International Journal of Applied Smart Interdisciplinary Technologies (IJASIT)

Home Page: https://ijasit.org **ISSN: 3139-759X**

https://doi.org/10.68104/ijasit.v1.i3.39

IoT-Blockchain Integration for Secure Smart Healthcare: Neural-Enhanced Encryption and Hybrid Anomaly Detection

Tanishka Pahwa[1], Geet Bawa[2, *]

[1] Department of Computer Science and Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India. *tanishka.2602051704@muj.manipal.edu*

[2] Department of Computer Science, Khalsa College for Women, Amritsar, Punjab, India, *geetbawa_mca@yahoo.co.in*

*** Corresponding author.**
E-mail: *geetbawa_mca@yahoo.co.in*

Article History:
Received Date: 13 August 2026
Revised Date: 26 August 2026
Accepted Date: 09 September 2026
Published Date: 14 September 2026

Keywords: *Internet of Things (IoT); Blockchain; Smart Healthcare; Anomaly Detection; Machine Learning; Data Security*

ABSTRACT

Background: The application of the Internet of Things (IoT) in healthcare has allowed continuous patient surveillance, data acquisition, and analytics for better patient care. However, the amount of healthcare data generated by IoT devices has created several security and privacy concerns related to information's confidentiality, integrity, and scalability in the health care system. **Problem Statement**: The current healthcare system lacks mechanisms to ensure data confidentiality, integrity, and effective monitoring of real-time patient statistics while providing efficient and effective healthcare services. In addition, the conventional security measures may not be sufficient to detect various forms of attacks in a real-time healthcare IoT environment. **Purpose**: This paper proposes an efficient and reliable healthcare framework that addresses several IoT-related security issues while ensuring confidentiality and integrity of health data and providing effective anomaly detection. **Methods**: The study presents a framework that uses a combination of IoT, blockchain, artificial intelligence, and neural-enhanced encryption to offer a more secure and reliable healthcare system. It utilizes neural networks to provide encryption and implement an anomaly detection model that uses a hybrid long short-term memory autoencoder and support vector machine detecting abnormal physiological observations in IoT-generated healthcare data. In addition, the framework uses a modified proof-of-authority consensus algorithm to ensure faster transaction validation and reliable processing in a permissioned blockchain network. The framework has been tested using simulated healthcare IoT networks with 150, 600, and 1200 nodes and a database with 1200 patient records. **Results**: The proposed framework achieved an anomaly detection accuracy of 98.99% with 0.89 precision, 0.93 recall, and 0.91 F1-Score. Besides, the framework detected 95% of the attacks and maintained optimal performance in the networks with varying node numbers. **Conclusion**: The study revealed that the combination of IoT, blockchain, intelligent anomaly detection, and neural-enhanced encryption could be an efficient and reliable solution to the current health care issues. The proposed framework offers several benefits, including improved confidentiality and integrity of health data, improved attack detection, and efficient and effective processing of transactions in a permissioned blockchain network.

1. Introduction

Recent developments in smart healthcare technologies have considerably reshaped how medical services are delivered, monitored, and managed [1]. The growing adoption of digital healthcare systems, remote monitoring, and personalized medicine has created new opportunities for improving efficiency in patient healthcare [2]. However, despite these advancements, traditional healthcare systems face several challenges, such as centralized data management, lack of real-time monitoring, limited interoperability, and vulnerability to cyber threats. These issues become more critical with the increasing reliance on data-driven healthcare solutions [1].

The integration of the Internet of Things (IoT) into healthcare has enabled continuous and real-time monitoring of patient health through wearable devices and smart sensors [3]. These devices produce diverse and time-dependent healthcare data at a large scale, including vital parameters such as heart rate, blood pressure, oxygen levels, and body temperature [4]. While IoT enhances accessibility and automation in healthcare, it also introduces significant concerns related to data privacy, security, and trust. Patient data transmitted across networks and stored in centralized architectures remains highly exposed to security threats and unauthorized access [5].

To address these challenges, blockchain technology has emerged as a promising solution for secure and decentralized data management in healthcare systems. Blockchain technology offers a decentralized and tamper-resistant ledger system where transactions are recorded transparently and cannot be altered once validated [6]. This facilitates data integrity, traceability, and trust among multiple stakeholders, including patients, healthcare providers, pharmacies, and insurance companies. Additionally, the use of cryptographic techniques and consensus mechanisms enhances security and eliminates reliance on centralized authorities. This also reduces the risk of single-point failures [7-9].

Despite the advantages of IoT and blockchain integration, several limitations persist in existing solutions. Most frameworks primarily focus on secure data storage and access control, but neglect intelligent threat detection and adaptive mechanisms of security [10]. Furthermore, the increasing volume and complexity of healthcare data make real-time processing, scalability, and efficient anomaly detection a difficult task. Additionally, traditional security mechanisms often fail to detect evolving cyber-attacks in dynamic IoT environments [11].

Artificial intelligence (AI) has the potential to address these limitations by enabling intelligent data analysis, pattern recognition, and anomaly detection [12]. Machine learning and deep learning models can learn complex temporal patterns in healthcare data and identify abnormal behaviours that may indicate cyber threats or system failures. However, integrating AI with blockchain and IoT in an efficient manner remains a challenging task [13].

In this context, this research proposes a secure and scalable hybrid healthcare framework that integrates IoT, blockchain, and artificial intelligence to address the limitations of existing systems. This integration has been presented in Figure 1. The Organization#1 develops IoT-enabled healthcare sensors that interact with patients using IoT protocols and help in collecting real-time patient health data, including heart rate, temperature, oxygen level, etc. These sensors send the collected data to cloud services for storage using web service APIs that act as a bridge between sensors and the cloud. These web services are managed by Organization#2. Another Organization#3 provides cloud storage to store patient data securely. They also host various services for data access. The collected data is then analysed using artificial intelligence to extract useful insights that help in predicting diseases and monitoring health. The artificial intelligence algorithms are provided by Organization#4. These algorithms analyse patient data to detect patterns and generate insights. This integrated system ensures secure data sharing, automation, and intelligent healthcare decision-making.

The proposed framework incorporates a neural-enhanced encryption mechanism in which the Elman Neural Network generates a transaction-dependent neural representation that is transformed into a dynamic encryption key for the subsequent Blowfish encryption process. Additionally, a hybrid anomaly detection model based on Long Short-Term Memory (LSTM) and Support Vector Machine (SVM) is employed to detect malicious activities and abnormal patterns in healthcare data.

To ensure efficient and low-latency transaction validation, a customized Proof-of-Authority (PoA) consensus mechanism is adopted, where domain-specific entities such as hospitals, laboratories, and pharmacies act as

trusted validators. This approach enhances performance, reduces computational overhead, and facilitates secure participation within a permissioned blockchain environment. The proposed framework is evaluated using a simulated IoT-based healthcare dataset and demonstrates improved performance in terms of security, anomaly detection accuracy, computational efficiency, and scalability.

Overall, this work contributes toward the development of a robust, intelligent, and secure healthcare ecosystem that supports real-time monitoring, reliable decision-making, and trustworthy data management in modern smart healthcare environments.

Fig. 1. IoT-enhanced Hybrid Healthcare System

1.1 Significance of Research

The integration of blockchain and Internet of Things technologies has emerged as an efficient solution to address challenges in modern healthcare systems. The decentralized and immutable characteristics of blockchain significantly strengthen data security and integrity. It ensures that the medical data cannot be altered or deleted once it is recorded on the blockchain. This minimizes the possibility of data manipulation and unauthorized usage and thus improves the reliability of healthcare information systems. Additionally, the use of blockchain reduces administrative overhead and operational costs by eliminating intermediaries and automating processes through smart contracts.

Figure 2 highlights how IoT and blockchain work together to securely manage healthcare data and logistics between different hospitals. Smart wearable devices and monitoring systems equipped with IoT sensors continuously capture real-time patient information. This data, along with logistics information, is securely stored on decentralized and distributed blockchain nodes. The logistics information contains transport and supply chain data, such as medicine delivery, equipment transfer, and organ transport. Every blockchain node securely records transactions, verifies their authenticity, and keeps a synchronized copy of the ledger. The patient data is safely shared between multiple healthcare centres. Thus, this integrated framework ensures decentralization by avoiding a single point of failure. The encryption and decryption of data ensure security. Furthermore, the framework ensures transparency by making all the transactions traceable. Additionally, hospitals can share data easily, ensuring interoperability. Real-time access assists in faster decision-making. The framework also ensures a trustworthy environment and enhances compatibility between different healthcare systems.

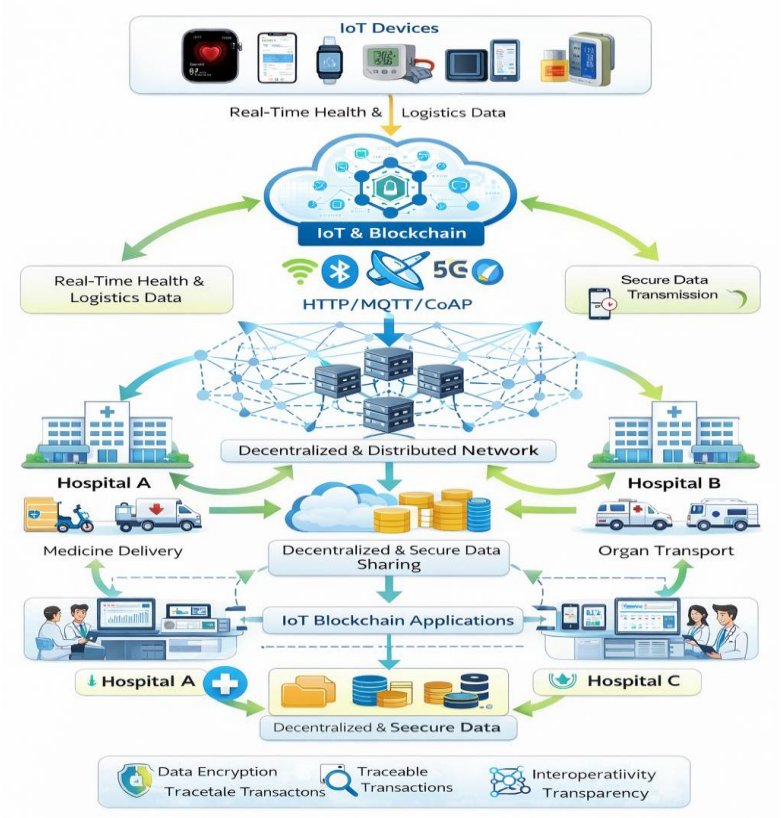

Fig. 2. IoT-Blockchain Integrated Hybrid Framework for Healthcare Data Management

Despite these advancements, existing healthcare systems face several challenges, including data privacy risks, cyber-attacks, and redundant records. Furthermore, the increasing volumes of multimedia healthcare data generated by IoT devices further make secure data storage and real-time processing more complex. These limitations highlight a need for a robust, secure, and intelligent framework that can efficiently manage healthcare data while ensuring privacy, scalability, and reliability.

