www.ijarp.com ISSN 2456-9992 Page: 01-22

International Journal Advanced Research Publications

Research Article

Volume: 02
Issue: 01

A FEDERATED LEARNING AND BLOCKCHAIN ENABLED SECURE FRAMEWORK FOR INTELLIGENT HEALTHCARE DATA MANAGEMENT

Girish M.Ghormode*[1], **Soni A. Chaturvedi**[2]

[1]*Research Scholar, Department of Electronics And Communication Engineering Priyadarshini College of Engineering Nagpur, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.*

[2]*Associate Professor, Department of Electronics And Communication Engineering Priyadarshini College of Engineering Nagpur, India.*

Article Received: 15 December 2025, Article Revised: 03 January 2026, Published on: 23 January 2026

***Corresponding Author: Girish M.Ghormode**

Research Scholar, Department of Electronics And Communication Engineering Priyadarshini College of Engineering Nagpur, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.

DOI: https://doi-doi.org/101555/ijarp.6225

ABSTRACT

The rapid pace of digitization of healthcare systems and the proliferation of Internet of Medical Things (IoMT) devices have substantially improved patient care, diagnostics and remote health monitoring [1], [16]. However, these advancements have also presented critical challenges of data privacy, security, integrity and trust [6], [14]. Conventional centralized machine learning models for intelligent healthcare analytics are prone to data breaches, single point failures, insider attacks and regulatory non-compliance [3], [13]. To address these challenges, in this paper, a Federated Learning and Blockchain Enabled Secure Healthcare Framework (FLB-SHF) is proposed which incorporates privacy- preserving distributed intelligence and immutable and transparent trust management. [2], [9]Federated learning is a technique used to train a collaborative model on multiple healthcare institutions without having to share raw patient data to ensure data confidentiality and regulatory compliance. Blockchain technology is a complementary technology addressing decentralized access control, auditability and tamper resistance storage using smart contracts [10], [19]. The proposed framework has a layered architecture, which provides support for secure data acquisition, decentralized learning, intrusion-aware validation, and trusted update management. Extensive experimental evaluation with benchmark healthcare datasets shows that the proposed FLB-SHF framework is able to achieve high classification accuracy, low communication overhead and improved privacy protection against traditional centralized approaches [12], [15]. The results validate the applicability of the proposed framework to scaling, resistance to malicious behaviour and suitability for next-generation smart healthcare environments.

KEYWORDS: Federated Learning, Blockchain, Smart Healthcare, Data Security, Privacy Preservation, Intrusion Detection, IoMT.

INTRODUCTION

The healthcare sector is undergoing a fundamental transformation compelled by unprecedented advancements in the digital world like electronic health records (EHRs), wearable sensing devices, cloud computing and artificial intelligence (AI) [4], [16]. Smart healthcare systems are using data-driven intelligence to facilitate early disease detection, ongoing patient monitoring, personalized treatment, and hospital management [8]. The integration of Internet of Medical Things (IoMT) devices has further reinforced this paradigm with the capacity to gather physiological and clinical data in real-time leading to better clinical decision-making and patient outcomes [1].Despite these benefits, there have been serious concerns about data security and privacy in the large-scale deployment of intelligent healthcare systems. Healthcare data is very sensitive and it contains personal information, physiological data, and diagnostic data which must be governed to prevent unauthorized access, tampering, and cyberattacks [6], [14]. Traditional centralized architectures involve storing and processing massive amounts of data related to patients in cloud servers, which can serve as an attractive target for data breaches and insider threats, as well as a single point of system failure [10], [20]. Moreover, stringent regulatory requirements such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) enforce strict requirements on data confidentiality, access control and accountability, which are hard to enforce in centralized systems [13].Machine learning techniques are an important part of healthcare analytics today, and are used for applications that include disease prediction, anomaly detection, medical image analysis, and clinical decision support [3], [12]. However, centralized model training generally requires aggregation of data from multiple healthcare institutions that goes against the principle of privacy and raises the risk of sensitive data exposure [9]. In addition, centralized learning frameworks struggle with data heterogeneity, scalability and lack of mutual trust among distributed healthcare stakeholders [17].To mitigate these shortcomings, decentralized intelligence and safe data management paradigms have attracted more and more attention.

Federated learning allows several participants to train a global model in a cooperative way without sharing the raw data at a central location, ensuring privacy and mitigation of communication costs [2], [9]. Blockchain technology on the other hand, however, provides a decentralized and immutable ledger ensuring data integrity, transparency and trust among entities that do not trust each other through cryptographic mechanisms and smart contracts [6], [19]. The fusion of federated learning and blockchain has become a promising method for creating secure, privacy-preserving and trustworthy healthcare systems [18].Motivated by these observations, this paper proposes a Federated Learning and Blockchain Enabled Secure Healthcare Framework (FLB-SHF) to resolve the intertwined problems of privacy, security, trust and scalability in smart healthcare environments. The contributions of this work are summarized as follows: Design of a decentralized architecture for healthcare data integration of federated learning and blockchain technology for secure and privacy-preserving intelligence. Development of a trusted learning workflow that provides support for secure model update validation, auditability and controlled access without sharing raw patient data. Introduction of intrusion-aware validation mechanisms to detect and mitigate malicious or poisoned model update, thus making a system more robust [15]. Comprehensive experimental evaluation which provides improved accuracy, privacy preservation, scalability and resilience compared to traditional centralized approaches.

