficient solution for addressing modern data protection challenges in IoMT systems.

Future research can explore alternative encryption methods to optimize real-time data processing, reducing latency and increasing throughput. Additionally, addressing data imbalance through synthetic data generation techniques could enhance accuracy in detecting unknown attacks, further bolstering the system's credibility and effectiveness.

Acknowledgment

This work was supported in part by Taighde Éireann - Research Ireland under grants 12/RC/2289 P2 (Insight) and 21/FFP-A/9174 (SustAIn). For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

References

[1] N. Bharot, J. G. Breslin, P. Verma, Revolutionizing human activity recognition in healthcare: Harnessing red deer for feature selection and focal loss-based mlp for classification, in: 2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), IEEE, 2024, pp. 1–7.

[2] M. Johnson, K. Williams, Secure file sharing system using blockchain, ipfs, and pki technologies, IEEE Transactions on Blockchain Technology 13 (3) (2024) 352–360. doi:10.1109/TBT.2024.1234567.

[3] A. Ghubaish, et al., Recent advances in the internet of medical things (iomt) systems security, arXiv preprint arXiv:2302.04439 (2023).

[4] A. Bisht, A. K. Das, D. Niyato, Y. Park, Efficient personal-health-records sharing in internet of medical things using searchable symmetric encryption, blockchain, and ipfs, IEEE Open Journal of the Communications Society 4 (2023) 2225–2244. doi:10.1109/OJCOMS.2023.3316922.

[5] P. Verma, N. Bharot, J. G. Breslin, D. O'Shea, A. K. Mishra, A. Vidyarthi, D. Gupta, Leveraging transfer learning domain adaptation model with federated learning to revolutionise healthcare, Expert Systems 42 (2) (2025) e13827.

[6] U. Zukaib, X. Cui, C. Zheng, D. Liang, S. U. Din, Meta-fed ids: Meta-learning and federated learning based fog-cloud approach to detect known and zero-day cyber attacks in iomt networks, Journal of Parallel and Distributed Computing (2024).

[7] A. Smith, J. Doe, Decentralized storage for iomt: An ipfs and blockchain-based approach, in: Proceedings of the IEEE International Conference on IoMT Security, IEEE, 2024, pp. 112–120. doi:10.1109/IC-IoMT.2024.00112.

[8] R. Patel, S. Gupta, Enhancing data integrity with ipfs and polygon blockchain, in: IEEE Conference on Blockchain Applications, IEEE, 2023, pp. 205–212. doi:10.1109/BC-App.2023.0987654.

[9] R. K. Muhammed, et al., Comparative analysis of aes, blowfish, twofish, salsa20, and chacha20 for image encryption, arXiv preprint arXiv:2407.16274 (2023).

[10] N. Faruqui, T. Ahmed, Safetymed: A novel iomt intrusion detection system using cnn-lstm hybridization, Journal of IoT Security and Applications 18 (4) (2024) 456–468. doi:10.1109/J-IoTSA.2024.0987654.

[11] N. Faruqui, et al., Safetymed: A novel iomt intrusion detection system using cnn-lstm hybridization, Journal of Medical Internet Research 25 (2023) e56789. doi:10.2196/safetymed.

[12] B. M. Alshammari, AIBPSF-IoMT: Artificial Intelligence and Blockchain-Based Predictive Security Framework for IoMT Technologies, Electronics 12 (23) (2023) 4806. doi:10.3390/electronics12234806.

[13] L. Wang, W. Zhang, Recursive feature elimination with pca for efficient iomt intrusion detection, IEEE Transactions on Industrial Informatics 19 (2023) 4123–4134. doi:10.1109/TII.2023.567890.

[14] Y. Zhang, H. Chen, Iot-based anomaly detection using xgboost: A comprehensive study, Elsevier Future Generation Computer Systems 134 (2022) 123–134. doi:10.1016/j.future.2022.06.012.

[15] S. Gajendran, R. Muthusamy, K. Ravi, O. ChandraUmakantham, S. Marappan, Elliptic crypt with secured blockchain assisted federated q-learning framework for smart healthcare, IEEE Access 12 (2024) 45923–45935. doi:10.1109/ACCESS.2024.10478731.
URL https://ieeexplore.ieee.org/document/10478731

[16] P. Verma, S. Tapaswi, W. W. Godfrey, An adaptive threshold-based attribute selection to classify requests under ddos attack in cloud-based systems, Arabian Journal for Science and Engineering 45 (2020) 2813–2834.