1.2 Contribution of Work

The novelty of this work lies not in the individual use of IoT, blockchain, Blowfish, neural networks, or anomaly-detection algorithms, which have been studied independently in previous healthcare systems, but in their integration into a unified security architecture with an explicit neural-to-cryptographic coupling. In particular, the proposed framework uses the Elman Neural Network to generate a transaction-dependent representation that is deterministically transformed into a dynamic key supplied to the Blowfish encryption stage. In parallel, an LSTM autoencoder and SVM form a two-stage physiological anomaly-detection module, while a customized Proof-of-Authority mechanism supports transaction validation in the permissioned blockchain. This combination provides a unified architecture covering data acquisition, adaptive encryption, anomaly detection, transaction validation, and tamper-resistant storage The major contributions of this research work have been summarized as follows:

- A secure and scalable hybrid healthcare framework has been proposed that integrates Internet of Things, blockchain technology, and artificial intelligence to ensure efficient and reliable healthcare data management.
- A neural-enhanced Blowfish encryption mechanism has been developed in which the Elman Neural Network generates a transaction-dependent neural representation that is transformed into a dynamic encryption key before Blowfish encryption, establishing an explicit mathematical coupling between neural processing and symmetric encryption.
- A hybrid two-stage anomaly detection model has been developed using LSTM autoencoder reconstruction-error features and SVM classification to identify abnormal physiological observations. Network-level attacks are evaluated separately through the simulated network security layer.

- A customized Proof-of-Authority consensus mechanism has been utilized that is specifically designed for healthcare environments. It allows faster transaction validation, reduced latency, and improved energy efficiency.
- The framework has been evaluated using a synthetic IoT-based healthcare dataset with 1200 records to preserve healthcare data privacy.
- A statistical and quantitative comparative analysis with existing approaches under a similar domain has been performed, which demonstrates its improved performance in terms of security, anomaly detection accuracy, computational efficiency, and scalability.

Table 1 provides a comparative analysis of the proposed framework with existing ones, highlighting its novel contributions.

Table 1
Comparative Analysis

Feature	Traditional Approach	Proposed Framework	Contribution of Work
Encryption Process	Standard encryption methods, such as Elliptic Curve Cryptography/Advanced Encryption Standard/Blowfish, are used separately without integration.	Integrates Elman neural-enhanced Blowfish encryption with blockchain-based transactions.	Adds intelligence to encryption, making it more adaptive and secure.
Static/Dynamic Encryption	Use static encryption settings.	Encryption is dynamically adjusted using neural networks.	Improves robustness.
Threat Detection	Use one-step detection on raw or semi-processed data.	Use a two-step detection process on encrypted blockchain data patterns.	Detects threats more effectively.
Blockchain Scope	Use blockchain for storing and controlling access to data.	Use blockchain as an active security mechanism for tracking, validating, and resisting attacks.	Blockchain allows an active defense mechanism and not just a storage database.
Consensus Algorithm	Use a general non-health-based consensus algorithm.	Use a healthcare-specific, customized Proof-of-Authority consensus algorithm for faster and more efficient healthcare applications.	Customized consensus algorithm.
Evaluation Criteria	Tested with artificial or limited data.	Tested using a controlled synthetic healthcare dataset and simulated network threat scenarios.	Controlled and reproducible proof-of-concept evaluation.

2. Literature Review

This section reviews previous research on the application of IoT and blockchain in the healthcare sector. Researchers have studied the benefits of these technologies, especially in the management of multimedia data related to healthcare.

BlockMedCare, developed by Azbeg et al. (2022), is an existing integrated system for healthcare that uses IoT, blockchain, and InterPlanetary File System (IPFS) for secure monitoring of patients, especially for chronic diseases. The system used Internet of Things devices to obtain health information promptly. It used blockchain to make sure that information is handled transparently. IPFS is used to store information and helps to reduce the amount of work that the blockchain network has to do. BlockMedCare helped to keep health information

safe and private. It also made it easier to access this information by the authorized stakeholders. Evaluation results highlighted that BlockMedCare works better and can handle information more efficiently than other systems. The study showed that using these technologies together can be a good way to keep healthcare information safe.

Another framework, named BCHealth, developed by Hossein et al. (2021), is a blockchain-based system that helps keep data private in healthcare systems and uses the Internet of Things technology. This system uses blockchain and encryption to protect data while still allowing access to it. BCHealth tackled issues like keeping data confidential, making sure data is not altered, and sharing data safely among different people involved in healthcare. Evaluation results showed the cost efficiency of BCHealth. This model proved to be helpful, especially for healthcare applications that need to monitor patients promptly.

Teli & Masoodi, (2021), and Quasim et al., (2020), discussed the usage of blockchain technology in the healthcare system to enhance the security and privacy of medical data. The work highlighted that blockchain is a decentralized database and does not need the intervention of any third-party intermediary, thus reducing the data security risks. Blockchain ensured data integrity, transparency, and authorized access to medical data. Furthermore, cryptographically generated hash addresses and smart contracts ensured safe data sharing among the stakeholders. Both studies focused on the potential of blockchain in transforming traditional healthcare data management systems into a more secure and trustworthy environment.

Chinaei et al. (2021) introduced a blockchain logging contract mechanism for efficiently analyzing IoT-generated healthcare data. The work focused on improving the verification and trustworthiness of data in a distributed healthcare environment. It proposed efficient logging strategies to reduce the need for blockchain for storage and thus reduce the computational overhead. The framework also ensured the immutable storage of IoT-generated healthcare data. Evaluation of the framework demonstrated its scalability for large-scale IoT healthcare deployments.

Mohammed et al. (2021), Al-Marridi et al. (2024) and Al-Nbhany et al. (2024) discussed the integration of blockchain and IoT technologies to improve the security, efficiency, and reliability of healthcare systems and addressed the challenges such as unauthorized access and data breaches. The studies presented the importance of a decentralized database for allowing secure data communication among IoT-enabled healthcare devices. Furthermore, Al-Marridi et al. (2024) extended this integration by utilizing reinforcement learning techniques to optimize system performance, scalability, and resource allocation. Mohammed et al. (2021) focused on strengthening IoT-based healthcare infrastructure using blockchain, and Al-Nbhany et al. (2024) provided a comprehensive review of current trends, applications, and challenges in this domain. Collectively, these works presented the growing importance of integrating blockchain, IoT, and intelligent techniques for developing secure and efficient healthcare solutions.

3. Proposed Framework

Traditional healthcare systems suffer from a major issue of managing and tracking data. This is because medical-related records are stored centrally across multiple organizations. To overcome this issue, the proposed framework integrates blockchain, Blowfish encryption based on the Elman Neural Network, and anomaly detection to ensure secure, transparent, and decentralized handling of medical data. Figure 3 highlights the overall architecture of the proposed framework.

As presented in Figure 3, the patient layer contains IoT sensors that collect real-time patient healthcare data, such as heart rate, blood pressure, oxygen level, etc. The collected healthcare data is first encrypted using a hybrid encryption scheme before being stored securely on the blockchain. This hybrid encryption model consists of two components, namely, the Elman Neural Network, which acts as an intelligence layer that adjusts the encryption process dynamically. The second component is Blowfish, which performs the actual encryption and converts data into a secure ciphertext. The blockchain layer consists of miners or validator nodes that verify transactions, a hash function that converts data into a fixed, secure hash value, and a ledger that stores data in immutable blockchain blocks. As a result, the data becomes secure, traceable, and resistant to tampering within a decentralized environment. The artificial intelligence processing layer consists of two artificial intelligence models, namely, Long Short-Term Memory (LSTM), which acts as an auto-encoder and learns normal patterns to detect anomalies, and Support Vector Machine (SVM), which classifies data as normal or malicious. Furthermore, LSTM is capable of capturing time-based patterns, which is very important for IoT-generated

healthcare data. Overall, the artificial intelligence layer identifies abnormal patterns in IoT-generated healthcare observations, while the network security layer evaluates network-level threats through simulated attack scenarios and corresponding security metrics. Next is the simulation and output layer that uses key security metrics, such as wormhole attack rate and product drop ratio, to generate authentication results, security reports, and alerts as outputs.

The key strengths of the proposed framework are:

- Multi-layer security
- Artificial intelligence-based anomaly detection
- Blockchain immutability
- Real-time monitoring
- Attack detection capability

The stakeholders and data communication among them have been presented in Figure 4. The figure shows that different participants, such as hospitals, doctors, and patients, act as blockchain nodes that enable secure and immutable storage of records via the SHA-256 algorithm. The figure highlights how patient data flows between doctors, pharmacies, insurance, and devices. Here, patients are given full access and control over their own data. Blockchain ensures immutability, while SHA-256 facilitates data integrity.

As shown in Figure 4, the healthcare process starts with patient X visiting doctor Y. Doctor send the prescription transaction to the pharmacy and billing details to the insurance company. These are recorded immutably and securely as blockchain transactions (Tx) with proper time stamping. On the other side, smart connected IoT devices generate patient data. The data received from these devices is also stored using SHA-256 hashing on the blockchain ledger. SHA-256 hashing ensures data integrity and tamper detection. Furthermore, patient data is saved from free accessibility, and ownership is controlled through blockchain, where only authorized entities can access data. The pharmacy receives the prescription from the doctor and possible data from smart devices via blockchain. An insurance company also receives billing information via blockchain to verify claims.

3.1 Dataset and Data Preparation

The framework uses an artificially generated dataset that mimics the real healthcare monitoring environment to conduct experimentation. This dataset contains 1200 simulated patient records that have been generated using realistic medical studies and are not the actual patient data. Each dataset entry consists of health-related attributes typically captured through IoT-based sensing devices. These parameters have been discussed as follows:

- **Heart rate values:** They are generated using a Gaussian distribution and are centered on typical resting heart rates. Heart rate is measured as beats/minute.
- **Blood pressure values:** They are also generated using a Gaussian distribution and highlight typical systolic ranges. Blood pressure is measured in mmHg units.
- **Body temperature values:** They are created close to normal human temperature with slight variations. Temperature is measured in °C.
- **Oxygen level values:** They are generated to represent typical pulse oximeter readings and are measured in percentage.

