INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

FLPPBC: A Federated Learning-Driven Privacy-Preserving Model Using Private Permissioned Blockchain for Healthcare Systems

M Sukanya[1]*, V Jude Nirmal[2], George Gabriel Richard Roy[2]

1 Research Scholar, Department of Computer Science, St.Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli – 620002, Tamil Nadu, India
2 Assistant Professor, Department of Computer Science, St.Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli – 620002, Tamil Nadu, India
3 Assistant Professor, Department of Computer Science, St.Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli – 620002, Tamil Nadu, India

OPEN ACCESS

Received: 13/12/2025
Accepted: 30/12/2025
Published: 22/01/2026

Citation: Sukanya M, Jude Nirmal V, Richard Roy GG (2026) FLPPBC: A Federated Learning-Driven Privacy-Preserving Model Using Private Permissioned Blockchain for Healthcare Systems. Indian Journal of Science and Technology 19(2): 59-70. https://doi.org/10.17485/IJST/v19i2.1956

* **Corresponding author**.

sukan2suresh@gmail.com

Funding: None

Competing Interests: None

Copyright: © 2026 Sukanya et al. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To utilize federated learning and blockchain for developing a layered security model to offer protection and discretion of patient data in a private healthcare system. **Method:** To improve the security and confidentiality in smart healthcare, this work proposes a Federated Learning-driven Privacy Preserving Blockchain (FLPPBC) model which contains three layers: data, blockchain and aggregated. In data layer, the homomorphic encryption algorithm is used to encrypt the data and local model training parameters. The gradient boosting algorithm is used to generate the local training model. The SHA-256 hashing method and Proof of Authority (PoA) consensus mechanism is employed in blockchain layer to provide the safety and privacy. The weighted average aggregation is utilized in aggregated layer to build the global model. The medical dataset heart disease and breast cancer from UCI repository is utilized to evaluate the effectiveness of FLPPBC in terms of accuracy, precision, recall, f-measure, latency and throughput. **Findings:** FLPPBC utilized healthcare datasets (heart disease and breast cancer) to analyze the performance. It attains more than 98% accuracy for health data. FLPPBC also achieves minimum latency (39.27 ms) and maximum throughput (125 Trans/Sec). The approach efficiently handles many transactions and adds them to the blockchain quickly, reducing latency. **Novelty:** FL efficiently trains decentralized data using machine learning models, and homomorphic and BC enables secure access to distributed patient data without compromising confidentiality. The proposed approach uses gradient boosting for healthcare data classification, and SHA-256 and PoA provide the security model.

Keywords: Blockchain; Federated learning; Healthcare; Homomorphic encryption; Privacy-preserving; Data security

1 Introduction

Federated Learning (FL) is an effective method that protects data security while assisting model training by enabling machine learning algorithms to be trained on decentralized data disseminated across different sources [1]. FL reduces latency and provides tailored guidance, thereby not only minimizing data security threats but also enhancing operations. However, challenges such as server failure and malicious attack persist. Due to differences in patient populations, medical information is often shared among institutions. This could reduce global model accuracy [2]. Additionally, the central server consolidation for model updates is under scrutiny due to concerns about probable weaknesses. Due to the increasing volume of medical information, it is critical to protect it from cyber attacks [3]. Secure aggregation and Secure Multi-Party Computation (SMPC) were investigated to address the privacy issues in federated learning environments.

With secure aggregation, the server receives aggregated changes, rather than individual client updates [4]. However, access to the aggregated gradients is allowed, which compromises data about the base model. One of the standard methods of FL is Differential Privacy (DP), which secures personal data by making model updates less reliable by adding noise [5]. Although DP is easy to implement, it is vulnerable to insufficient confidentiality guarantees, which reduces accuracy. In addition, DP may cause privacy issues because it transfers gradients to a central server. SMPC allows multiple clients to compute a function over their private data without sharing it [6]. However, geo-distributed FL cannot leverage SMPC due to its high processing overhead and complex synchronization.

Blockchain (BC) is a decentralized, shared ledger that makes secure, accessible data storage and transactions. With the database continually updated by all parties involved, it preserves an extensive record of all transactions, doing away with centralized authority [7]. Figure 1(a) shows a blockchain structure that contains a sequence of blocks with hash values. The single block in BC is shown in Figure 1(b), which contains a header and a data section. The block data comprises a set of transactions and is connected to the preceding block using cryptographic hashes.

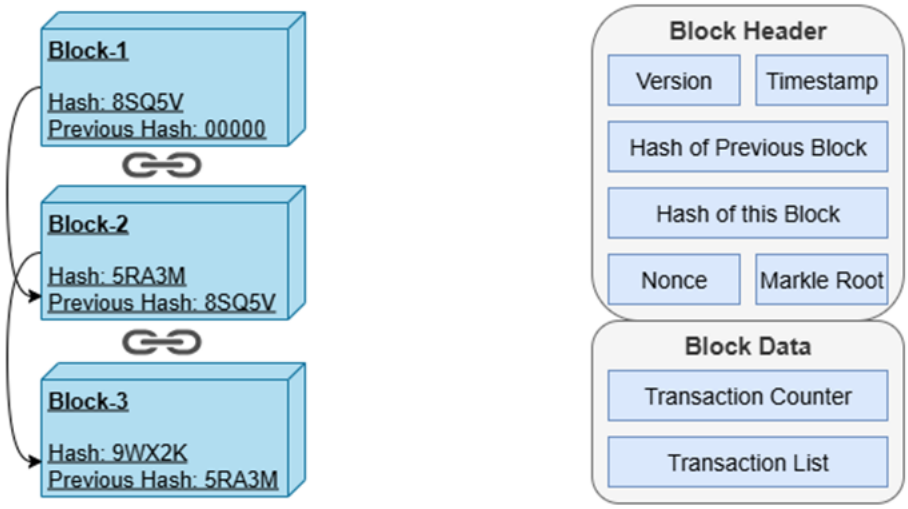

Fig 1. Blockchain structure and Single block in blockchain

One main benefit of BC is that it does not require intermediaries in transactions due to its decentralized nature. To strengthen security and reduce fraud, the distributed consensus approach ensures that all nodes in the network agree on the legality of transactions [8]. The smart contracts and consensus mechanism are the main elements of BC. Consensus methods are used to ensure that network members agree on the legitimacy of transaction and their proper order in the BC. Some examples of consensus methods are Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), etc. Smart contracts are programs that autonomously execute predefined activities when certain conditions are met. The contracts become automatic and legally binding.

