International Journal of Multidisciplinary Sciences and Technology
ISSN: XXXX-XXXX | Volume 1 Issue 1, 18-28, July-September 2025
DOI: https://doi.org/10.64137/XXXXXXXX/IJMST-V1I1P103

Received: 05/08/2025 Revised: 11/08/2025 Accepted: 24/08/2025 Published: 12/09/2025

Original Article

Design and Implementation of a Blockchain-Assisted Federated Learning Framework for Privacy-Preserving Healthcare Data Analytics

NISSI JOY
Data Analyst, Conflowence, USA.

ABSTRACT: *The use of both federated learning and blockchain ensures better privacy for healthcare data analysis. Traditional approaches to machine learning in healthcare are affected by risks related to data breaches, data privacy, and having data from several sources that may be biased. In federated learning, several medical institutions join forces in training data without giving away patients' private details. Even so, there are problems that FL has to face, such as hidden practices, the possibility of bad quality in training, and the struggle to ensure trust and justice for all participants. Because of these obstacles, a blockchain-enabled federated learning platform for healthcare analytics is presented in this paper. The use of blockchain allows the framework to guarantee clear, unchanged, and trackable model updates, along with effective administration of members and encouragement for honest teamwork among them. The architecture design involves incorporating bias-reduction measures in the FL process, relying on blockchain to gather and study models, encourage fairness, and identify any dishonest or malicious parties. Simulated healthcare settings have proven that the framework increases the precision and fairness of models and significantly cuts down the chances of private information being leaked by putting parameters under decentralized control. Because the system resists single issues of failure, meets different needs, and is scalable, healthcare analytics benefit from it, and this helps improve fairness and quality of healthcare. Advanced ways of motivating users and using new technologies, such as edge computing, could be added in the future to protect privacy and enhance performance.*

KEYWORDS: *Blockchain, Federated learning, Privacy-preserving, Healthcare analytics, Bias mitigation, Fairness, Distributed architecture, Medical data, Transparency, Security*

1. INTRODUCTION

1.1. THE NEED FOR PRIVACY-PRESERVING HEALTHCARE ANALYTICS

The digital transformation of healthcare has caused patient data to accumulate at an unprecedented pace, which includes EHRs, medical images, and outputs from wearable devices. [1-3] All this information can greatly boost our ability to predict diseases, use tailored treatments, and keep track of public health using data science and AI. Using such information brings big challenges when it comes to privacy and security. Since HIPAA and GDPR impose strong regulations, and more people are concerned about confidentiality, healthcare organizations have a hard time sharing their data for machine learning. Traditional systems usually experience challenges because of fragmented data, limited sharing, and increased risks of data breaches.

1.2. FEDERATED LEARNING: OPPORTUNITIES AND LIMITATIONS

Federated learning (FL) is now viewed as a good way to deal with these problems. Training machine learning models jointly with multiple healthcare organizations does not require them to share their raw data, thus protecting confidentiality and following regulations. Models are trained using each institution's data, and no information about the training is shared until the parameters are sent to a server. Federated learning has benefits, but it still has its own drawbacks. The main server is at risk of breaking down and being dishonest, and the process might experience malicious intervention, wrongly influenced models, and unequal contributions. Moreover, when information about the updates and the process of aggregating models is not open, entities may find it difficult to trust the process.

1.3. BLOCKCHAIN-ASSISTED FEDERATED LEARNING: A NOVEL FRAMEWORK

Resolving these issues becomes possible by joining blockchain technology with federated learning. All updates and transactions in the model are clearly recorded and checkable by all members of the network because of the decentralized and unchangeable nature of blockchain. By automating the process and making rules official, smart contracts guarantee both safety and fairness for participants. A federated learning model supported by blockchain makes it possible for medical institutions to cooperate with each other safely, transparently, and with proper auditing. By doing this, privacy risks and possible single causes of failure are considerably reduced, which helps create trust, makes people accountable, and supports equal participation. By making use of federated learning and blockchain in the architecture, the proposed framework intends to greatly improve privacy-friendly healthcare data analysis, contributing to accurate, fair, and safe medical discoveries.