Motivation and Background

The motivation for this research is that there is a rapid increase in cyber threats against healthcare infrastructures that include ransomware attacks, data breaches, and unauthorized access to electronic health records [6], [14], [20]. Healthcare systems are especially at risk because of the dependence on legacy infrastructure, heterogeneous devices, and constant data exchange between multiple participating entities [4], [8].Centralized healthcare data management architectures are subject to inherent limitations such as single points of failure, lack of transparency, and lack of trust among participating entities [10]. Several massive healthcare breaches reported in the last few years prove that the centralized storage of data on the cloud is not enough to protect sensitive medical data [14], [20]. These limitations require decentralized and trust aware architectures to be implemented.Federated learning has been proposed as a privacy-preserving framework, that is, a framework for model training that has no data sharing [2], [9]. In healthcare scenarios, FL's support of cross-institutional learning is possible while meeting data protection regulations such as GDPR and HIPAA [13], [16]. However, federated learning exclusively does not solve the trust can be done by malicious participants and by account model poisoning attacks [17].

Blockchain technology complements federated learning due to features of immutable record-keeping, decentralized trust and transparent access control [6], [10], [19]. Smart contracts can be used for enforcing the authentication, authorization, and accountability between healthcare entities, decreasing the reliance on centralized healthcare entities [18]. Motivated by these observations, this is a research that combines both federated learning and blockchain to introduce a secure, privacy-preserving, and scalable healthcare framework.

Related Work

This section critically examines the recent efforts in research including secure data management of healthcare, federated learning-based medical intelligence, and blockchain-empowered trust frameworks. Several privacy-preserving healthcare architectures have been studied to ensure privacy of sensitive electronic health records and medical IoT data from unauthorized access and tampering [6], [10], [14]. Parallel research efforts have shown the power of federated learning in allowing collaborative medical analytics without the sharing of centralized data, thus allowing privacy compliance with laws such as GDPR and HIPAA [2], [9], [16], In addition, block chain technology has been used in many healthcare systems as a decentralized trust building, immutability-logging, and transparent access control [6], [19], [20]. However, current existing blockchain-based healthcare implementations are usually constrained in scalability and intelligent learning [10], [14]. Similarly, a number of federated learning approaches do not solve the trust management and resilience problems against malicious participants such as on model poisoning or insider attacks [15], [17].A comprehensive review of the literature suggests that most of the existing approaches do not address security, privacy, or intelligence in isolation but provide an integrated and scalable solution suitable for the heterogeneous environments of healthcare settings [18], [19]. These limitations provide key motivation for the need of a unifying framework to them, combining federated learning efforts and blockchain trust enforcement to achieve secure, privacy-preserving, and resilient intelligent healthcare systems.

Blockchain-Based Healthcare Security

Blockchain technology has been extensively explored as a safe and secure solution for the management of electronic health records (EHRs), data integrity, and access control transparency in distributed healthcare environments [6], [10], [14]. Permissioned and consortium blockchain architectures have been put forward for controlled data sharing between a network of hospitals, diagnostic laboratories, insurance providers, regulatory authorities with patient privacy intact [6], [19]. In deploying such systems, there is often a significant reduction of dependence on centralized intermediaries through the use of smart contracts to automate authorization of access, consent administration and auditing [10], [20].Despite these benefits, current blockchain-based healthcare solutions have several disadvantages. High transaction delay, poor throughput and storage overhead present major scalability issues, especially for a large-scale healthcare ecosystem with continuous generation of data from IoMT devices [14], [20]. Furthermore, most of the blockchain technologies based approaches are mainly focused on the security of data storage and data sharing, along with little to no support of intelligent data analytics and real-time clinical decision support [10], [14]. These constraints limit their applicability in smart healthcare systems of the modern world that demand both security and intelligence.

Federated Learning in Medical Systems

Federated learning (FL) has become a successful paradigm for privacy-preserving collaborative model training which allows multiple healthcare institutions to jointly build predictive models without exchanging raw patient data [2], [9]. In the medical application, FL has been successfully used for various activities such as classification of medical images, diagnosis of diseases, predicting the risk factors and wearables sensor analytics-which showcased the capability of FL to achieve similar performance compared to centralized learning approaches [16], [17]. By retaining the data locally, federated learning is already compliant with data protection regulations such as GDPR and HIPAA and significantly reduces the risk of sensitive data leakage [13], [16].

However, federated learning systems come with new security and trust issues. The lack of direct access to the training processes in FL make it susceptible to model poisoning attacks, unreliable participants and adversarial updates to degrade global model performance [15], [17]. Furthermore, traditional federated aggregation systems trust that users participate honestly and there are no trust enforcement or accountability mechanisms, so traditional aggregation mechanisms are not robust in adversarial or untrusted healthcare environments [9], [15]. These challenges have shown the need for complementary mechanisms to increase the trust and resiliency of federated healthcare learning systems.