Each record in the dataset is labelled as 'Normal' or 'Abnormal'. The dataset contains 85% normal records and 15% abnormal records to realistically simulate anomalies in the proposed healthcare monitoring framework. Additionally, a fixed random seed has been utilized so that every time the dataset can be generated in the same way. Moreover, since the records are artificial, there is no need to remove any sort of personal information.

It should be noted that the present dataset is synthetic and relatively small, and the four physiological attributes represent a simplified representation of healthcare monitoring data. Furthermore, the original implementation does not provide sufficient documentation to establish a specific temporal sequence length or windowing configuration for the LSTM model. Therefore, the present results are considered a controlled proof-of-concept evaluation rather than a comprehensive validation of temporal physiological anomaly detection in real-world healthcare environments.

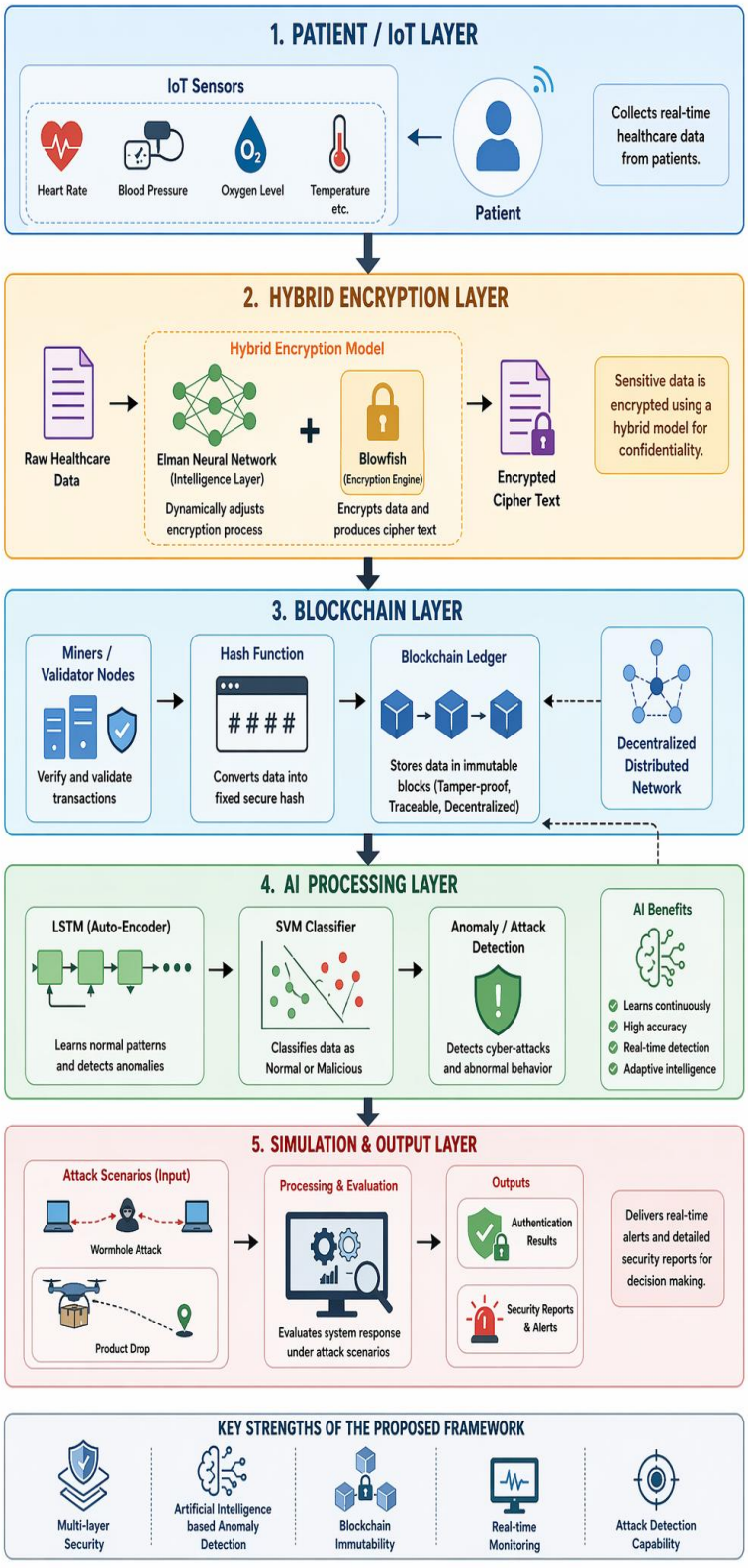

Fig. 3. Architecture of the Proposed Framework

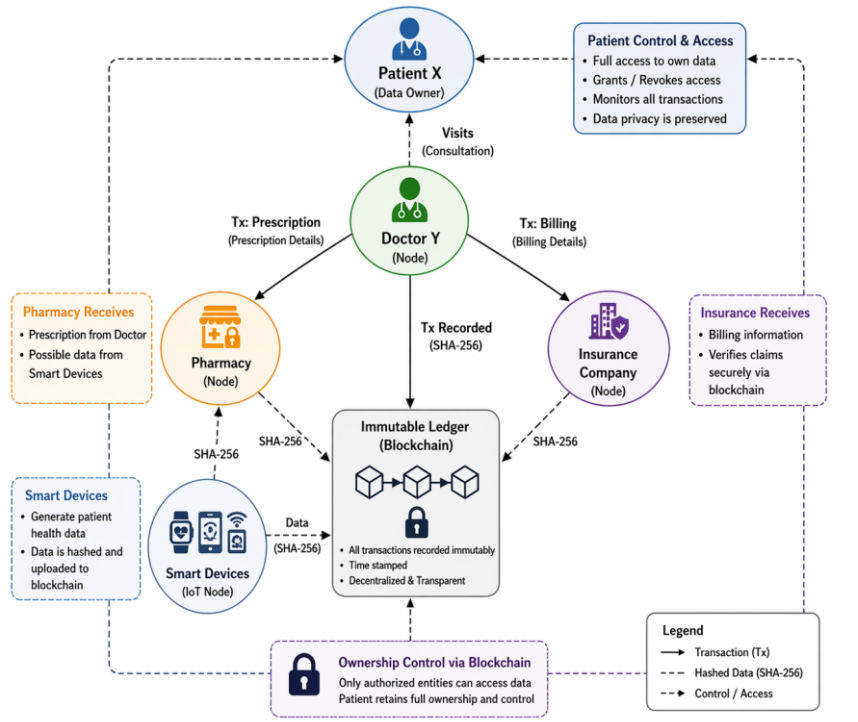

Fig. 4. Blockchain-IoT Integrated Healthcare Data Flow

3.1.1 distinction between physiological and network anomalies

The anomalies represented in the synthetic healthcare dataset correspond to physiological or patient-health anomalies rather than network-level cyber-attacks. Specifically, abnormal records are generated by introducing deviations in the physiological parameters, including heart rate, blood pressure, body temperature, and oxygen saturation, from their normal ranges. These records are used to evaluate the LSTM-SVM anomaly detection module for identifying abnormal healthcare observations. In contrast, network-level security events, such as wormhole attacks and packet loss, are generated separately within the simulated IoT network environment described in Section 4 and evaluated using network-level security metrics. Therefore, the physiological anomaly detection task and the network cyber-attack evaluation represent two complementary but distinct security functions of the proposed framework.

3.1.2 dataset characteristics and experimental partitioning

The dataset used in this study is a controlled synthetic healthcare IoT dataset consisting of 1,200 records and four physiological attributes: heart rate, systolic blood pressure, body temperature, and oxygen saturation. The dataset was generated programmatically using Gaussian-based distributions around clinically plausible normal ranges. Approximately 85% of the records represent normal physiological observations, while 15% represent abnormal observations generated by controlled deviations from the corresponding normal ranges. A fixed random seed was used to ensure reproducibility of dataset generation.

The dataset was designed specifically to evaluate physiological anomaly detection while avoiding the use of identifiable patient information. The abnormal class represents physiological deviations rather than network cyber-attacks. Network-level attacks, including wormhole behavior, were generated separately within the simulated IoT network and were not included as labels in the physiological dataset.

Before model training, the four physiological attributes were normalized using Min–Max scaling to the range [0,1]. The available implementation uses the labelled records for the subsequent SVM classification stage, while the LSTM autoencoder learns reconstruction patterns without using the Normal/Abnormal labels during its reconstruction-learning stage. The dataset was divided into training and testing subsets before model evaluation, with the training portion used for model learning and the unseen testing portion used for performance evaluation.

Because the dataset is synthetic, relatively small, and contains only four physiological variables, it is intended as a controlled proof-of-concept dataset rather than a substitute for large clinical or benchmark healthcare datasets. Furthermore, the current implementation does not document a dedicated temporal

window length for the LSTM input. Therefore, the reported results should be interpreted as an initial evaluation of the proposed integrated framework rather than evidence of generalization to all real-world healthcare IoT environments. Table 2 explains the characteristics possessed by the dataset.

Table 2
Dataset Characteristics

Parameter	Description
Dataset type	Synthetic healthcare IoT dataset
Number of records	1,200
Physiological attributes	Heart rate, blood pressure, body temperature, SpO_2
Normal records	85%
Abnormal records	15%
Labels	Normal / Abnormal
Abnormality generation	Controlled deviations from normal physiological ranges
Cyberattack labels	Not included
Network attacks	Simulated separately
Scaling	Min–Max normalization [0,1]
Randomization	Fixed random seed
Purpose	Proof-of-concept physiological anomaly detection

3.2 Mathematical Symbols and Cryptographic Methods

This section explains the encryption technique, hashing process, and consensus mechanisms used in the proposed framework. Table 3 highlights mathematical symbols used further in this section.

Table 3
Mathematical Notations Used

Notation	Description
d	Input data d, either a transaction or a message
SHA-256(d)	Hash function
H(d)	Hash address of input data d
k	Random nonce
n	Small positive integer
G	Fixed predefined base public point on the elliptic curve
$\mathbf{x_1}$	x-axis of the elliptic curve point
$\mathbf{y_1}$	y-axis of the elliptic curve point
r	First half component of the digital signature
s	Second half component of the digital signature
$\mathbf{K_P}$	Private key of the sender
$\boldsymbol{\omega}$	Modular inverse of s
$\boldsymbol{\alpha}$	Message-dependent scalar
$\boldsymbol{\beta}$	Signature-dependent scalar
C	Reconstructed elliptic curve point
$\mathbf{K_u}$	Public key of the sender

The SHA-256 hashing technique has been utilized to ensure that blockchain data remains immutable and secure. This has been shown mathematically in Equation 1. The hash generated is always a 256-bit value, regardless of the size of the input data.

$$H(d) = SHA\text{-}256(d) \quad (1)$$

The framework uses Elliptic Curve Digital Signature Algorithm (ECDSA) to generate, verify, and validate the accuracy and truthfulness of a transaction's digital signature. ECDSA is a widely used digital signature generation algorithm in blockchain systems, especially Bitcoin and Ethereum. Following steps and equations mathematically highlight the process of transaction digital signature generation using ECDSA.