The integration of BC and FL has been investigated by researchers to address the issues with secure aggregation and DP. This can decentralize the process and enhance the security. It provides a feasible option by increasing data decentralization and ensuring data reliability through immutable ledgers[9]. By optimizing the use of medical data while protecting patient privacy, this combination presents a game-changing opportunity in healthcare.

Ethereum's advanced smart contract capabilities make it easy to execute complex agreements, to ensure that model revisions are clearly documented and comply with established standards[10]. The Proof-of-Authority (PoA) is one of the consensus mechanisms that uses a lot of energy but improves security by discouraging bad participants and exerting computing effort[11]. The BC with FL enhances both the safety and reliability of the learning process, instilling confidence among all participants in the shared model and in one another.

Stephanie et al.[12] introduce a federated learning model that incorporates blockchain technology, allowing hospitals to work together securely while protecting patients' privacy. This method uses BC to ensure the data authenticity and reliability. This approach has high computational and communication costs, along with privacy and storage issues. To enhance the confidentiality of healthcare IoT data, Moulahi et al.[13] combine BC with FL. Ruvunangiza et al.[14] offer an architecture that integrates Blockchain with federated learning to improve the secure sharing of healthcare data. FL facilitates decentralized data analysis, whereas Blockchain guarantees an immutable record for monitoring data transactions, thereby enhancing patient privacy and adherence to data governance rules, but it faces scalability challenges. Alsamhi et al.[15] explain the technical foundations of federated learning and Blockchain, revealing their roles in transforming healthcare data sharing. This method safeguards patient confidentiality while allowing healthcare professionals and academics access to diverse datasets, resulting in improved models and better diagnoses. The drawbacks of this method include technical complexity, scalability, and regulatory compliance.

Commey et al.[16] present a paradigm that combines BC, FL, and DP for safe health information analytics in blockchain-based IoT systems. It guarantees data confidentiality, openness, and privacy while upholding high precision in health analytics operations. Munusamy et al.[17] suggest aprivacy-preserving methodto improve the management of Electronic Health Records. This approach addresses issues such as substantial processing costs, communication latency, and security concerns. The three-layer design ensures data privacy via Differential Privacy and SMPC, while the blockchain layer provides tamper-proof auditability, making it suitable for secure and efficient healthcare applications. This approach was susceptible to model and poisoning attacks. Khan et al.[18] examine an innovative method that combines BC with FL to enhance healthcare information exchange. Blockchain guarantees data integrity and trust through a decentralized ledger, while smart contracts enforce data usage regulations. The possible constraints of smart contracts in monitoring data usage regulations, which may affect data governance, have not been well examined.

To protect the medical data against poisoning assaults, Prashanth et al.,[19] suggests a method which integrates blockchain technology and federated learning. The framework employs SMPC for model verification, ensuring that compromised models are detected and eliminated before to aggregation. Myrzashova et al.[20] propose a blockchain-based Federated Learning system for the diagnosis of 15 lung illnesses, safeguarding patient data privacy. It attains 92.86% accuracy and 43.52 ms latency, exhibiting robustness against cyber threats with resilience metrics approaching 87%. Bhardwaj et al.[21] suggest the Privacy Preserving Federated Blockchain Explainable Artificial Intelligence Optimization framework, which amalgamates blockchain technology, Explainable AI (XAI), and optimization methodologies to guarantee privacy, traceability, and resilience in federated learning systems. It struggles with large-scale deployments and higher latency for large networks.

Recent studies have discovered blockchain-based federated learning frameworks to improve the security and confidentiality of healthcare information sharing. However, existing methods often rely on differential privacy, secure multi-party computation, or complex consensus mechanisms, which introduce high computational overhead, increased latency, and scalability limitations. In particular, widely used consensus protocols such as Proof of Work, Proof of Stake, and PBFT are inefficient for time-sensitive healthcare environments. Moreover, most prior works focus on secure data storage or access control, while offering limited support for efficient and privacy-preserving collaborative model training. To address these challenges, this study proposes a secure and scalable blockchain-assisted federated learning framework for healthcare data sharing. This study integrates homomorphic encryption to preserve data confidentiality during model training and employs a Proof of Authority consensus mechanism to reduce latency and improve scalability. In addition, gradient boosting is utilized for accurate healthcare data classification. The key novelty of this work lies in the unified integration of federated learning, homomorphic encryption, and lightweight blockchain consensus to achieve secure, efficient, and privacy-preserving collaborative analytics, addressing critical limitations of existing solutions.

Table 1 summarizes the related work, including the methods used, findings, limitations, and research gaps. The previous approaches have data privacy issues, a lack of data in FL, and model updates are not well protected, which disclose deficiencies in privacy-preserving data analysis, a significant computational and communication burden. To resolve these issues, this paper

presents a Federated Learning-driven Privacy-Preserving Blockchain (FLPPBC) model utilizing homomorphic encryption to augment security and confidentiality in smart healthcare. It reduces the significance of the central server, facilitates collaborative model training among healthcare organizations, and enhances data security and privacy. Homomorphic encryption enables encrypted gradient aggregation, guaranteeing that the central server remains devoid of access to unprocessed model updates. The main objectives of this research work are:

- To develop a privacy-preserving framework that integrates blockchain, federated learning, and homomorphic encryption to secure patient data.
- To generate a local training model using a gradient boosting algorithm that effectively classifies the healthcare data.
- To utilize the SHA-256 hashing method and the PoA consensus mechanism to provide security, privacy, and reduce latency and throughput.
- To formulate a weighted average aggregation to generate the global model.
- To evaluate the efficiency of the suggested approach through simulation and discuss the performance results.