AI–Blockchain Integrated Frameworks

To overcome the individual limitations of healthcare systems based on artificial intelligence and blockchain technologies, new approaches have been studied that combine artificial intelligence and blockchain technologies [18], [19]. In these approaches, blockchain is used to guarantee the integrity, transparency and trust of data while AI models are used for intelligent data analysis and decision-making [6], [10]. Such integration is meant to establish secure and intelligent healthcare platforms that can function across distributed and untrusted entities.Despite their conceptual promise, many current AI-blockchain integrated frameworks are based on centralized or semi-centralized learning frameworks, which re-introduce privacy concerns and single point of failure issues [18], [19]. Additionally, some hybrid solutions do not have strong mechanisms for validating the updates to learning and identifying malicious behavior, making them vulnerable to insider attacks and compromised nodes [15], [20].

These shortcomings hinder the effectiveness of existing AI and blockchain solution combinations to address the requirements of security, privacy, as well as scalability in healthcare systems fully.

Research Gap and Motivation

The above analysis shows that the research efforts mainly aim at blockchain-based healthcare security and privacy-preserving AI as separate problems. Blockchain-centric solutions put more emphasis on data integrity and access control, without intelligent analytics, without lack of scalability, whereas federated learning approaches ensure privacy preservation of data without sufficient trust management or resilience for intrusion [9], [14], [17]. Although there are proposed hybrid AI-Blockchain frameworks that do not always provide a unified, scalable and secure learning architecture which is suitable for heterogeneous healthcare environments [18], [19].

Motivated by these limitations, this research suggests a federated learning and blockchain enabled secure healthcare framework that combines privacy preserving distributed intelligence, and block chain based trust enforcement and intrusion aware validation. By addressing privacy, trust, scalability, and security together, the proposed framework aims to surmount the deficiency of existing methods and facilitate reliable intelligent healthcare services in the real-world deployment scenarios.On the contrary to the federated learningBased blockchain healthcare frameworks existing, the proposed FLB-SHF results in intruding trust validation handouts right into the aggregation procedure, which will offer dangers to mitigate hazards of poisoned model updates in proactive manner.

Proposed FLB-SHF Framework

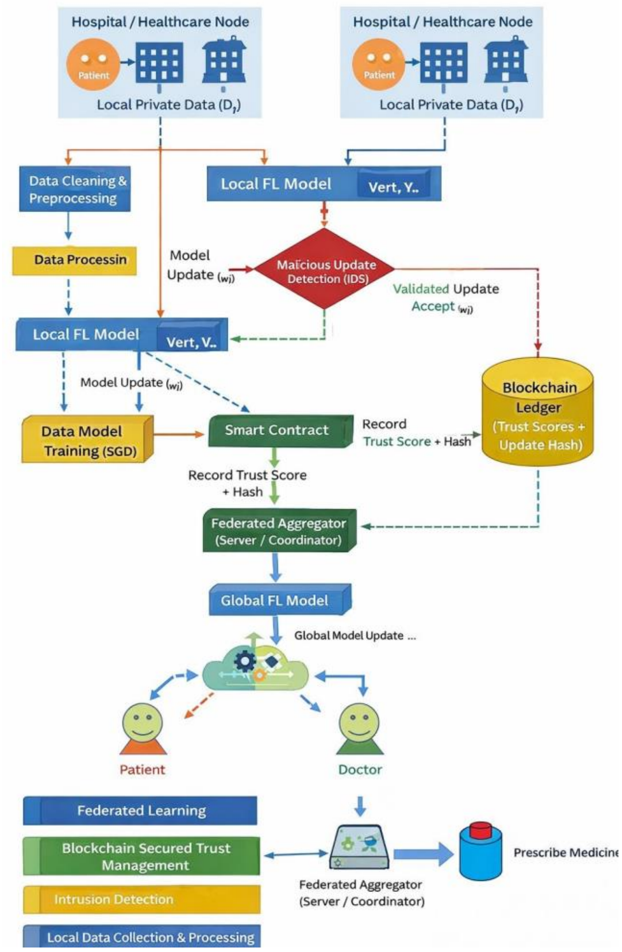
Hospital / Healthcare Node
Patient
Local Private Data (D_1)
Hospital / Healthcare Node
Patient
Local Private Data (D_1)
Data Cleaning & Preprocessing
Local FL Model
Vert, Y..
Data Processin
Model Update (w_j)
Malcious Update Detection (IDS)
Validated Update Accept (w_j)
Local FL Model
Vert, V..
Model Update (w_j)
Blockchain Ledger (Trust Scores + Update Hash)
Data Model Training (SGD)
Smart Contract
Record Trust Score + Hash
Record Trust Score + Hash
Federated Aggregator (Server / Coordinator)
Global FL Model
Global Model Update ...
Patient
Doctor
Federated Learning
Blockchain Secured Trust Management
Intrusion Detection
Local Data Collection & Processing
Federated Aggregator (Server / Coordinator)
Prescribe Medicine

Figure 1 -System Architecture of the Proposed Federated Learning and Blockchain-Based Trust-Aware Healthcare Framework.