Step 1: A random nonce k is selected between 1 and n-1, as shown in equation 2. Here n is a selected such that n.G reaches the point of infinity O. The value of k must be unique and secret for every signature. Reusing k can expose the sender's private key, which is a critical risk to system security.

$k \in [1, n-1]$ (2)

Step 2: Elliptic curve point (x1, y1) is calculated as shown mathematically in equation 3.

$(x1, y1) = k.G$ (3)

Step 3: The first half component of the final digital signature is computed as shown in equation 4. If r becomes zero, a new k is generated using step 1, and the process is repeated.

$r = x1 \bmod n$ (4)

Step 4: The second half component of the final digital signature is computed as shown in equation 5. Here, k-1 is the modular inverse of k modulus n, such that $k.k1 \equiv 1 \pmod n$.

$s = k\text{-}1\ (H(d) + KP.\ r\ ) \bmod n$ (5)

Step 5: The final digital signature (r, s) is obtained from equations 4 and 5.

The following steps and equations mathematically highlight the process of transaction digital signature verification using ECDSA.

Step 6: The modular inverse of the transaction digital signature second component is calculated as shown in equation 6.

$\omega = s\text{-}1 \bmod n$ (6)

Step 7: Using the value obtained from step 1, two intermediate parameters are obtained as shown in equation 7.

$\alpha = H(d)\ .\ \omega \bmod n$ (7)

$\beta = r.\ \omega \bmod n$

Step 8: The reconstructed elliptic curve point $C = (x_C, y_C)$is calculated using Equation 8.

$$C = (x_C, y_C) = G\alpha + K_u\beta \quad (8)$$

Step 9: The transaction digital signature is valid if the x-coordinate of the reconstructed elliptic curve point satisfies the verification condition.

$xc\ n = r$ (9)

Since $C = (x_C, y_C)$ is an elliptic-curve point whereas r is a scalar signature component, the verification compares the x-coordinate of C, reduced modulo n, with r. If $x_C\ n = r$, the ECDSA signature is considered valid; otherwise, it is rejected.

Figure 5 presents the flowchart of the transaction digital signature generation and verification process.

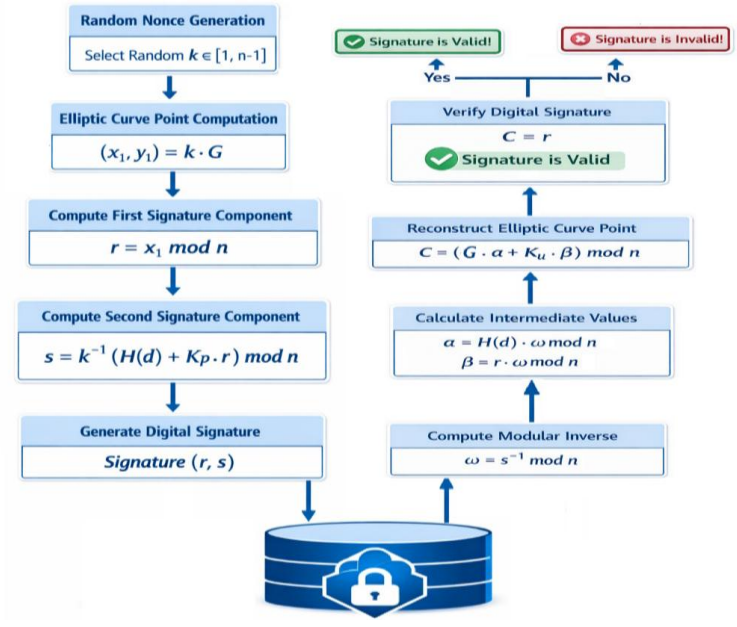

Fig. 5. Digital Signature Generation and Verification Process Flowchart

3.2.1 neural-enhanced blowfish encryption

The proposed framework enhances the conventional Blowfish encryption process by integrating an Elman Neural Network (ENN) as a dynamic key-generation layer. The purpose of the ENN is to generate a transaction-dependent neural representation from the healthcare data, which is subsequently used to derive the encryption key for Blowfish. Thus, the neural network is mathematically coupled with the symmetric encryption process rather than being used as an independent processing component.

For each healthcare transaction at time t, the normalized healthcare parameters are represented as:

$$X_t = [H, R_t, B, P_t Temp_t SpO_{2,t}] \quad (10)$$

where HR_t, BP_t, $Temp_t$, and $SpO_{2,t}$represent heart rate, blood pressure, body temperature, and oxygen saturation, respectively.

The Elman Neural Network processes the input vector using its recurrent hidden state. The hidden state is calculated as:

$$h_t = f(W_x X_t + W_h h_{t-1} + W_c c_{t-1} + b_h) \quad (11)$$

where $h_t$is the current hidden state, $h_{t-1}$is the previous hidden state, $c_{t-1}$is the context state, W_x, W_h, and $W_c$are the corresponding weight matrices, $b_h$is the bias vector, and $f(\cdot)$represents the activation function. The neural output is then calculated as:

$$z_t = W_o h_t + b_o \quad (12)$$

where $W_o$and $b_o$represent the output weight matrix and output bias, respectively.

The neural output $z_t$is transformed into a fixed-length key-derivation value using a deterministic function $G(\cdot)$. The transaction-dependent encryption key is then generated as:

$$K_t^* = K_p \oplus G(z_t) \quad (13)$$

where $K_p$is the authorized base secret key, $G(z_t)$represents the key-derivation value obtained from the neural output, and $K_p \oplus G(z_t)$ represents the bitwise exclusive-OR operation. Therefore, the encryption key is dynamically associated with the current neural state rather than relying only on a fixed encryption parameter.

The resulting dynamic key $K_t^*$is supplied to the Blowfish encryption algorithm:

$$C_t = Blowfish(P_t, K_t^*) \quad (14)$$

where P_t represents the plaintext healthcare data and $C_t$represents the resulting ciphertext. This establishes the mathematical coupling between the Elman Neural Network and Blowfish encryption. The coupling occurs at the Blowfish key-input layer: the ENN output z_t determines the derived component $G(z_t)$, which is combined with the authorized base key K_p to produce the transaction-dependent Blowfish key K_t^*. The internal Blowfish round function and S-box structure remain unchanged. The complete encryption process can therefore be represented as:

$$X_t \rightarrow h_t \rightarrow z_t \rightarrow K_t^* \rightarrow C_t$$

For authorized decryption, the corresponding neural representation and dynamic key are reconstructed, after which the ciphertext is decrypted using:

$$P_t = Blowfish^{-1}(C_t, K_t^*) \quad (15)$$

The encrypted transaction is subsequently processed using SHA-256 hashing to generate an integrity value before blockchain validation and storage. The complete workflow of this mechanism is illustrated in Figure 6.

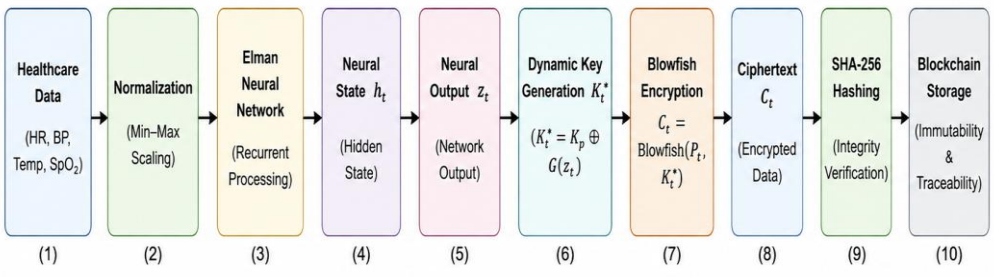

Fig. 6. Neural-enhanced Blowfish encryption and blockchain integration process

As shown in Figure 6, the process begins with the acquisition of healthcare parameters from IoT devices, which are normalized to eliminate scale variations (Stages 1–2). The normalized data are then fed into the Elman

Neural Network, which maintains contextual information through its recurrent structure (Stage 3). The resulting hidden state h_t(Stage 4) and the network output z_t(Stage 5) capture the temporal dependencies of the input data. These outputs are transformed into a dynamic encryption key K_t^*using the key-derivation function $G(\cdot)$and combined with the authorized base key K_p(Stage 6). The dynamic key is then supplied to Blowfish encryption to generate the ciphertext C_t(Stages 7–8). Subsequently, the ciphertext is hashed using SHA-256 to produce an integrity value (Stage 9), and finally, the encrypted data and its corresponding hash are validated through the PoA mechanism and stored on the blockchain (Stage 10).

3.3 Consensus Mechanism

The framework uses a customized Proof-of-Authority (PoA) consensus mechanism to validate and verify transactions before storing them on the blockchain. PoA is highly suitable for this framework because here only authorized and authenticated participants are allowed to validate the transactions. Additionally, PoA is a faster and cost-efficient consensus mechanism as compared to other methods, such as Proof of Work and Practical Byzantine Fault Tolerance. Thus, PoA could allow fast healthcare-related operations while observing rules and maintaining scalability.

Unlike in standard PoA, where only authorized validators can validate blocks, the proposed customized PoA consensus mechanism allows domain-specific validator selection. Here, validators are not random nodes, but are pre-approved regulated entities such as hospitals, pharmacies, labs, and insurance systems. Furthermore, this customized PoA is tightly coupled with Blowfish encryption, Elman Neural Network, SHA-256 hashing, and anomaly detection models, including LSTM and SVM.

Total time taken by PoA to validate a block is the sum of signature generation time for each transaction Ti(tx) and block processing time T(blk), as shown in equation 16.

$$T_{val} = \sum_{i=1}^{n} T_i \text{ (tx)} + \text{T(blk)} \quad (16)$$

With n as the total number of validating nodes in the network and m as the total number of malicious nodes, the probability that a randomly selected node is malicious is:

$$P_{mal} = \frac{m}{n} \quad (17)$$

To protect patient data stored off-chain, the proposed framework uses the neural-enhanced Blowfish encryption mechanism described in Section 3.2.1. In this process, the healthcare data is first processed by the Elman Neural Network to generate a transaction-dependent neural representation. The neural output is then transformed into a dynamic encryption key K_t^*, which is supplied to the Blowfish encryption algorithm. Therefore, the encryption process is expressed as:

$$C_t = Blowfish(P_t, K_t^*) \quad (18)$$

where $P_t$represents the plaintext healthcare data and $C_t$represents the resulting ciphertext. The SHA-256 hash of the encrypted transaction is subsequently generated to support data integrity verification and tamper detection within the blockchain. This process allows the neural component to directly influence the encryption stage while retaining Blowfish as the underlying symmetric encryption algorithm.