2 Methodology

The proposed FLPPBC methodology develop layered privacy-preserving security framework which integrates federated learning, blockchain and homomorphic encryption to secure patient data. The proposed layered framework has three layers: Data layer, Blockchain layer and aggregated layer shown in Figure 2. The data layer has a different number of healthcare providers; each provider collects data and encrypts it using homomorphic encryption. The gradient boosting algorithm was used to generate the local training model which effectively classifies the healthcare data. The parameter of the local training model was encrypted using homomorphic encryption and sent to Blockchain layer. The blockchain layer uses the SHA-256 hashing method and the PoA consensus mechanism to provide security and privacy of healthcare data which reduces latency and throughput. The aggregated layer employs weighted average aggregation for generating the global model and distributes the model to the data layer.

Federated learning utilizes machine learning models for training decentralized data without compromising confidentiality, and BC and homomorphic encryption allow secure and privacy-preserving data access. This work uses heart disease and breast cancer dataset collected from UCI repository and publicly available at link: https://archive.ics.uci.edu/dataset/45/heart+disease and https://archive.ics.uci.edu/dataset/17/breast+cancer+wisconsin+diagnostic.

The FLPPBC has an 'N' number of Healthcare Providers (HP), each with a local server. Each HP is expected to have its own server that can process or train on the healthcare data it holds, guaranteeing the privacy and security of data. Every HP collects data locally, encrypts it using homomorphic encryption, and generates a local model. The blockchain layer not only retains the local model but also keeps track of modifications to the local model. Each local model is aggregated by the aggregation layer, and a new global model is generated using the average of the local models. This architecture is designed to provide decentralized data sharing and learning that utilizes the benefits of FL and BC to improve data security and privacy. In the data layer, the homomorphic encryption is used to encrypt the local data and training model, the blockchain layer employs a private permission blockchain and tamper-proof storage, which uses SHA256 and PoA to provide privacy, and the aggregated layer uses weighted average aggregation to generate a global model. Algorithm 1 explains the proposed FLPPBC.

This algorithm generates the blockchain ledger as well as the global federated learning model. Before beginning local model training, each healthcare provider encrypts their local dataset using homomorphic encryption. Integrity and traceability are then guaranteed by recording the encrypted model updates as blockchain transactions. The global model is then created by securely aggregating the encrypted updates. The step 5 was used to encrypt the dataset, and Step 6 was used to generate the local training model. The local model training parameters are also encrypted using homomorphic encryption and stored in blockchain. The global model was generated using weighted average aggregation.

2.1 Homomorphic Encryption and Local Mode Training

In this layer, several healthcare providers preserve their distinct medical records for each patient. Consequently, each healthcare provider maintains patient data within their local databases. The healthcare data is encrypted using homomorphic encryption. A homomorphic encryption strategy is one that fulfils **Eq. (1)**, where E is the encryption algorithm, and M is the set of messages [22].

$$E(m_1) \circledast E(m_2) = E(m_1 \circledast m_2), \quad \forall m_1, m_2 \in M \tag{1}$$

Table 1. Summary of Related Works

Ref.	Methods Used	Findings	Limitations/Research Gap
[12]	Secure-Multiparty Computation-based ensemble FL	A privacy-preserving blockchain-based federated learning scheme improved the accuracy of the models.	Healthcare 4.0 data privacy issues, with different institutions' storage and computing capacities.
[13]	Trusted Blockchain-based FL	It provides data privacy and model integrity.	Privacy concerns in the sharing of healthcare IoT data.Safeguarding medical machine learning systems from cyberattacks
[14]	Unified framework that integrates FL, Blockchain, and quantum cryptography	A cohesive structure improves secure sharing of healthcare data.	The potential scalability challenges of the integrated system across diverse healthcare facilities remain unaddressed.
[15]	Decentralized data sharing using the Synergy of Blockchain with FL	The integration of federated learning with Blockchain aims to create a healthcare ecosystem that emphasizes individual privacy while advancing medical science.	The legal and regulatory aspects need the examination of frameworks that protect privacy during data sharing.
[16]	Differential privacy, adaptive noise distribution	Attains robust privacy assurances while preserving elevated precision in analytical endeavors.	Discerns deficiencies in privacy-preserving data analysis
[17]	Differential privacy, Secure-Multiparty Computation, PoS + BFT consensus	It attained higher accuracy on the CIFAR-10 dataset, illustrating its efficacy in model performance. It demonstrated significant resilience to adversarial attacks, signifying powerful security and privacy protection features.	Extensive communication delay due to repeated model updates and computational issues on edge devices. It is vulnerable to model and data poisoning attacks.
[18]	Consensus-based mechanism, Smart contracts, secure aggregation	The incorporation of Blockchain improves data integrity, immutability, and trust within a decentralized framework, functioning as a secure ledger for model modifications.	The possible constraints of smart contracts in monitoring data usage regulations, which may affect data governance, have not been well examined.
[19]	Secure-Multiparty Computation model verification	It highlights the significance of safeguarding the model's privacy while simultaneously identifying detrimental updates in federated learning contexts.	A persistent issue remains in obtaining the aggregation of local models after verification, which is crucial for maintaining the reliability of the global model.
[20]	Deep learning model, Ethereum BC with PoW,	It markedly reduced dependence on centralized computational resources, promoting efficient resource utilization and cost savings.	The unresolved potential impact of disparate data quality from various hospitals on the model's performance may influence diagnostic accuracy.
[21]	XAI, Entropy Deep Belief Network	It attained superior accuracy, reduced latency and loss, and enhanced throughput and interpretability.	Blockchain integration elevates computational and communication burdens, presenting scalability and real-time implementation obstacles. Synchronization expenses increase with the quantity of nodes, impacting performance in extensive networks.