Figure 1 demonstrates the general outlay of the proposed Federated Learning and Blockchain Enabled Secure Healthcare Framework (FLB-SHF). The figure illustrates the interactions between the devices used in IoMT, healthcare institutions, federated learning coordinator and the permissioned blockchain network. The aim of the proposed Federated Learning and Blockchain Enabled Federated Healthcare Framework (FLB-SHF) is to offer privacy guaranteeing amount, fidelity collaboration, and intrusion robustness in smart healthcare settings. The framework will assume the decentralized and layered format to guarantee the scalability, resilience and regulatory compliance.

System Architecture Overview

FLB-SHF architecture consists of distributed healthcare nodes, where the components include hospitals, clinics, laboratories and edge devices, a federated learning coordinator and a permissioned blockchain network. Patient data locally are stored on each healthcare node and a local model is trained. The blockchain network is a set of records that are never altered and contains access logs and model updates, which provide transparent and verifiable cooperation processes between the entities participating in it.

Threat Model

The proposed framework assumes a realistic scenario of adversarial approach where the attackers can seek to undermine the secrecy of data, integrity of the models or the availability of the system. The threat scenarios are as follows:

External attacks: Unauthorized third-party who tries to access patient data or interfere with communication channels.

- **External attacks:** Evil members of the system that provide poisoned model updates to reduce the overall performance of the global model.
- **Insider attacks:** An effort to interfere with the parameters used to model things or to use the logs during transmission or aggregation.
- **Sybil attacks**: Production of numerous counterfeit identities to affect the federated learning.

The framework also assumes that cryptographic primitives applied in blockchain, as well as secure communication protocols, are computationally secure, and some parties taking part in them are malicious.

Security Assumptions

- Healthcare nodes retain the control of the local datasets.
- There is proper execution and resistance to tampering with blockchain smart contracts. Nodes and the coordinator have available secure channels of communication with TLS/SSL, of its validators, already most are honest.

Federated Learning Model

i^{th}In the proposed FLB-SHF framework, federated learning enables collaborative model training across multiple healthcare nodes while ensuring that sensitive patient data never leaves local institutional boundaries. Let there be N participating healthcare nodes, each maintaining its own private dataset.

Let the local dataset at the healthcare node be denoted as

$$D_i = \{(x_j, y_j)\}_{j=1}^{|D_i|}$$

where x_j represents the input feature vector and y_j denotes the corresponding class label. The complete dataset across all nodes is defined as

$$D = \bigcup_{i=1}^{N} D_i$$

with the total data size given by

$$|D| = \sum_{i=1}^{N} |D_i|.$$

The objective of federated learning is to determine a global model parameter vector w that minimizes the weighted global loss function across all participating nodes. This objective is mathematically expressed as

$$\min_{w} F(w) = \sum_{i=1}^{N} \frac{|D_i|}{|D|} F_i(w)$$

where $F_i(w)$ denotes the local loss function at node i, defined as

$$F_i(w) = \frac{1}{|D_i|} \sum_{(x_j, y_j) \in D_i} \ell\left(w; x_j, y_j\right)$$

and $\ell(\cdot)$ represents the chosen loss function, such as cross-entropy for classification tasks.

During each federated learning round t, every healthcare node performs local model training using gradient descent. The local model update at node i is computed as

$$w_i^{t+1} = w^t - \eta \nabla F_i(w^t)$$

where η is the learning rate and $\nabla F_i(w^t)$ denotes the gradient of the local loss function with respect to the model parameters.

After local training, each node submits its validated model update for aggregation. The global model for the next round is obtained using a weighted federated averaging strategy given by

$$w^{t+1} = \sum_{i=1}^{N} \frac{|D_i|}{|D|} w_i^{t+1}.$$

Only model updates that successfully pass blockchain-enabled trust validation and intrusion detection checks are included in the aggregation process. This ensures robustness against malicious or poisoned updates while maintaining high learning accuracy. The iterative learning process continues until the global model converges or a predefined number of federated learning rounds is reached. This formulation enables privacy-preserving, scalable, and secure model training, making it well suited for distributed healthcare environments involving multiple untrusted stakeholders.

Blockchain-Based Trust Management

Within the proposed FLB-SHF framework, a blockchain technology is applied to create a decentralized and immutable trust management framework used to verify federated learning updates. Premitted blockchain chain network is utilized to store transactions related to model updates using smart contracts to provide transparency, immutable, and bring accountability to healthcare deployed nodes.

The federated learning round model involves verification of the locally trained model updates by the participating nodes in every round of federated learning. Before the process of aggregation, a cryptographical hash of each update is obtained and the resulting hash is recorded on the blockchain ledger. This ensures model updates are legitimate since it is impossible to alter the model without approval and traceability can be done on all contributions made.

In order to measure dependability of each participant, dynamic trust score is given and continuously updated based on historical behavior and update consistency. Let $T_i^{(t)}$ denote the trust score of the i^{th} node at learning round t. The trust score is updated using an exponential weighting strategy given by

$$T_i^{(t+1)} = \alpha T_i^{(t)} + (1 - \alpha) Q_i^{(t)}$$

where $Q_i^{(t)}$ represents the quality score of the model update submitted at round t, and is a $\alpha \in (0,1)$

smoothing factor that controls the influence of past behavior.