3.4 Integration of Blockchain

The framework has two main components: first, the user interface designed for interaction among stakeholders, and second, the blockchain backend for secure data storage and processing. Different stakeholders of the framework, administrators, doctors, and patients, are provided with login IDs to use the framework securely. This multilevel authentication and encryption enhances confidentiality among patients as well as provides the integrity of data. There are two types of nodes in the blockchain network: the miner nodes and the executor nodes. Miner nodes conduct verification and validation of healthcare-generated transactions, such as prescriptions, medical test reports, and medicine bills. The executor nodes execute smart contracts and add records onto the blockchain after they are validated and verified.

The framework has been simulated using two virtual machines. The Virtual_Machine#1 acts as an executor blockchain node that manages patient-related smart contracts. Virtual_Machine#2 acts as a hybrid node that performs both mining tasks and execution tasks. These virtual machines simulate the real-world healthcare network, which involves components such as hospitals, pharmaceuticals, and insurance companies. The data communication between these components is done through a secure blockchain channel. Furthermore, the framework also includes real-time detection of anomalies and delays to ensure a secure, transparent, and traceable process. The blockchain integration within the proposed framework has been presented in Figure 7.

Every healthcare transaction is encrypted before being stored on the blockchain. The framework uses Blowfish encryption, which is a lightweight and efficient technique and is very well-suited for IoT-based frameworks. Furthermore, the Elman neural network is used as a dynamic control layer that improves robustness and can handle diverse healthcare data. The SHA-256 hashing technique has been utilized to generate the hash address of encrypted transactions. Every healthcare entity, such as a doctor, patient, hospital, pharmacy, and laboratory, acts as a blockchain node. Each block of the chain contains encrypted transactions, the hash address of the block, and the previous block's hash address. Any alteration in the stored data generates a different block hash, which invalidates the further blocks, making tampering easily detectable. This ensures immutability and security of the framework. Each patient's data is recorded step-by-step on the blockchain, including registration, doctor visits, prescriptions, lab testing, pharmacy bills, and insurance bills. It allows easy auditing of any medical case. Furthermore, smart contracts and consensus mechanisms ensure that all the transactions are valid and trusted. The framework gives selective access permissions to patients that increase their confidence and control over their data to a great extent.

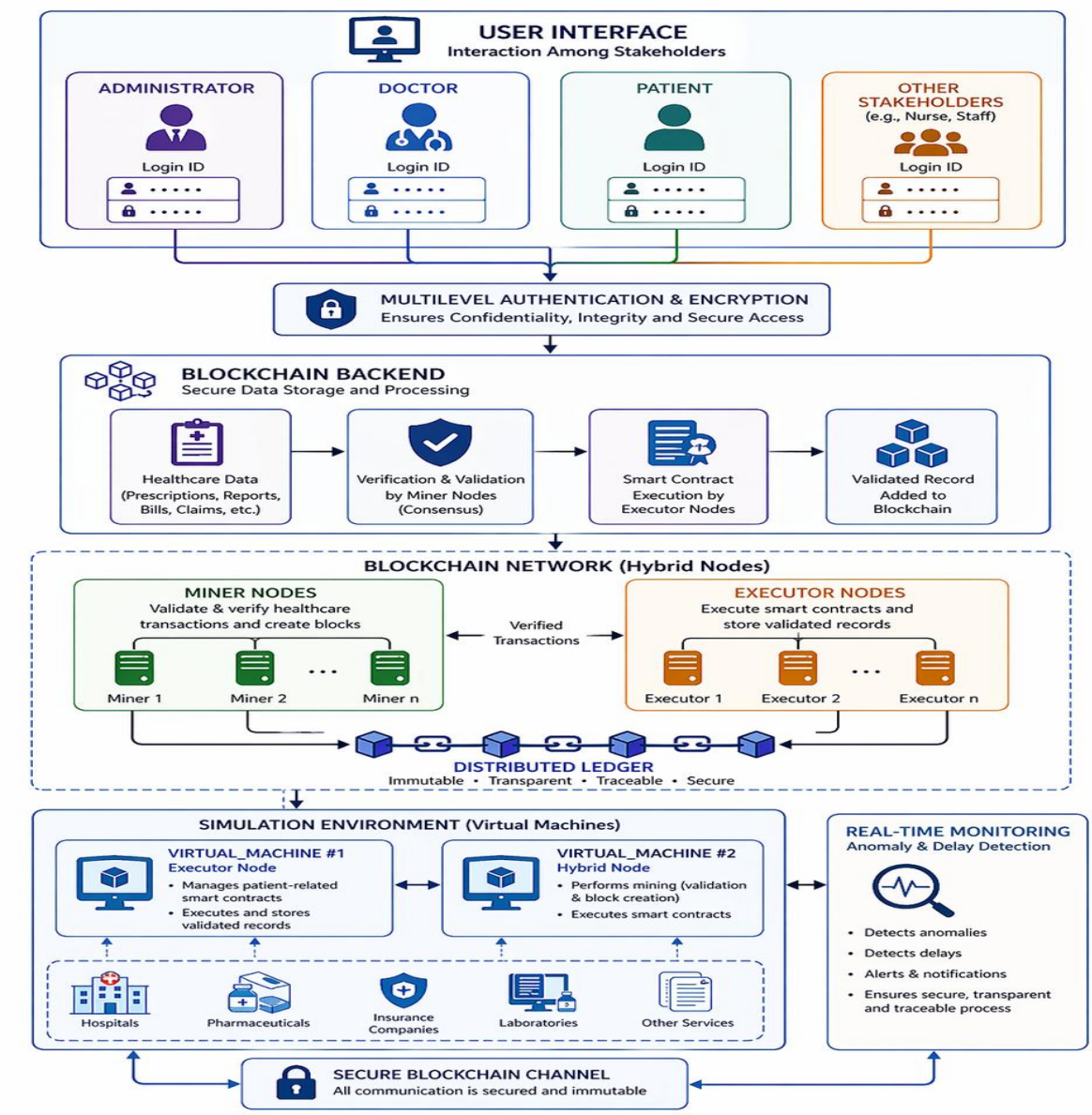

Fig. 7. Blockchain Integration within the Proposed Framework

4. Implementation

The framework has been implemented using the Python programming language on Google Colaboratory. A synthetic IoT-based healthcare dataset with 1200 records has been created with realistic attributes to mimic healthcare monitoring. The framework has been coded and tested in a simulated setup. Instead of using complex external software, various Python libraries, such as Keras for the Elman neural network, Scikit-learn for machine learning-based data processing, and PyCryptodome for Blowfish encryption, have been used.

Three simulated IoT healthcare networks with different node sizes (number of IoT devices), Network#1 with 150 nodes, Network#2 with 600 nodes, and Network#3 with 1200 nodes, were created to test the scalability of the framework. Each simulated network was placed inside a square area of 550 meters by 550 meters to mimic a virtual hospital campus where each node could only communicate wirelessly within 100 meters. Every encrypted patient data has been taken as 128 bytes long. This size of packet helps maintain load on the network, transmission delays, and storage requirements. The detailed experimentation settings have been given in Table 4.

Table 4

	Experimentation Setup Network Configuration
Types of Networks	Network#1 (150 nodes), Network#2 (600 nodes), Network#3 (1200 nodes)
Area of Network	550 meters by 550 meters
Communication Range	100 meters
	Data Characteristics
Packet Size	128 bytes
Dataset Source	Synthetic healthcare IoT dataset with 1,200 simulated records
	Simulation Settings
Duration of each test	60 seconds
	Security and Intelligence
Encryption Techniques	Blowfish and Elman Neural Network
Anomaly Detection Techniques	LSTM and SVM
	Implementation Platform
Programming Setup	Python on Google Colaboratory

The framework has been evaluated using three security metrics, namely, attack rate, data loss, and validation delay. To simulate malicious activities in the network, a few nodes were intentionally made malicious, and others were made validators or miners, as shown in Figure 8.

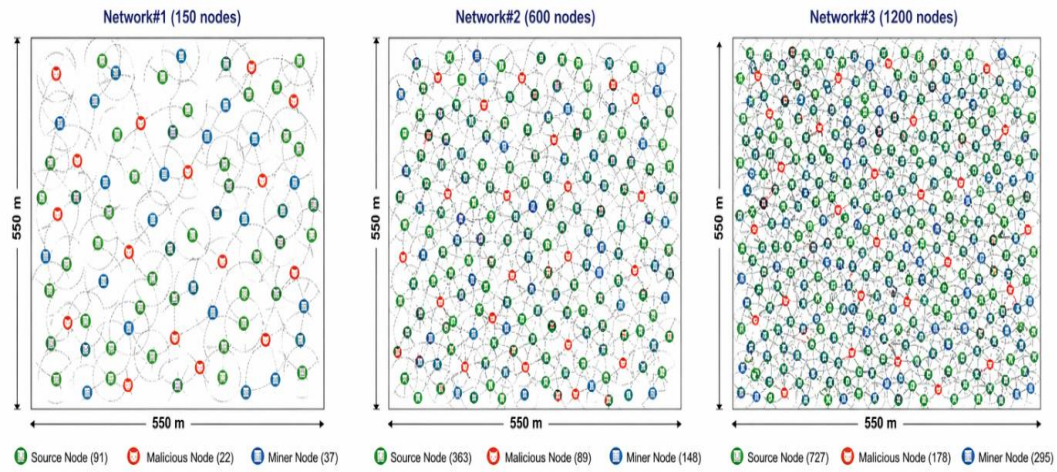

Fig. 8. The Simulated Environment

Table 5 presents different roles assigned to different nodes in different network setups. Furthermore, different cyber-attacks were simulated to test the security of the framework at multiple levels.

Table 5
Network Setups

Network Name	Network Type	Source Nodes	Malicious Nodes	Miner Nodes	Total Nodes
Network#1	Small-scale	91	22	37	150 nodes
Network#2	Medium-scale	363	89	148	600 nodes
Network#3	Large-scale	727	178	295	1200 nodes

4.1 Implementation Challenges and Proposed Solutions

Even though the blockchain enhances security, it introduces various implementation challenges, such as delays, storage requirements, computational cost, and scalability. These challenges must be addressed while implementing the framework in a real environment with limited resources. Table 6 highlights these challenges and solutions implemented to alleviate them.