There are typically three main categories of homomorphic encryption[22]: *Partially Homomorphic Encryption:* It can be used for an endless number of times to perform a single type of operation (e.g., only additions or only multiplications). *Somewhat Homomorphic Encryption:* Both operations are allowed, but with a limit on how many times they can be performed. *Fully Homomorphic Encryption:* endless execution of an infinite number of operations. Due to the computational efficiency and appropriateness, this work focuses Partially Homomorphic Encryption (PHE) for securing data.

In this work, the Python library LightPHE[23] was employed. This is a lightweight library for hybrid partly homomorphic encryption (PHE) intended for Python. It offers a pragmatic and effective method for executing computations on encrypted data without necessitating full homomorphic encryption (FHE), which tends to be more computationally demanding. It encompasses all requisite methods for homomorphic operations, including the addition of ciphertexts, multiplication of ciphertexts, XOR of ciphertexts, scalar multiplication of a ciphertext with a constant, and ciphertext regeneration.

The procedure for preserving the confidentiality of healthcare data through PHE is defined below:

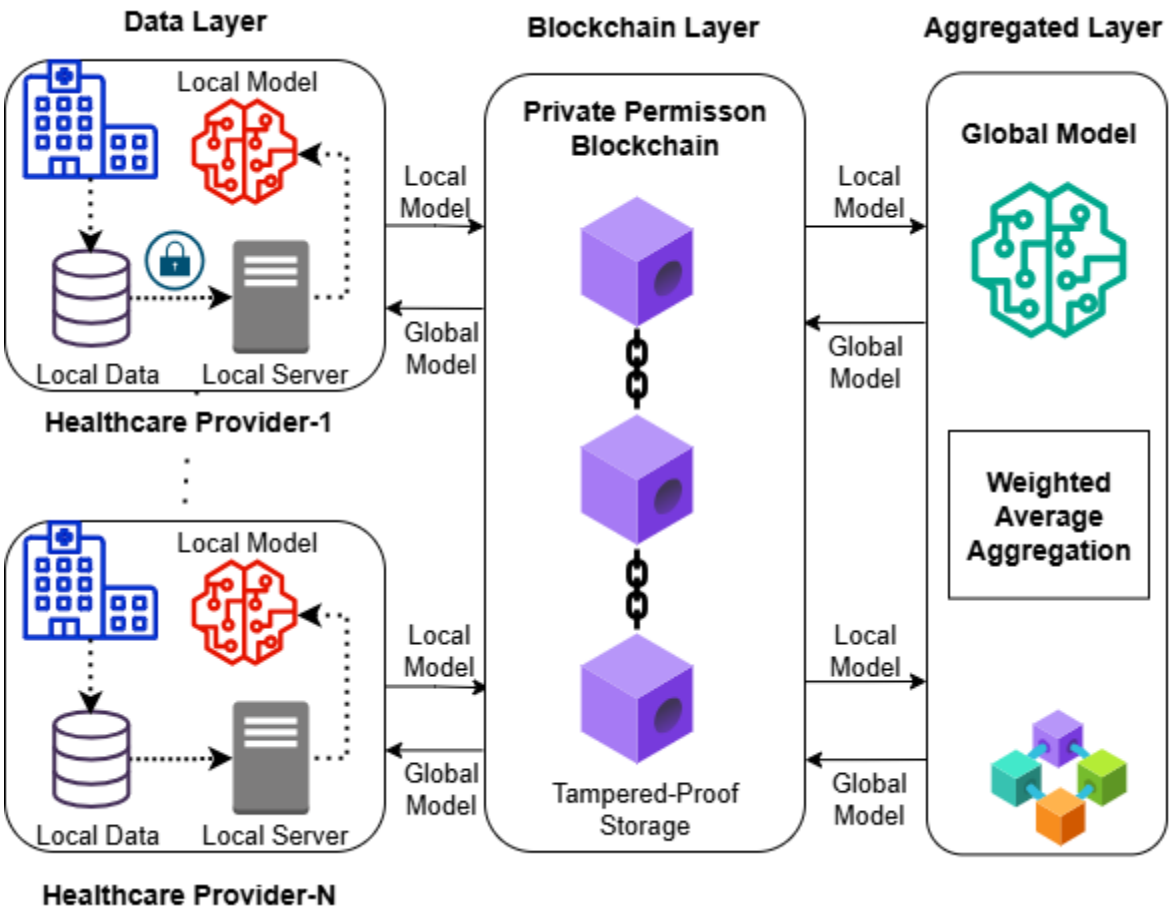

Fig 2. Proposed Framework

Algorithm-1 FLPPBC
Input: N healthcare providers, D_i local dataset
Output: Global Model $\mathcal{MG}$ and Blockchain Ledger BC_{led}
Step01: Initialize global model parameters ($\mathcal{MG}_{param}$), blockchain network (BC)
Step02: For each healthcare provider's HP_i
Step03: Collect local dataset D_i
Step04: Use homomorphic encryption
Step05: Encrypt the dataset D_i using Eq. (3)
Step06: Apply local model training using Eq. (8)
Step07: EndFor
Step08: For each healthcare provider's HP_i
Step09: Create a blockchain transaction with ID, hash of model, timestamp
Step10: Add blockchain transaction to BC_{led}
Step11: EndFor
Step12: Aggregate the global model using Eq. (10)

Key generation: Each healthcare provider generates a public-private key pair.

$$Key \rightarrow (Pub_k, Pri_k) \tag{2}$$

Encryption: The medical data is encrypted with the public key.

$$c_i = E_{pub_k}(m_i) \tag{3}$$

$$\text{Where} \quad E_{pub_k}(w) = \left(\prod_{i=1}^{n} E_{pub_k}(w_i)^{x_i}\right) \ mod\ N^2 \tag{4}$$

$where\ E_{pub_k}$ indicates a homomorphic encryption function, w represents model weight, x_i indicates input data, and N denotes a large number, m_i indicates plaintext, and c_i indicates ciphertext.