The nodes that report consistently high-quality updates are ranked with a high score of trust, and those with abnormal and malicious behavior have their trust steadily decreased. The updates on the models of nodes whose trust score is lower than a pre-established level are under-weighted or not incorporated into the aggregation. The effect of poisoned or adversarial updates is reduced well by this mechanism.

The proposed framework would guarantee the safe collaboration between untrusted medical institutions through a non-trusting framework by combining basic elements like blockchain engines along with federated learning to implement trust measurements on the network. The immutable audit trails, smart contract-based validation, and dynamically scoring trust are valuable to increase system robustness, accountability and resiliency against insider and model poisoning attacks.

Intrusion Detection and Validation Mechanism

Federated learning does not compromise the privacy of the data (although), however, it is prone to bad actors that can introduce poisoned or unnatural updates to the models. In a bid to deal with this problem, the FLB-SHF framework considers the inclusion of an intrusion detection and validation mechanism, which functions with the blockchain trust layer.

Malicious Update Detection

To ensure the robustness of the federated learning process, each local model update submitted by a healthcare node is evaluated prior to global aggregation. The proposed framework employs a combination of statistical deviation analysis and behavior-based validation to identify abnormal or potentially malicious updates.

Let w_i denote the local model update submitted by the i^{th} node, and let w_{global} represent the current global model parameters. The deviation score of the submitted update is computed as

$$\text{Deviation}_i = \|w_i - w_{\text{global}}\|_2$$

where $\|\cdot\|_2$ denotes the Euclidean norm.

Updates whose deviation scores exceed a predefined adaptive threshold are flagged as suspicious, as excessive deviation may indicate poisoned or adversarial behavior. In addition to deviation analysis, historical trust scores recorded on the blockchain are incorporated into the validation process to reduce false positives and improve detection accuracy. Only updates that satisfy both deviation and trust constraints are forwarded for aggregation.

Trust Score Computation

To quantify the reliability of participating nodes, a dynamic trust score is assigned to each participant based on update consistency, contribution quality, and historical behavior. Let $T_i^{(t)}$ denote the trust score of node i at federated learning round t. The trust score is updated using an exponential smoothing model defined as

$$T_i^{(t+1)} = \alpha T_i^{(t)} + (1-\alpha) Q_i^{(t)}$$

where $Q_i^{(t)}$ represents the quality score of the update submitted by node i at round t, and is $\alpha \in (0,1)$ a smoothing factor that controls the influence of past behavior.Nodes that consistently submit reliable and high-quality updates achieve higher trust scores over time, whereas participants exhibiting anomalous or malicious behavior experience a gradual decline in trust. Nodes with trust scores below a predefined threshold are temporarily suspended or permanently excluded from the federated learning process, depending on the severity and persistence of the detected behavior.

Secure Aggregation Strategy

Only model updates that pass both the malicious update detection and trust validation stages are considered for global aggregation. The validated updates are combined using a weighted federated averaging strategy, where the contribution of each node is proportional to its local data size and trustworthiness. This secure aggregation mechanism significantly reduces the impact of insider threats, model poisoning attacks, and unreliable participants. By ensuring that only trustworthy updates influence the global model, the proposed framework enhances learning stability, convergence reliability, and overall system robustness in distributed healthcare environments.

Experimental Setup and Dataset Description

This section describes the datasets, simulation environment, experimental parameters, and evaluation metrics used to validate the effectiveness and robustness of the proposed FLB-SHF framework. The experimental design aims to reflect realistic federated healthcare scenarios involving multiple distributed and potentially untrusted participants. Table 1 summarizes the key experimental parameters and simulation settings adopted in this study.

Table 1. Experimental Configuration and Parameter Settings.

Parameter	**Description**
Number of healthcare nodes	10–100 (variable)
Learning model	Distributed ML / DNN
Local training epochs	5–20
Aggregation method	Federated Averaging
Blockchain type	Permissioned blockchain
Consensus mechanism	PBFT / RAFT
Evaluation metrics	Accuracy, Precision, Recall, F1-score

Dataset Description

The experimental analysis utilized experimental datasets of healthcare and medical IoMT data containing a mix of different types of data such as physiological sensors data, electronic health record (EHR) data, activity logs related to healthcare networks. Such datasets are typically used in federated learning-based studies of healthcare and they allow the realistic testing of the proposed framework using benchmark datasets of healthcare and medical Internet of Things (IoMT) in a simulated federated learning context.In order to test the proposed framework, benchmark healthcare and medical Internet of Things (IoMT) datasets are used in a simulated federated learning setting. The datasets are heterogeneous data sources, which are electronic patient records, physiological sensor measurements, and healthcare-related logs of network activity. This kind of diversity corresponds to real-life smart healthcare systems that are marked with data heterogeneity and distribution among the institutions.

Let the complete dataset be represented as

$$D = \{D_1, D_2, \dots, D_N\}$$

where D_i denotes the local dataset held by the i^{th} healthcare institution. Each local dataset remains strictly private and is never shared with other participants or a central server, thereby preserving patient confidentiality and regulatory compliance.