Table 6
Framework Challenges and Proposed Solutions

Parameter	Challenge	Solution	Advantage
Delay	Blockchain security checks slow down transaction processing.	The framework uses a customized Proof-of-Authority consensus mechanism in place of traditional Proof-of-Work.	Delay is reduced to 85 ms from 110-120 ms.
Storage Requirements	Healthcare data includes high-resolution images and videos that require significant storage.	The framework stores only a small hash address on the blockchain and actual data on IPFS.	Reduces storage load while maintaining security and traceability.
Computational Cost	Blockchain processes are very heavy for IoT devices with limited power.	The framework uses a hybrid technology of Blowfish encryption with Elman Neural Network, which reduces computational cost.	Computational cost is reduced to approximately 30 times compared to traditional encryption.
Scalability	With the increase in the number of nodes, network congestion increases.	The framework is tested against different-sized networks to evaluate scalability.	Consistent performance is maintained irrespective of network size.

5. Evaluation Results

The framework has been tested on three different network sizes to evaluate its performance and security capabilities. These networks simulate small, medium, and large-sized healthcare systems.

5.1 Security Evaluation

To evaluate the strength and robustness of the proposed framework, three metrics have been used. These metrics test the security, reliability, and practicability of the framework under attack conditions. The security evaluation in this section focuses specifically on network-level security behavior. The wormhole attacks are introduced within the simulated network environment and are evaluated using network-oriented metrics, namely wormhole attack probability, product drop ratio, and verification latency. These network-level attack measurements are independent of the physiological anomaly classification performed by the LSTM-SVM model in Section 5.2.

- **Wormhole Attack Probability**: It measures the rate at which attackers manipulate the network traffic by creating tunnels. This is a serious attack in the case of healthcare systems, as it can compromise sensitive healthcare data. The lower the attack rate, the better the framework security. It is expressed in percentage.
- **Product Drop Ratio**: It measures the data loss rate due to attacks and failures. The higher the drop ratio, the more the quality of the healthcare framework is compromised. It is expressed in percentage.
- **Verification Latency**: It measures the latency caused while verifying and validating users and transactions within the framework. Latency can cause issues in emergency healthcare situations. The lesser the latency, more improved will be the quality of real-time data transfer and healthcare operations. It also impacts the integration of IoT devices with blockchain facilities. It is measured in milliseconds.

It has been noticed from Table 7 that increasing the density of nodes and involvement of miners has led to a decrease in wormhole attack and product drop ratio, improving the performance of the framework. These improvements have been observed especially in Network#2, where the attack rate of 1.2% and product drop ratio of 1.3% are minimum. This network setup could be considered as having an optimal balance of node density and miners' distribution that are involved in the validation and verification of transactions. Furthermore, in large-scale Network#3, both metrics have been noticed to increase, which indicates that this network may be affected by congestion and coordination overhead. Verification latency increases slightly with an increase in the size of the network, although this increase is very small and acceptable. These results have been presented graphically in Figure 9.

Table 7
Security Evaluation Results

Network Name	Wormhole Attack Probability	Product Drop Ratio	Verification Latency	Result
Network#1	2.3%	2.8%	110.12 ms	Lower security and reliability
Network#2	1.2%	1.3%	111.11 ms	Optimal and most efficient performance
Network#3	1.8%	1.5%	111.19 ms	Scalable but with performance tradeoffs

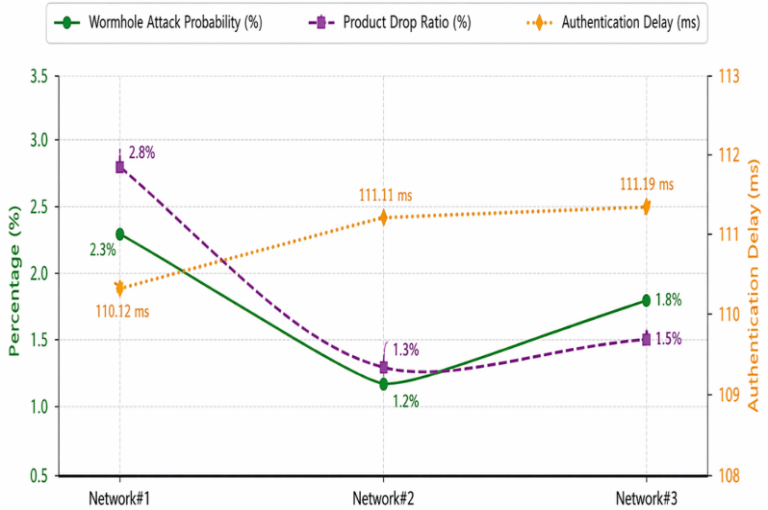

Fig. 9. Comparative Security Performance across Different-Sized Networks

5.2 Physiological Anomaly Detection Evaluation

To evaluate the ability of the proposed artificial intelligence module to identify abnormal healthcare observations, an LSTM autoencoder and an SVM classifier are applied to the synthetic physiological dataset

described in Section 3.1. The input data consist of four IoT-derived physiological parameters: heart rate, blood pressure, body temperature, and oxygen saturation. The anomalies represented in this dataset correspond to deviations in patient-health parameters from their normal patterns and therefore represent physiological anomalies, rather than network-level cyber-attacks.

During the LSTM training stage, the Normal/Abnormal labels are not provided to the autoencoder, allowing the model to learn the reconstruction pattern of the physiological observations. Abnormal observations are subsequently identified using their reconstruction error. The SVM classifier then uses the labelled anomaly-detection data to perform supervised classification. Accordingly, the accuracy, precision, recall, and F1-score reported in this section quantify the performance of the framework in detecting physiological anomalies in IoT-generated healthcare data.

Network-level cyber-attacks are evaluated separately in Section 5.1. In that evaluation, wormhole attack probability, product drop ratio, and verification latency are obtained from the simulated IoT-blockchain network under different network configurations. These metrics characterize network-level security and resilience and are not treated as outputs of the physiological LSTM-SVM classifier.

To detect suspicious and malicious activities with the framework, artificial intelligence models, namely, LSTM and SVM, have been used. These models learn normal behaviour within the proposed IoT Blockchain integrated healthcare framework and then detect the abnormal behaviours. As already discussed in Section 3.1, the framework uses an artificially generated dataset containing 1200 simulated patient records where each record includes health parameters that could be measured by IoT sensors, including heart rate values, blood pressure values, body temperature values, and oxygen level values. Furthermore, each record in the dataset is labelled as 'Normal' or 'Abnormal'. The dataset contains 85% normal records and 15% abnormal records to detect any sort of anomaly or attacks.

During the training phase of LSTM, the 'Normal' or 'Abnormal' labels are made hidden, allowing unsupervised learning. Furthermore, the data has been scaled between 0 and 1 using MinMax scaling to prevent the neural network from being dominated by large values, allowing fast and smooth coverage. The model was trained for 60 epochs using a batch size of 30 samples. The available implementation description does not specify a separate temporal sequence length for the LSTM input; therefore, the batch size should not be interpreted as the temporal sequence length (T). This helps balance speed, memory usage, and learning stability of the model. Mean Absolute Error (MAE) has been utilized to calculate the reconstruction loss as:

$$\text{MAE} = | \text{ Original} - \text{Reconstructed } | \tag{19}$$

The lower the MAE value obtained, the better the reconstruction and the fewer anomalies.

5.3 LSTM–SVM Interface

The interface between the LSTM autoencoder and the SVM classifier is based on the reconstruction-error representation generated by the autoencoder. For an input vector x_t and its reconstructed output $\hat{x}_t$, the feature-wise reconstruction error is calculated as:

$$e_t = | \, x_t - \hat{x}_t \, |. \tag{20}$$

The reconstruction-error vector e_t is then supplied to the SVM classifier as its input feature representation. The SVM uses the corresponding Normal/Abnormal labels during supervised training to classify the observations. Thus, the LSTM autoencoder performs representation learning and reconstruction-based anomaly scoring, while the SVM performs the final supervised classification. The SVM is therefore not trained directly on the raw physiological measurements or on the LSTM training loss; it receives the reconstruction-error representation produced by the LSTM stage.

The overall two-stage process can be expressed as:

$$x_t \rightarrow LSTM\ Autoencoder \rightarrow \hat{x}_t \rightarrow e_t \rightarrow SVM \rightarrow \hat{y}_t. \tag{21}$$

This explicit interface clarifies the role of each component and makes the hybrid anomaly-detection pipeline reproducible.

Figure 10 represents the training behaviour of LSTM by presenting the training loss and validation loss for 60 epochs. The figure highlights that during the initial phase of 0 – 3 epochs, both training and validation losses are very high, but then it drops sharply. This is because the model starts with no prior knowledge and then quickly learns basic patterns from the dataset. During the early learning phase of 4 – 15 epochs, loss decreases gradually, and train and validation curves closely follow each other. This highlights that the model is still

learning general patterns and no overfitting is present yet, showing good generalization capability of the model. Furthermore, during the mid-training phase of 16 – 25 epochs, more reduction in loss has been observed. This indicates that the LSTM autoencoder progressively improves its reconstruction of the input physiological patterns during training. Because the present dataset is synthetic and the original implementation does not document a specific temporal-window configuration, the results are interpreted primarily as evidence of reconstruction-based anomaly-detection capability rather than as a comprehensive assessment of long-term temporal dependencies in real-world physiological signals.

This phase significantly highlights the improved reconstruction quality. The late training phase of 41 – 60 epochs, both training and validation loss reach near constant values, which indicates that the model has fully converged. The consistent decrease in loss and close alignment of both curves indicate that LSTM is highly suitable for reliable anomaly detection within an IoT Blockchain-integrated healthcare framework.