The additive homomorphic encryption function can be expressed as:

$$C_{sum} = c_1 \oplus c_2 \oplus \cdots \bigoplus c_n = E_{pub_k}(m_1 + m_2 + \ldots + m_n) \tag{5}$$

The multiplicative homomorphic encryption function can be expressed as:

$$C_{mul} = c_1 \otimes c_2 \otimes \cdots \otimes c_n = E_{pub_k}(m_1 \times m_2 \times \ldots \times m_n) \tag{6}$$

Decryption: The decryption is performed by

$$m_r = D_{pri_{key}}(c_r) \tag{7}$$

After data encryption, the next step is local model training. At each timestamp (ts), every healthcare provider's hp_i downloads the global model $\mathcal{M}G^{ts}$, and conducts local training with their dataset D_i. The computation of local training models is conducted as follows:

$$\mathcal{M}\_local_{hp}^{ts} = Train\left(D_{hp}, \mathcal{M}G_{param}\right) \tag{8}$$

Where D_{hp} represents data stored in hp, $\mathcal{M}G_{param}$ indicates the global model parameters.

The local model is encrypted using homomorphic encryption and stored in Blockchain.

Example of medical data encryption using homomorphic encryption

Attributes	age, sex, cp, trestbps, chol, fbs, restecg, thalach, exang, oldpeak, slope, ca, thal, target
Original Data	48,0,2,130,275,0,1,139,0,0.2,2,0,2,1
Encrypted Data	146675753781346064, 729283264272918238, 64452542198404465, 253241884463168049, 832136224255998128, 100902528654247573, 568734322230186944, 750753361934210572, 776451174162140315, 274661794246417822, 624210701630114532, 809425664291051206, 812952118871780731, 224463302616907024

2.2 Blockchain PoA and SHA-256

This layer provides safe and immutable storage for each healthcare provider. The blockchain creates a chain of transactions with timestamps, and each block stores encrypted patient data and local models, which provide immutability and data integrity. To guarantee accurate patient identification within the system, each block consists of patient information, which includes the patient identifier and the hash value of the patient identity. Smart contracts on the BC describe the rules and permissions for data access and distribution. To create a decentralized and unchangeable record of the model, this work uses the Proof-of-Authority (PoA) consensus mechanism.

PoA is a reputation-based consensus mechanism that is an effective method for protecting sensitive information. It selects set of trusted nodes (N) called authorities. Each authority has a unique ID, and at least half of them are honest. The authorities conduct a consensus to organize the transactions submitted by clients. The foundation of PoA is the mining rotation scheme, which is a common way for distributing the blocks across authorities.

Based on the identity and reputation, PoA selects a group of trusted authorities to validate the transactions. Their unreliability and overall commitment to the network are the main factors in their selection. The PoA is accountable because the identities of the validators are usually public and easily verifiable. Validators have a strong incentive to maintain and enhance the network integrity. PoA enhances the transaction throughput, latency, and energy efficiency because it requires only minimal

computation, and it relies on a limited collection of validators to reach consensus. It safeguards members' privacy and makes it easy to maintain blockchain. It reduces the concurrent execution of a larger volume of transaction. PoA needs minimal computation, delay, and energy compared to alternative methods. It can be a game-changing method for private blockchain networks. This layer uses the SHA-256 cryptographic algorithm to generate a 256-bit hash from any input data. Depending on the encryption technique, the length of the encrypted data may remain the same size or change somewhat. Conversely, hashing transforms data into an output of fixed length. In contrast to encryption, deducing the original content from its hash value is challenging due to the one-way nature of hashing. A brute-force attack would require 2^{256} attempts to replicate the original data. Moreover, there is a low likelihood of a collision, where two distinct inputs yield the same hash value.

Blockchain technology utilizes SHA-256 to generate a unique hash value for every data unit. The hash function takes inputs and generates fixed-length outputs H(x),

$$H(x) = SHA-256(x) \tag{9}$$

where x denotes the block data, which includes index, timestamp, content, and the preceding block hash value.

2.3 Global Model Generation

The local models learn from the unique patterns and trends of each healthcare provider's dataset. A global model is created by summarizing and combining local models from various healthcare providers. It incorporates the collective knowledge of all contributors. This kind of aggregation ensures that the global model incorporates the patterns and insights found in many local datasets. In order to create a global model, the aggregation phase involves consolidating the parameters of separate local models.

The following equation is used to compute the aggregated global model at timestamp ts+1,

$$\mathcal{M}G^{ts+1} = \sum_{i=1}^{HP} \frac{|D_i|}{\sum_{j=1}^{HP} |D_j|} \times \mathcal{M}\_local_i^{ts} \tag{10}$$

Where $|D_i|$ represents the number of data in i^{th} HP.

The weighted federated averaging is intended to train a collective global model among several decentralized entities without the need for raw data. In this methodology, each provider trains the model locally on its own dataset and transmits the updated model parameters to an aggregation layer. The aggregated layer computes a weighted average of these updates, with each provider's contribution adjusted according to the magnitude of its local dataset. This guarantees that providers possessing more data exert a proportionately bigger impact on the global model, enhancing convergence and performance. Weighted federated average optimizes efficiency, privacy, and model quality in distributed settings.

Upon completion of the aggregation, the global model was updated, which safeguards the confidentiality of local data of each healthcare provider because it processes only encrypted information. The global model was used by each healthcare provider and evaluated using a gradient boosting algorithm for classifying healthcare data stored in a local server. The updated global model parameters are subsequently stored in the data layer for future reference.

Overall, each healthcare provider in the data layer collects local data and trains a local model using gradient boosting. The local data and local model were encrypted by homomorphic encryption and sent to Blockchain layer. The block layer employs SHA-256 and PoA consensus mechanism for providing security and integrity of the model. The aggregated layer collects encrypted local mode parameters and utilizes average weighted aggregation to generate the global model. Without sharing their data, a global model was obtained by an aggregation layer and evaluated the health data to predict the classification performance. Each layer maintains local servers to store its corresponding data, model, parameter, hash value, and performance.

3 Results and Discussion

This section presents the performance assessment of the proposed FLPPBC methodology. The performance analysis includes the model and blockchain performance. The metrics accuracy, precision, recall, f-measure, latency and throughput are used to analyze the performance of the FLPPBC approach.