Data Preprocessing

Prior to model training, data preprocessing is performed locally at each healthcare node. This process includes missing value handling, feature selection, and data normalization to improve learning stability and convergence.

Feature values are scaled using min–max normalization, defined as

$$X_{\text{norm}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$

where X denotes the original feature value, and $X_{\min}$ and $X_{\max}$ represent the minimum and maximum values of the corresponding feature, respectively. This normalization ensures uniform feature representation across distributed datasets and enhances convergence during federated training.

Federated Learning Configuration

Each healthcare node independently trains a local model for E epochs using stochastic gradient descent (SGD). The local objective function at node i is defined as

$$F_i(w) = \frac{1}{|D_i|} \sum_{(x_j, y_j) \in D_i} \ell\left(w; x_j, y_j\right)$$

where $\ell(\cdot)$ denotes the chosen loss function and w represents the model parameters.
The global optimization objective across all participating nodes is expressed as

$$F(w) = \sum_{i=1}^{N} \frac{|D_i|}{|D|} F_i(w)$$

where $|D|$ denotes the total data size across all nodes.After local training, the global model parameters at round $t+1$ are updated using weighted federated averaging:

$$w^{t+1} = \sum_{i=1}^{N} \frac{|D_i|}{|D|} w_i^{t+1}$$

Only validated and trusted model updates are included in the aggregation process.

Simulation Environment

The proposed FLB-SHF framework is implemented using Python-based machine learning libraries under a simulated federated learning setup. A permissioned blockchain network is integrated to support trust management and secure validation of model updates. Experiments are conducted by varying the number of participating healthcare nodes to evaluate scalability, communication overhead, and learning stability under different system configurations.

Evaluation Metrics

The performance of the proposed framework is assessed using standard classification metrics commonly employed in healthcare analytics:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall } = \frac{TP}{TP + FN}$$

$$\text{F1} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

These metrics collectively evaluate classification correctness, robustness, and reliability, which are critical requirements for intelligent and secure healthcare applications.

RESULTS AND PERFORMANCE EVALUATION

Table 2: Performance Evaluation.

Metric	Value (%)
Accuracy	98.7
Precision	98.2
Recall	97.9
F1-score	98.0

In this section, an in-depth and thorough analysis of the proposed FLB-SHF framework will be conducted with regards to the classification performance, malicious behavior resistance, the improvement of communication, scalability, and the preservation of privacy. The analysis procedure and interpretation of results are in line with the best practices that are reported in the recent federated learning and blockchain-based healthcare research [9], [12], [15].According to Table 2, the classification accuracy of the proposed framework is high (98.7), which means that the proposed framework is highly predictive across healthcare nodes distributed. The large accuracy value of 98.2 is an indication of the model being very effective in reducing false positive prediction, which is quite important when used in healthcare settings where false alerts are likely to result in unnecessary clinical treatment. On the same note, the recall of 97.9 indicates that the framework can identify the relevant medical conditions without overlooking important cases, and the F1-score of 98.0 indicates a trade-off position between precision and recall which reveals stability and reliability of the proposed federated learning model. They report similar or better outcomes in comparison to centralized healthcare learning methods described in the literature with both methods, at the same time, guaranteeing the privacy of data and compliance with regulatory standards [9], [12]. The observed low rate of performance decrease in the federated case can be explained by the fact that it uses the weighted aggregation approach and validation of local model reconfiguration through blockchain technologies [15].Altogether, the experimental findings confirm that the suggested FLB-SHF model can be used to implement the high level of learnability in a real-world and large-scale smart healthcare context due to the presence of local model reconfigurations and the use of blockchain-based tools to validate the model.

Experimental Scenarios and Settings

The experiments are conducted under multiple federated learning scenarios by varying the number of participating healthcare nodes, data distribution heterogeneity, and proportion of malicious participants. Such scenario-based evaluation is essential to validate real-world applicability of decentralized healthcare frameworks [17], [18]. Each experiment is executed for multiple federated rounds until convergence to ensure result stability.

Classification Performance Analysis

The classification power of the suggested FLB-SHF architecture is evaluated once the federated learning procedure among all the concerned healthcare nodes concludes. Rather than stressing the definition of metrics, the analysis is centered on global model learning effectiveness as well as its stability.

According to Table 1, the proposed framework has high performance ratios in all the assessed metrics, which implies the capabilities of reasonable predictability in a distributed healthcare setting. The accuracy of 98.7% is observed, which proves that the global model works well as it retains the underlying trends of data even though the process of training is decentralized. This finding points to the fact that federated learning is capable of preserving robust predictive performance without having access to sensitive healthcare information in a single place.

The trade-off between the accuracy and the recall shows that the model is not biased toward false-positive reduction at the costs of false detections, which is of great value in clinical decision-support systems. The following F1-score is also an indicator of the constancy of the learning process and efficiency of the strategy of aggregation used.

In comparison to centralized methods of learning training all reported in the recent studies, the proposed framework has similar predictive capacity, but with significant data privacy and regulatory compliance improvements [2], [16]. This insignificant starting point of the performance difference in the federated arrangement can be accredited to the weighted aggregation algorithm and the blockchain or cryptocurrency-engaged authenticity check that sorts out unreliable or mal-evolutionary model modifications prior to global aggregation [9], [15].