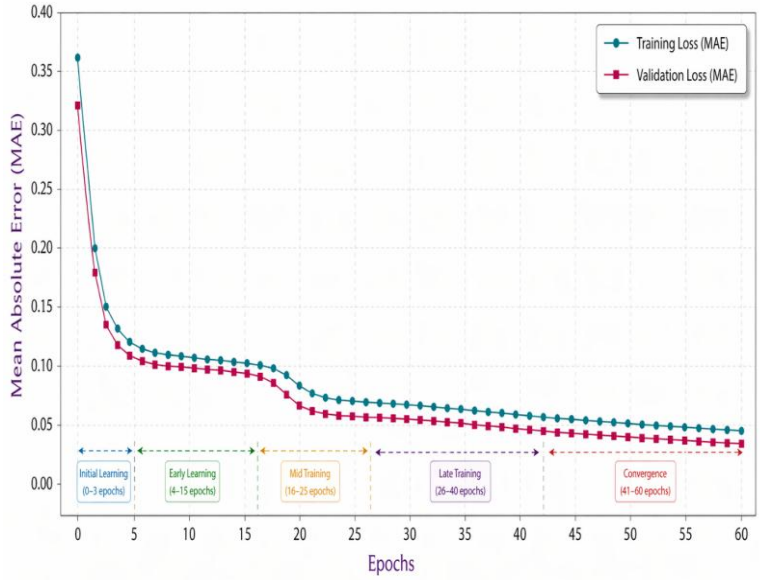

Fig. 10. Training pattern of LSTM

After the training phase, reconstruction error at each point has been calculated to generate the anomaly score. A reconstruction loss threshold value has been selected to identify abnormal data using the following rule:

if error > Threshold
    Abnormal Data Identified
else
    Normal

The classification accuracy has been further improved using SVM. Unlike LSTM, where the 'Normal' or 'Abnormal' labels are made hidden during the training phase, SVM is trained using labelled data, allowing supervised learning. The performance has been evaluated using confusion matrix metrics. The results in Table 8 demonstrate the performance of the LSTM-SVM model in identifying physiological anomalies within the IoT-generated healthcare observations. The recall of 0.93 indicates that the model identifies a high proportion of abnormal healthcare observations, while the precision of 0.89 indicates that some normal observations may be incorrectly classified as abnormal. The F1-score of 0.91 reflects a balanced classification performance. These results should be interpreted specifically as physiological anomaly-detection performance and should not be considered a direct measurement of network-level cyber-attack detection.

Table 8
Physiological Anomaly Detection Evaluation Results

Parameter	Value
Threshold	0.17867
Accuracy	98.99%
Precision	0.89

Recall	0.93
F1-Score	0.91

6. Discussion

This section presents a comprehensive analysis of the proposed IoT-blockchain integrated healthcare framework for anomaly detection by interpreting the experimental results and evaluating overall performance. The discussion highlights how the integration of IoT, blockchain, and artificial intelligence contributes to improved healthcare data management. Furthermore, the section also compares the proposed framework with existing approaches to demonstrate its effectiveness in addressing challenges related to data security, real-time monitoring, and reliable decision-making in smart healthcare environments.

6.1 Benefit of Blockchain Integration

Traditional approaches for healthcare management are based on centralized technology and suffer from a lot of limitations. In these systems, the data is managed by third parties, which may lead to the issue of data vulnerability and unauthorized alterations to it. Additionally, such approaches do not provide transparency of associated processes for the stakeholders, thus making them less confident and trustless on the healthcare system. Another major issue includes the healthcare providers' connectivity gap and a single point of failure.

The proposed blockchain-enabled framework is distributed and decentralized. Blockchain is not stored at a single centralized location, so the single point of failure issue is totally resolved. Blockchain is stored across multiple nodes worldwide in a network where each node has a copy of the blockchain ledger. This enhances fault tolerance and data availability. Furthermore, there is no central authority that controls and manages the database. Rather, decision-making power is shared among participants, such as miners and validators, which prevents control, censorship, or manipulation by any single entity. Additionally, due to anonymity, decentralization, 51% validation rule, immutability, consensus mechanisms, one-way process of hash generation, and cryptographic protections, blockchain is considered the most secure database.

As highlighted in Figure 11, there is a noticeable improvement in verification latency, attack mitigation, anomaly detection rate, specificity, accuracy, and processing overhead efficiency in the proposed framework.

6.2 Benefit of IoT Integration

The integration of Internet of Things technology will allow real-time and continuous monitoring of patient health remotely by capturing important parameters, such as heart beat rate, blood pressure, temperature, and levels of oxygen. This real-time data allows early detection of health issues and timely medical treatment. IoT technology reduces the need for visiting the hospital frequently, especially for elderly and chronically ill patients. This is because healthcare professionals can access patient data remotely, and allow telemedicine and easy accessibility of healthcare services. In the proposed framework, IoT serves as a data generation layer that supplies continuous input to blockchain and artificial intelligence models. This facilitates secure, reliable, and intelligent healthcare decision-making.

6.3 Benefit of Hybrid Anomaly Detection Process

The proposed framework uses a hybrid anomaly detection model that combines an LSTM autoencoder and an SVM classifier for identifying abnormal patterns in IoT-generated healthcare observations. The LSTM autoencoder learns the normal reconstruction pattern of physiological parameters, while the SVM classifier performs supervised classification of normal and abnormal observations. The model achieves an accuracy of 98.99%, with a precision of 0.89, recall of 0.93, and F1-score of 0.91, as presented in Table 8. These results indicate that the hybrid model provides effective detection of physiological anomalies in healthcare data. It is important to distinguish this function from the network-level security evaluation presented in Section 5.1. The LSTM-SVM module is evaluated using physiological healthcare observations, whereas network-level threats such as wormhole attacks are evaluated separately using attack probability, product drop ratio, and verification latency in the simulated IoT-blockchain network. Thus, the framework addresses both healthcare-data anomalies and network-level security threats, but these two detection tasks are evaluated through different mechanisms and metrics.

6.4 Scalability

The proposed framework has been tested on three scaled networks: Network#1 with 150 nodes, Network#2 with 600 nodes, and Network#3 with 1200 nodes. In most of the cases, whenever the network grows, latency and computational overhead also grow. But the presented framework remains efficient even at a large scale,

which is very important for IoT-integrated healthcare environments. The combination of Blowfish encryption and Elman Neural Network improves both security and computational efficiency of the framework. Due to the capability of the proposed framework to handle large networks efficiently while maintaining low delay, it is very well suited for real-time healthcare systems and large-scale deployments.

6.5 Comparative Analysis with Existing Approaches

The proposed framework has been comparatively analysed against existing approaches based on different metrics, as highlighted in Figure 11. The statistical comparative analysis has been presented in Figure 12, and the quantitative analysis has been presented in Table 9.

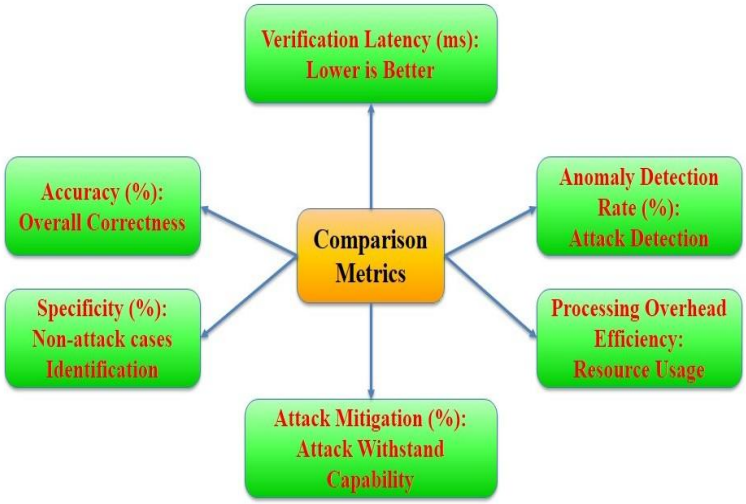

Fig. 11. Metrics used for Comparative Analysis

Table 9

Quantitative Comparative Analysis

Study	Authentication Delay (ms)	Attack Resistance (%)	Sensitivity (%)	Specificity (%)	Accuracy (%)	Computational Efficiency
Azbeg et al., 2022 [14]	120	74	80	91	88	1 (Moderate)
Hossein et al., 2021 [15]	110	76	85	93	90	2 (High)
Teli & Masoodi, 2021 [16]; Quasim et al., 2020 [17]	115	78	83	90	89	1 (Moderate)
Chinaei et al., 2021 [18]	108	79	86	94	91	2 (High)
Mohammed et al., 2021 [19]; Al-Marridi et al., 2024 [20]; Al-Nbhany et al., 2024 [21]	100	80	87	95	92	2 (High)
Proposed Framework	**111**	**95**	**89.7**	**98.7**	**98.98**	**3 (Optimized)**

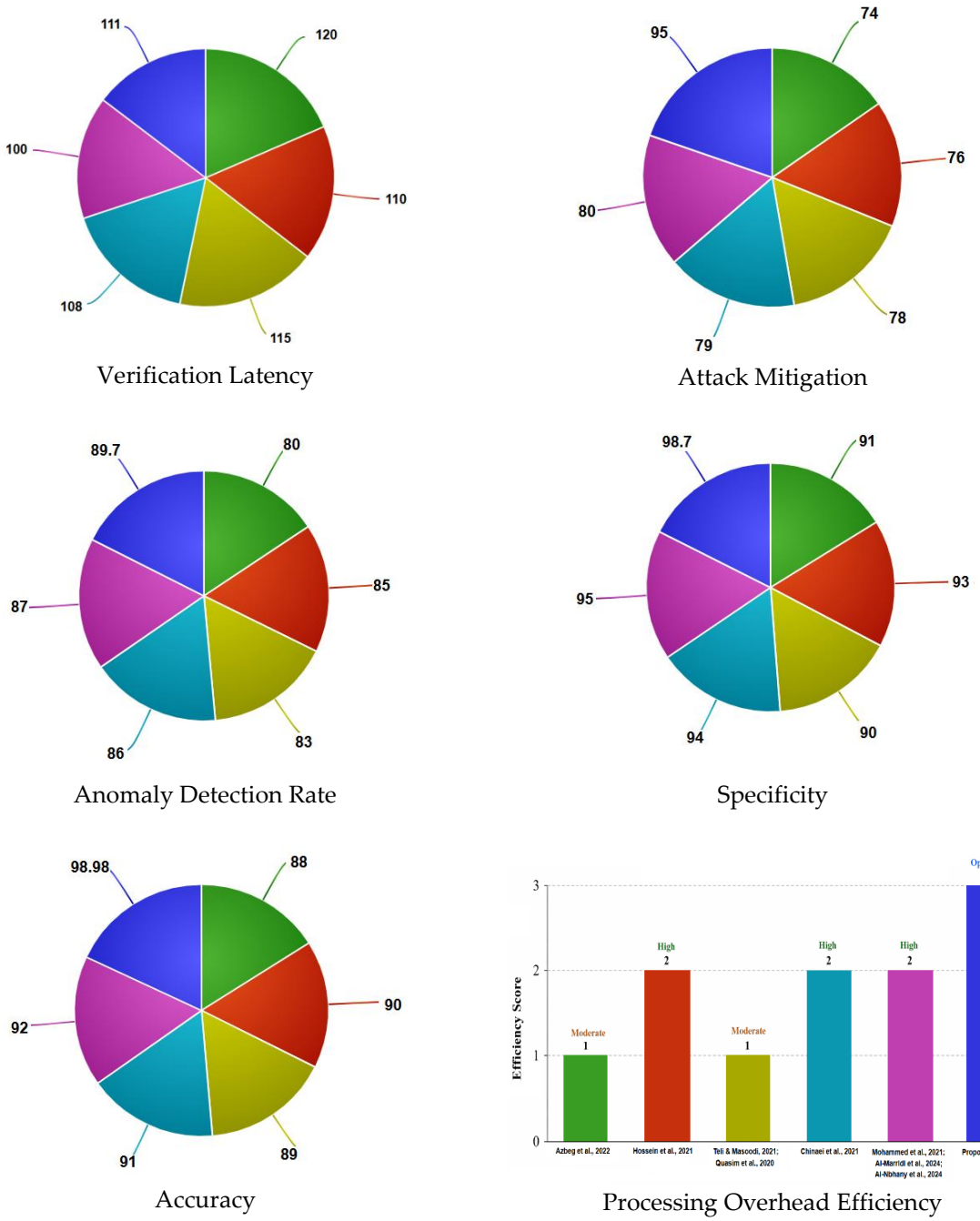

Fig. 12. Statistical Comparative Analysis

7. Limitations

Even though the proposed framework performs very well in terms of security and successfully includes anomaly detection mechanisms, some challenges and constraints remain.