3.1 Model Performance

To analyze the model performance, this work utilizes two real-time healthcare datasets (heart disease[24] and breast cancer[25]) that were obtained from the UCI repository. The Gradient Boosting model was utilized for performing the classification tasks

on the healthcare datasets. It effectively improves predictive accuracy by sequentially combining multiple weak learners to form a strong, optimized model. The FLPPBC approach is compared with other methods, such as PPFBXAIO[21], FedHFP[26], and Defedhdp[27] based on the following performance metrics.

Accuracy: It is described as the proportion of correctly predicted results to all forecasts. It can be computed as,

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{11}$$

Precision: It is the proportion of genuine positives to false positives. It highlights how reliably the model labels events as positive.

$$Precision = \frac{TP}{TP+FP} \tag{12}$$

Recall: The proportion of true positive forecasts is calculated by dividing the number of true positives by the sum of false negatives and true positives. This statistic demonstrates the efficacy of a model in recognizing genuine positive situations.

$$Recall = \frac{TP}{TP+FN} \tag{13}$$

F-Measure: It integrates accuracy and recall into a singular metric, offering a comprehensive evaluation of the model. It is especially beneficial when class distributions are imbalanced, and it is crucial to equilibrate false positives, and false negatives.

$$F-Measure = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{14}$$

The datasets Heart disease[24] and Breast cancer[25] are divided into an equal number of subsets based on the number of healthcare providers. Each provider generates a local training model and sends it to Blockchain layer. The global model was generated using weighted average aggregation. The performance of the global model for different numbers of health providers was evaluated using different metrics. In this work, the number of healthcare providers ranges from 2 to 10. Each provider divides the dataset into 80% for training and 20% for testing. Gradient Boosting model was used to test the testing data. The average accuracy of the proposed approach was 98.90% for heart disease and 98.25% for the Breast cancer dataset.

Table 2 presents a comparison of different privacy-preserving frameworks according to distinct evaluation parameters.

Table 2. Evaluation Metrics Comparison

Dataset	Method	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
Heart Disease	PPFBXAIO[21]	93.07	91.19	95.39	93.24
	FedHFP[26]	86.79	86.25	90.60	87.09
	Defedhdp[27]	88.78	88.68	92.0	89.03
	FLPPBC	**98.90**	**98.92**	**98.90**	**98.89**
Breast Cancer	PPFBXAIO[21]	95.07	95.44	96.54	95.98
	FedHFP[26]	87.17	88.60	90.41	89.49
	Defedhdp[27]	89.28	89.77	92.66	91.20
	FLPPBC	**98.25**	**98.30**	**98.25**	**98.24**

Figure 3 illustrates the accuracy comparison of PPFBXAIO[21], FedHFP[26], DeFedHDP[27], and the proposed methodology. The suggested approach achieves an accuracy of 98.90% for heart disease and 98.25% for breast cancer. For the heart disease dataset, the proposed approach increases accuracy by 6.26% for PPFBXAIO[21], 13.95% for FedHFP[26], and 11.39% for Defedhdp[27] approach. Similarly, the breast cancer dataset also increases the accuracy of the proposed approach by 3.34% for PPFBXAIO[21], 12.71% for FedHFP[26], and 10.05% for Defedhdp[27] approach.

3.2 Blockchain System Performance

This section provides the blockchain performance using latency and throughput. In the blockchain context, latency refers to the duration required to append a new block to the Blockchain, whereas throughput quantifies the volume of transactions executed during a specified timeframe. The FLPPBC method has high throughput and low latency. It handles a large number

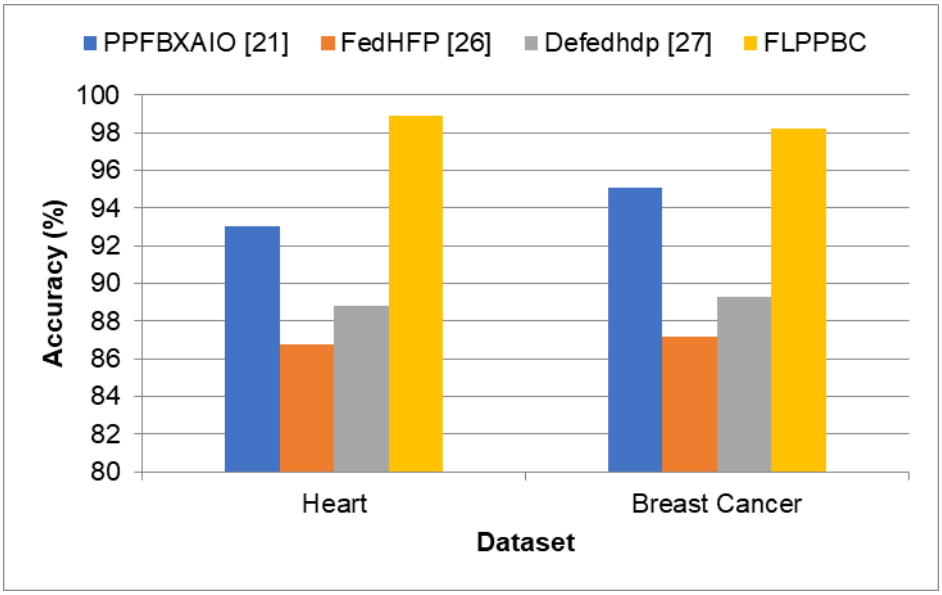

Fig 3. Accuracy Comparison

Table 3. Latency and Throughput Comparison

Method	Latency (ms)	Throughput (Trans/sec)
EPP-BCFL [17]	50	100
BCFLH [20]	43.52	116
PPFBXAIO [21]	81	109
FLPPBC	**39.27**	**125**

of transactions with ease and adds a block to the BC quickly, which reduces latency. The proposed FLPPBC approach was compared with EPP-BCFL [17], BCFLH [20], and PPFBXAIO [21]. Table 3 shows the comparison of latency and throughput.