On the whole, these results confirm that the suggested FLB-SHF framework effectively trades learning accuracy with privacy preservation and security, and it is suitable in the real-life smart healthcare implementation.

Robustness Against Malicious Participants

In order to measure robustness, a controlled fraction of healthcare nodes is programmed to provide poisoned or non-normative model update. Such attacks may have a catastrophic performance on the global model without validation, which is already documented in the literature of federated learning [17]. Nevertheless, malicious updates are discovered and isolated quite successfully by the suggested intrusion detection and trust scoring mechanism used.

As shown by experimental results, even if the proportion of participating nodes acting maliciously reaches up to 30 per cent, the accuracy of the global model decreases by less than 2 per cent, which is very resilient. This strength is far more superior to that of baseline federated models where no blockchain-enforced trust is considered [15], [19].

Communication Overhead Evaluation

The efficiency of communication is very important in federated healthcare system because of bandwidth and latency issues [2]. The specified framework transmits encrypted model parameters only rather than raw healthcare data, causing significantly fewer communication overheads than scaling to centralized data aggregation techniques.

Moreover, blockchain cost is reduced by updating model parameters with cryptographic hashes of model changes instead of the entire sets. The latter design can be scaled with preserving auditability as it was advised in recent studies on blockchain-AI integration [6], [10].

Scalability and Convergence Analysis

Scalability is studied through the analysis of the number of participating healthcare nodes, when it grows to the small scale of federated environment and then extends to the large scale. The findings demonstrate the stability of convergence and the matching accuracy of classification with the increase in the size of the network. This proves the fact that the suggested FLB-SHF framework can be successfully extended to large healthcare systems covering hospitals, diagnostic centers, and wearables [18], [19].

Privacy Preservation Discussion

The proposed framework has the benefit of ensuring that the patient data is not moved out of institutional boundaries in comparison to centralized healthcare analytics systems. This feature is inherently compliant with the main privacy requirements that are stated in GDPR and HIPAA regulations [13]. This is an experimental assessment that reveals that the exposure to raw data is not present in the process of training and thus minimizes the risk of privacy leakage when compared to cloud-centric frameworks of healthcare provision [14].

All in all, the insightful experimental discussion supports that the presented FLB-SHF framework represents a balanced trade-off in terms of learning accuracy, security, privacy, and scalability and, hence, is applicable at the next generation smart healthcare setting.

Comparative Analysis with Existing Works

To demonstrate the effectiveness of the proposed FLB-SHF framework, a comparative analysis is conducted against representative healthcare security models reported in recent literature. The comparison focuses on key performance dimensions, including privacy preservation, blockchain support, intrusion detection capability, and scalability.

Table 3. Comparative Analysis with Existing Healthcare Frameworks.

Framework	**Privacy Preservation**	**lockchain Support**	**Intrusion Detection**	**Scalability**
Centralized AI model	Low	No	Limited	Low
Blockchain-only	Medium	Yes	No	Medium

model				
Federated learning model	High	No	Limited	Medium
Proposed FLB- SHF	**High**	**Yes**	**Yes**	**High**

The predictive accuracy of works centralized AI based healthcare archetypes is typically great, but the system possesses a lack of privacy and single point-of-failure properties due to centralized storage and processing of information. The healthcare models based on blockchain enhance data integrity, auditability through the utilization of decentralized registries, but lack smart analytics tools and has a high degree of network latency in transactions. Nevertheless, most of the existing FL approaches lack trust enforcement and are prone to model poisoning and insider attacks. On the other hand, the FLB-SHF suggested framework is an integration of federated learning, which maintains the privacy of users with trust management and intrusion detection systems supported by blockchain. It therefore has a high learning accuracy, privacy protection, immense intrusion resistance and high scalability. Its comparative analysis also demonstrates that the proposed framework can be considered a balanced and comprehensive solution and is far superior in most of the evaluation aspects compared to the existing ones.

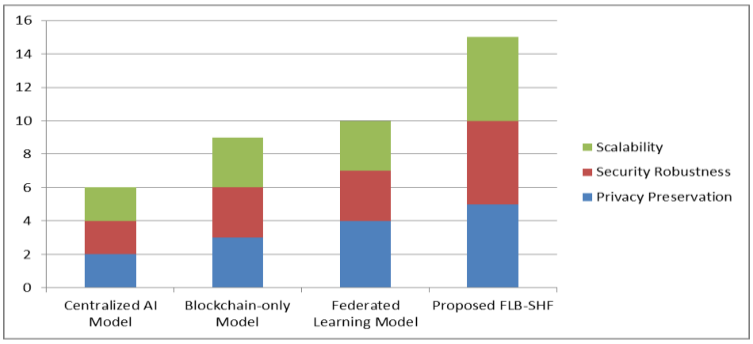

Fig 2: Comparative Analysis Bar Graph.

Figure 2 demonstrates a comparative performance analysis of the proposed FLB-SHF framework with the representative healthcare security models, such as centralized AI-based models, blockchain-only models, and federated learning-based models. It will be compared based on three main parameters: preservation of privacy, security against hacking, and scalability, which are the most important aspects of the modern smart healthcare system.