- **Use of Synthetic Data:** Since the framework has been evaluated using synthetic data for preserving healthcare data privacy, it may lack the complexity and unpredictability of real data.
- **Simulation-based Evaluation:** Since the framework has been evaluated using simulated environments, it may not fully capture real-world healthcare processes and the dynamic conditions of hospital networks.
- **Use of Permissioned Blockchain:** The framework uses a permissioned blockchain to store and process the data, due to which, when used under a fully decentralized public blockchain environment, performance and security may vary.
- **Use of only one Consensus Mechanism:** Framework uses a customized Proof-of-Authority consensus mechanism to validate and verify transactions. However, the results may vary with the use of other mechanisms or hybrid ones.
- **Assessment of only Network-Level Security:** The framework lacks evaluation of other types of security, such as device-level, application-level, and user-level.
- **Lack of IoT Resource Constraints Measurements:** Framework lacks measurement of computational load, memory usage, and energy consumption of IoT devices, which is very crucial for real-world deployments.
- **Limited Attacks Detection:** The framework only focuses on wormhole attacks, ignoring other attacks, including replay attacks, insider attacks, and data poisoning attacks.
- **Limited Cross-Dataset Validation:** The present evaluation uses a controlled synthetic healthcare IoT dataset containing four physiological variables. Although this design provides reproducibility and avoids patient privacy concerns, it does not establish generalization across independent benchmark datasets. Cross-dataset validation using publicly available healthcare and IoT security datasets will therefore be considered in future work.

8. Future Scope

- The framework could be deployed in hospitals or healthcare for real-world implementation, pilot testing, and practical validation.
- Edge nodes could be utilized for faster processing and reducing latency in critical healthcare environments.
- Proof-of-Authority could be replaced by other lightweight consensus mechanisms to reduce delays and energy consumption.
- Blockchain sharding could be implemented to improve throughput and handle large-scale networks.
- Experiments could be extended to analyze other types of attacks, including replay attacks, insider threats, data poisoning, DDoS attacks, etc.
- The power consumption and computational efficiency of IoT devices could be analyzed and optimized accordingly.
- The framework could be aligned with healthcare standards for data protection and security regulations.

9. Conclusion

This paper presented a secure, scalable, and intelligent healthcare framework that integrates Internet of Things (IoT), blockchain technology, artificial intelligence, and advanced cryptographic mechanisms to address critical challenges related to healthcare data management. The proposed system ensures secure handling of sensitive medical data through neural-enhanced Blowfish encryption and blockchain-based immutability. This prevents accessing of data in an unauthorized way as well as tampering. The use of a permissioned blockchain with customized Proof-of-Authority consensus further enhances efficiency by reducing authentication delay and computational overhead. A key contribution of this work is the implementation of a hybrid anomaly detection model combining an LSTM autoencoder and SVM for identifying abnormal patterns in IoT-generated healthcare observations. The experimental results demonstrate an accuracy of 98.99% and an F1-score of 0.91 for physiological anomaly classification. In parallel, the simulated network evaluation demonstrates the framework's ability to assess network-level security using wormhole attack probability, product drop ratio, and verification latency. Thus, the proposed framework provides complementary mechanisms for identifying abnormal healthcare observations and evaluating resilience against network-level security threats. The

experimental results demonstrate high detection performance having an accuracy of 98.99% and an F1-score of 0.91. This highlights the reliability of the proposed approach. Additionally, the framework shows improved resistance to network-level attacks, reduced packet drop ratio, and stable performance across different network sizes. These results indicate promising scalability and low-latency behaviour within the simulated evaluation environment; real-world deployment would require further validation. The integration of IoT allows continuous health monitoring and real-time data acquisition, while blockchain ensures transparency, traceability, and trust among stakeholders. Overall, the proposed framework successfully combines security, efficiency, and intelligence, making it a promising solution for next-generation smart healthcare systems. Future enhancements involving real-world deployment, advanced attack modelling, and optimization of resource-constrained IoT devices can further strengthen its practical applicability.

References

1. Bawa, G., Singh, H., Rani, S., Kataria, A., & Min, H. (2025). Smart traceable framework for transportation of transplantable organs using IPFS, IoT, and smart contracts. Scientific Reports, 15(1), 23364. https://doi.org/10.1038/s41598-025-06471-2
2. Bawa, G., Singh, H., Rani, S., Kataria, A., & Min, H. (2024). Exploring perspectives of blockchain technology and traditional centralized technology in organ donation management: A comprehensive review. Information, 15(11), 703. https://doi.org/10.3390/info15110703
3. Taherdoost, H. (2024). Wearable healthcare and continuous vital sign monitoring with IoT integration. Computers, Materials & Continua, 81(1), 79–104. https://doi.org/10.32604/cmc.2024.054378
4. Kumar, P., Sharma, R., & Singh, A. (2024). Internet of Things-enabled wearable sensors for real-time health monitoring and smart healthcare applications. IEEE Access, 12, 45678–45695. https://doi.org/10.1109/ACCESS.2024.3378945
5. Alsubaei, F., Abuhussein, A., & Shiva, S. (2024). Security and privacy challenges in Internet of Things-enabled healthcare systems: A review. Sensors, 24(3), 1187. https://doi.org/10.3390/s24031187
6. Bawa, G., & Singh, H. (2024). A Decentralized Application for Managing Organ Donation, Transportation, and Transplantation Processes through Blockchain, Smart Contracts, and Internet of Things Integration. https://doi.org/10.21203/rs.3.rs-4324347/v1
7. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2024). Blockchain for secure healthcare systems: Architecture, applications, and challenges. Future Generation Computer Systems, 154, 210–226. https://doi.org/10.1016/j.future.2024.01.015
8. Bawa, G., & Singh, H. (2025). A framework for IoT-enabled transportation of transplantable organs using smart contracts. In *Proceedings of the 3rd International Conference on Signal and Data Processing* (pp. 517–533). Springer. https://doi.org/10.1007/978-981-97-9578-9_45
9. Bawa, G., & Singh, H. (2026). Revolutionizing organ transplantation logistics through blockchain, smart contracts, and Internet of Medical Things-driven system. *Indian Journal of Transplantation, 20*(2), 183–195. https://doi.org/10.4103/ijot.ijot_118_25
10. Rahman, M. A., Hossain, M. S., Islam, S. R., Alrajeh, N. A., & Muhammad, G. (2024). Blockchain-enabled IoT healthcare systems: Security challenges, limitations, and future directions. Journal of Network and Computer Applications, 233, 103947. https://doi.org/10.1016/j.jnca.2024.103947
11. Sharma, V., You, I., Andersson, K., & Palmieri, F. (2024). Artificial intelligence-based intrusion detection and scalable security solutions for dynamic IoT healthcare environments. Future Generation Computer Systems, 152, 98–114. https://doi.org/10.1016/j.future.2023.11.021
12. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2024). Artificial intelligence applications for intelligent healthcare data analytics and anomaly detection: A review. Healthcare Analytics, 6, 100312. https://doi.org/10.1016/j.health.2024.100312
13. Khan, M. A., Salah, K., Jayaraman, R., Arshad, J., & Omar, M. (2024). Artificial intelligence, blockchain, and IoT convergence for smart healthcare: Opportunities and integration challenges. IEEE Internet of Things Journal, 11(8), 14521–14539. https://doi.org/10.1109/JIOT.2024.3365821

14. Azbeg, K., Ouchetto, O., Andaloussi, S.J. (2022). BlockMedCare: A healthcare system based on IoT, blockchain and IPFS for data management security. Egyptian Informatics Journal, 23(2), 329–343. https://doi.org/10.1016/j.eij.2022.02.001

15. Hossein, K.M., Esmaeili, M.E., Dargahi, T., Khonsari, A., Conti, M. (2021). BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. Computer Communications, 180, 31–47. https://doi.org/10.1016/j.comcom.2021.08.007

16. Teli, T.A., Masoodi, F. (2021). Blockchain in healthcare: Challenges and opportunities. In: Proceedings of the International Conference on IoT Based Control Networks & Intelligent Systems (ICICNIS). https://dx.doi.org/10.2139/ssrn.3882744

17. Quasim, M.T., Radwan, A.A.E., Alshmrani, G.M.M., Meraj, M. (2020). A blockchain framework for secure electronic health records in healthcare industry. In: Proceedings of the International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), pp. 605–609. IEEE. https://doi.org/10.1109/ICSTCEE49637.2020.9277450

18. Chinaei, M.H., Gharakheili, H.H., Sivaraman, V. (2021). Optimal witnessing of healthcare IoT data using blockchain logging contract. IEEE Internet of Things Journal, 8(12), 10117–10130. https://doi.org/10.1109/JIOT.2021.3062744

19. Mohammed, R., Alubady, R., Sherbaz, A. (2021). Utilizing blockchain technology for IoT-based healthcare systems. Journal of Physics: Conference Series, 1818(1), 012111. https://doi.org/10.1088/1742-6596/1818/1/012111

20. Al-Marridi, A.Z., Mohamed, A., Erbad, A. (2024). Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning. Journal of Network and Computer Applications, 224, 103834. https://doi.org/10.1016/j.jnca.2024.103834

21. Al-Nbhany, W.A.N.A., Zahary, A.T., Al-Shargabi, A.A. (2024). Correction to: Blockchain-IoT healthcare applications and trends: A review. IEEE Access, 12, 134084–134084. https://doi.org/10.1109/ACCESS.2024.3431768