Figure 4 shows the latency comparison of different methods. The proposed FLPPBC has less latency compared to other methods. The proposed FLPPBC approach reduces latency by 21.46%, 9.76%, and 51.52% for the EPP-BCFL [17], BCFLH [20], and PPFBXAIO [21] approaches.

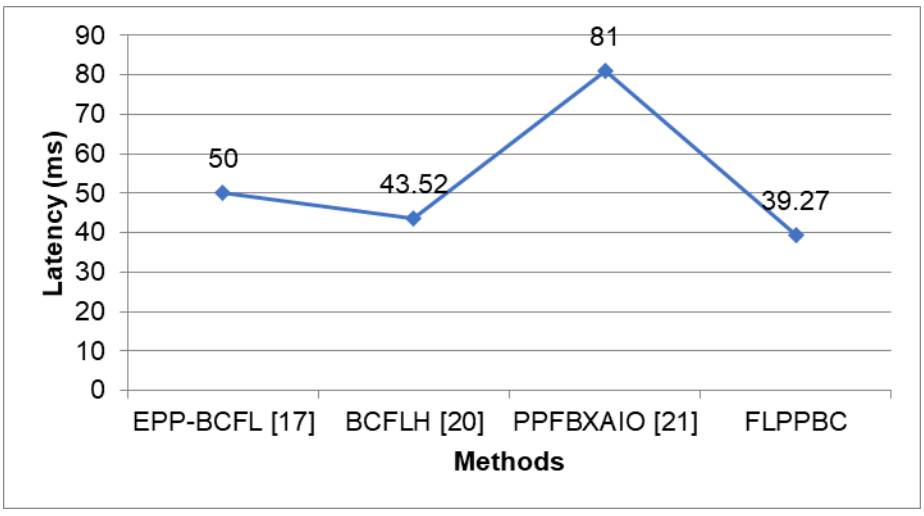

Fig 4. Latency Comparison

The proposed FLPPBC has a high throughput compared to other methods. The proposed FLPPBC approach increases throughput by 25%, 7.75% and 14.68% for EPP-BCFL[17], BCFLH[20], and PPFBXAIO[21] approaches.

3.3 Discussion

The suggested FLPPBC method is evaluated against PPFBXAIO[21], FedHFP[26], and Defedhdp[27] using accuracy, precision, recall, and f-measure as metrics for assessing prediction systems. These algorithms are applied to a publicly accessible dataset of patients with heart disease and breast cancer, comprising various variables related to their health. For classification, the existing approaches PPFBXAIO[21] and Defedhdp[27] used Entropy Deep Belief Network (EDBN), FedHFP[26] utilized Long Short-Term Memory (LSTM), and the proposed FLPPBC employed Gradient Boosting.

The FLPPBC method achieves more than 98% accuracy for health data compared to other methods. The performance accuracy is contingent upon the classification algorithm employed. The gradient boosting algorithm is an ensemble learning method that has minimal computational cost, overfitting risk and excellent interpretability, and maximum accuracy. But the EDBN and LSTM, has high complexity and overfitting with time-consuming process, resulting in minimum accuracy.The high accuracy shows that the FLPPBC, which consists of local training, blockchain, and aggregation, works together to ensure the best training model and effective categorization.

The result of the latency and throughput is influenced by the participant count, type of blockchain (public, private, and consortium), size of block, and type of consensus (PoW, PoA, PoS). Due to the trustworthiness of the nodes, a private permissioned blockchain using PoA consensus can outperform other blockchain types and consensus mechanisms in terms of throughput and minimal latency. The results showed a latency of 39.27 ms, which is the average time between consecutive block addition. Compared to other methods, the proposed FLPPBC has minimum latency, which means it efficiently processes the new blocks and adds them to blockchain. PoA consensus worked well, and the imposed security precautions did not significantly restrict performance.

This method is strong basis, along with its tremendous accuracy, throughput, and low latency which makes it scalable among health providers. This demonstrates that the method maintains its performance when the number of healthcare providers or dataset augments. The recommended federated learning using blockchain reduces the need for a centralized, reliable machine. The calculation is distributed among local clients, there by requiring reduced computational power and optimizing the utilization of available resources. This optimization can result in significant cost reductions in practical implementation.

4 Conclusion and Future Scope

The security and privacy are the most important problem in a healthcare system. To enhance the safety and reliability, this paper develops a layered secure model using federated learning and blockchain. The homomorphic encryption algorithm was used to provide the privacy-preserving patient data access. With the federated learning, privacy is not sacrificed when ML models are trained on decentralized data. To provide the safety of patient health information, FLPPBC employed homomorphic encryption, gradient boosting technique, SHA-256 and PoA consensus mechanism. The global model was generated by using weight average aggregation for patient data classification. The security and privacy are improved by integrating the FL, BC and homomorphic encryption. The healthcare data from the UCI repository was utilized to analyze the performance of the FLPPBC. The results indicate that the proposed FLPPBC approach improves the performance in terms of accuracy, latency, and throughput compared to other approaches. The integration of FL and BC generates a robust global model and securely protects data. The future research includes-

- To utilize an effective consensus mechanism to sustain minimal latency during processes involving big data.
- To safeguard patient anonymity, employ zero-knowledge proofs
- To establish resilient frameworks for authenticating various entities (patients, healthcare providers) and to implement attribute-based access control for information exchange.
- To implement ethical standards for data exchange, auditability, and patient privacy.

References

1) Issa W, Moustafa N, Turnbull B, Sohrabi N, Tari Z. Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Computing Surveys*. 2023;55(9):1–43. 10.1145/3560816.
2) Cui L, Li Y, Zhou Y, Qu Y, Liu J. Accelerating Blockchain-Enabled Federated Learning with Clustered Clients. *IEEE Transactions on Big Data*. 2024;11(5):2148–2161. 10.1109/TBDATA.2024.3403390.