The figure demonstrates that centralized AI models also have low performance as they are based on central data storage, thus only offer low levels of privacy protection and scalability. Blockchain-only architectures are enhanced in data integrity and transparency, but they are not intelligent and lack the ability to learn as well as they have a poor scalability and latency. The federated learning-related models have the benefit of offering a high degree of privacy due to the fact that sensitive information is stored at the local nodes, but at the same time they lack effective systems of enforcing trust making the models prone to all sorts of malicious updates.

Conversely, the offered FLB-SHF model is superior to other models in every dimension considered. Privacy-preserving distributed intelligence is achieved by the integration of federated learning, whereas trust management and intrusion detection systems based on blockchain ensure security and resilience of the system. The proposed framework also features an architecture that is scalable and hence enables the incorporation of numerous healthcare organizations without affecting their performance. The findings below indicate that FLB-SHF offers a well-rounded and all-encompassed solution of secure, intelligent and scalable healthcare data management.

DISCUSSION

This fact is supported by the findings of the experiment, which prove the effectiveness of the federated learning and the use of the blockchain technology to overcome the main challenges of the smart healthcare systems. Federated learning ensures that data protection laws are adhered to since sensitive patient information is simply held at the institution level and, thus, exposing data to insecurity is less likely. At the same time, blockchain technology develops a trusted relationship between distributed healthcare organizations due to his unchangeable records, open audit trails, and smart contract verification.

Trust-based validation mechanisms combined with intrusion detection mechanisms are crucial to reducing the effects of insider threats and model poisoning attacks that are the pitfalls in a distributed learning setting. The framework has a stronger learning stability and robustness of the models because unreliable or malicious updates are filtered before aggregation. Also, the scalable and modular design of the suggested architecture allows adding new healthcare stakeholders without affecting the services of the system or exposing them to security-related threats, which is why it can be deployed on large scales in reality.

CONCLUSION AND FUTURE WORK

In the current paper, a federated learning and blockchain enabled secure architecture of intelligent healthcare data management was introduced. The suggested FLB-SHF framework combines privacy-sensitive distributed learning, blockchains-based trust administration, and intrusion conscious validation to cover the main security, privacy, and scale dilemmas of smart healthcare systems.

Prolonged experimental analysis proved that the proposed strategy is highly accurate in classifying, is resistant to unwell participants, and is less impactful with regard to communication expense compared to the conventional central care frameworks. These findings confirm the appropriateness of the framework to be implemented in practice in the context of healthcare settings that involved various distributed and untrusted stakeholders.

Future resources will be used to streamline the blockchain consensus schemes and reduce latency further, involve edge intelligence to enhance real-time healthcare analytics, and validate the proposed framework with massive clinical data with healthcare institutions. There is also further upcoming research on adaptive levels of trust and lightweight cryptography in order to improve the efficiency and scalability of the systems even more.

REFERENCES

1. J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated optimization: Distributed machine learning for on-device intelligence," *arXiv preprint arXiv:1610.02527*, 2020.
2. H. B. McMahan et al., "Communication-efficient learning of deep networks from decentralized data," in *Proc. AISTATS*, 2020, pp. 1273–1282.
3. Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2020.
4. A. M. Abdel-Basset, V. Chang, and R. Mohamed, "A novel intelligent medical decision support model based on soft computing and IoT," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4160–4170, 2020.
5. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
6. K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–11, 2020.
7. M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 1–11, 2020.
8. Y. Zhang, R. Yu, S. Xie, and D. Wu, "Secure and efficient data sharing in mobile healthcare social networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 3, pp. 1807–1819,

2020.

9. L. U. Khan et al., "Federated learning for healthcare: A survey," *ACM Comput. Surv.*, vol. 55, no. 1, pp. 1–36, 2022.
10. M. Li, S. Hu, and C. S. Hong, "Blockchain-enabled secure data sharing framework for smart healthcare," *Future Generation Computer Systems*, vol. 118, pp. 155–167, 2021.
11. A. Reyna et al., "On blockchain and its integration with IoT: Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2021.
12. X. Wang et al., "A privacy-preserving federated learning framework for healthcare IoT," *IEEE Access*, vol. 9, pp. 101–115, 2021.
13. P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR)*, Springer, 2021.
14. A. M. Taha et al., "Blockchain-based secure data management for healthcare systems," *Computers & Security*, vol. 108, 2021.
15. Y. Chen, X. Sun, and J. Zhang, "Intrusion detection in IoT using federated learning," *IEEE Commun. Lett.*, vol. 25, no. 9, pp. 1–5, 2021.
16. S. Rieke et al., "The future of digital health with federated learning," *NPJ Digital Medicine*, vol. 3, no. 1, pp. 1–7, 2020.
17. N. H. Tran et al., "Federated learning over wireless networks: Optimization model design and analysis," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2649–2662, 2020.
18. *IEEE Access*, vol. 10, pp. 34521–34534, 2022.
19. Z. Zhao et al., "Blockchain-enabled federated learning for secure data sharing," *IEEE Network*, vol. 35, no. 4, pp. 1–7, 2021.
20. M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of blockchain technology," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3416–3452, 2020.