3) Hai T, Zhou J, Srividhya SR, Jain SK, Young P, Agrawal S. BVFLEMR: An integrated federated learning and blockchain technology for cloud-based medical records recommendation system. *Journal of Cloud Computing*. 2022;11(1). 10.1186/s13677-022-00294-6.
4) Fereidooni H, Marchal S, Miettinen M, Mirhoseini A, Möllering H, Nguyen TD, et al. SAFELearn: Secure aggregation for private federated learning. IEEE. 2021. 10.1109/SPW53761.2021.00017.
5) Onireti MY, Shukla RM, Das T. Splitting smarter: Differential privacy for secure healthcare federated learning. *Scientific Reports*. 2025;15(1). 10.1038/s41598-025-27472-1.
6) Singh JP, Aqsa A, Ghani I, Sonani R, Govindarajan V. Privacy-Aware Hierarchical Federated Learning in Healthcare: Integrating Differential Privacy and Secure Multi-Party Computation. *Future Internet*. 2025;17(8). 10.3390/fi17080345.
7) Alshudukhi KSS, Ashfaq F, Jhanjhi NZ, Humayun M. Blockchain-enabled federated learning for longitudinal emergency care. *IEEE Access*. 2024;12:137284–137294. 10.1109/ACCESS.2024.3449550.
8) Cheng R, Sun Y, Liu Y, Xia L, Feng D, Imran MA. Blockchain-empowered federated learning approach for an intelligent and reliable D2D caching scheme. *IEEE Internet of Things Journal*. 2021;9(11):7879–7890. 10.1109/JIOT.2021.3103107.
9) Jin R, Hu J, Min G, Mills J. Lightweight blockchain-empowered secure and efficient federated edge learning. *IEEE Transactions on Computers*. 2023;72(11):3314–3325. 10.1109/TC.2023.3293731.
10) Kushwaha SS, Joshi S, Singh D, Kaur M, Lee HN. Systematic review of security vulnerabilities in ethereum blockchain smart contract. *IEEE Access*. 2022;10:6605–6621. 10.1109/ACCESS.2021.3140091.
11) Ullah I, Deng X, Pei X, Jiang P, Mushtaq H. A verifiable and privacy-preserving blockchain-based federated learning approach. *Peer-to-Peer Networking and Applications*. 2023;16(5):2256–2270. 10.1007/s12083-023-01531-8.
12) Stephanie V, Khalil I, Atiquzzaman M, Yi X. Trustworthy privacy-preserving hierarchical ensemble and federated learning in healthcare 4.0 with blockchain. *IEEE Transactions on Industrial Informatics*. 2023;19(7):7936–7945. 10.1109/TII.2022.3214998.
13) Moulahi W, Jdey I, Moulahi T, Alawida M, Alabdulatif A. A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. *Computers in Biology and Medicine*. 2023;167. 10.1016/j.compbiomed.2023.107630.
14) Ruvunangiza J, Valderrama C. A Unified Framework for Secure Healthcare Data Sharing: Integrating Federated Learning, Blockchain, and Quantum Cryptography. *Journal of Biomedical Research and Environmental Sciences*. 2024;5(9):1081–1088. 10.37871/jbres1993.
15) Alsamhi SH, Myrzashova R, Hawbani A, Kumar S, Srivastava S, Zhao L, et al. Federated learning meets blockchain in decentralized data sharing: Healthcare use case. *IEEE Internet of Things Journal*. 2024;11(11):19602–19615. 10.1109/JIOT.2024.3367249.
16) Commey D, Hounsinou S, Crosby GV. Securing health data on the blockchain: A differential privacy and federated learning framework. *arXiv preprint*. 2024;2405.11580. 10.48550/arXiv.2405.11580.
17) Munusamy S, Jothi KR. Blockchain-enabled federated learning with edge analytics for secure and efficient electronic health records management. *Scientific Reports*. 2025;15(1):1–20. 10.1038/s41598-025-12225-x.
18) Khan S, Khan M, Khan MA, Wang L, Wu K. Advancing medical innovation through blockchain-secured federated learning for smart health. *IEEE Journal of Biomedical and Health Informatics*. 2025;29(9):6482–6495. 10.1109/JBHI.2025.3532976.
19) Prashanth K, Kumar KP. Secure Federated Learning with Blockchain and SMPC: Protecting Healthcare Systems from Poisoning attacks. *International Journal of Engineering Research and Science & Technology*. 2025;21(2):1032–1042. 10.62643/ijerst.2025.v21.i2.pp1032-1042.
20) Myrzashova R, Alsamhi SH, Hawbani A, Curry E, Guizani M, Wei X. Safeguarding patient data-sharing: Blockchain-enabled federated learning in medical diagnostics. *IEEE Transactions on Sustainable Computing*. 2024;10(1):176–189. 10.1109/TSUSC.2024.3409329.
21) Bhardwaj T, Sumangali K. An explainable federated blockchain framework with privacy-preserving AI optimization for securing healthcare data. *Scientific Reports*. 2025;15(1). 10.1038/s41598-025-04083-4.
22) Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (CSUR)*. 2018;51(4):1–35. 10.1145/3214303.
23) Serengil SI, Ozpinar A. LightPHE: Integrating Partially Homomorphic Encryption into Python with Extensive Cloud Environment Evaluations. *arXiv preprint*. 2024;2408.05219. 10.48550/arXiv.2408.05219.
24) UCI Heart Disease Dataset. *UCI Machine Learning Repository*. Available from: https://archive.ics.uci.edu/dataset/45/heart+disease.
25) UCI Breast Cancer Wisconsin Diagnostic Dataset. *UCI Machine Learning Repository*. Available from: https://archive.ics.uci.edu/dataset/17/breast+cancer+wisconsin+diagnostic.
26) Lohachab A, Kumar K. FedHFP: a federated deep learning framework for heart failure prediction. *IETE Journal of Research*. 2025;71(2):479–491. 10.1080/03772063.2024.2428741.
27) Wei M, Yang J, Zhao Z, Zhang X, Li J, Deng Z. Defedhdp: Fully decentralized online federated learning for heart disease prediction in computational health systems. *IEEE Transactions on Computational Social Systems*. 2024;11(5):6854–6867. 10.1109/TCSS.2024.3406528.