2. RELATED WORK

2.1. FEDERATED LEARNING IN HEALTHCARE

Federated learning is now being used in healthcare data analytics to meet the important need for collaborative and private machine learning among various medical organizations. [4-7] FL allows healthcare organizations to work together on similar models by keeping sensitive patient data protected at each organization instead of gathering the data in one place. In the healthcare sector, this approach has become vital since laws like HIPAA and GDPR prevent patient information from being freely exchanged.

An extensive study looking at FL in healthcare demonstrates how rapidly it has become popular, being practiced in radiology, oncology, urology, and other fields. FL is most used in neural networks and medical imaging, though it has also been used for EHRs, supporting diagnoses, and monitoring people's health. Many clinicians and researchers have adopted FL because the framework works with different data types and various machine learning tools. Projects such as HealthChain in France and FeTS let us see how large-scale shared efforts between institutions can boost both the usability and precision of AI models.

Even though FL is promising, it has several obstacles in healthcare. These difficulties in conveyance involve creating reliable ways to update the model, working with different kinds of datasets, and stopping threats such as model poisoning. Issues with overseeing regulation, managing inventorship, and guaranteeing intellectual property rights are mostly not solved in the present implementations. Even so, the use of FL is growing as an important way to support precision medicine, by ensuring fair, large-scale, and private analytics for the advancement of healthcare.

2.2. BLOCKCHAIN APPLICATIONS IN DATA SECURITY

Blockchain made a difference in data security by creating a system that is transparent, easy to follow, and safe to alter. Blockchain is able to address serious issues with data integrity, manage access to information, and ensure medical information is safely shared in healthcare. Blockchains spread data across multiple nodes and use different consensus methods to make sure there is no single point of weakness and to lower the chances of unauthorized changes.

Blockchain in healthcare covers various areas, like handling digital health records, checking the accuracy of trial data, and getting patient permission. With this technology, both patients and providers can officially track and log any adjustments or access to their data, helping to create trust and responsibility everywhere within healthcare. Smart contracts make the system more secure by automating the sharing of data in line with policies and denying access to people who are not authorized.

When blockchain is linked with federated learning, it increases the positive aspects of both technologies. Blockchain makes sure federated learning is secure, as it keeps track of model changes and the efforts of each participant in a fixed record. Therefore, all activities on the network can be reliably checked, making it difficult for someone to change the models or to deceive by reporting results. Also, smart contracts and other incentives promoted by blockchains can lead to sincere cooperation and good distribution of resources among collaborative firms. As digital and distributed technologies are adopted in healthcare, blockchain proves to be a main tool for protecting sensitive data, improving how different systems exchange information, and making analytics more reliable and private.

2.3. PRIVACY-PRESERVING MACHINE LEARNING

PPML includes various approaches meant to keep sensitive data safe during both the training and use of machine learning models. PPML serves to uphold privacy and rules in healthcare and keep the public trust, since patient data must be confidential in this sector. Differential privacy, homomorphic encryption, secure multi-party computation, and federated learning are common techniques used now.

Differential privacy adds random numbers to model outputs or gradients to cut down the chances of identifying individuals from the group data. This type of encryption enables analysis to happen on encrypted information so that private details are never revealed. Secure multi-party computation makes it possible for several parties to work together on a function computation, while keeping their inputs hidden. The way federated learning works helps preserve privacy because it never transfers the data and only shares updated models.

Using these privacy measures is especially necessary in healthcare because the risks connected to leaked data are much greater. PPML allows various institutions to analyze and create new models that do not reveal patient information, boosting efforts in both disease prediction, treatment improvement, and population health management. But, applying PPML on a large scale brings difficulties related to increased computational load, efficient information sharing, and ensuring privacy does not limit how useful the model is. Experts keep exploring how to find the best balance between these factors and build systems using a combination of privacy-focused methods, such as blockchain-based operations in federated learning, for effective healthcare data analytics.

3. SYSTEM ARCHITECTURE AND DESIGN

A security framework that makes use of blockchain and federated learning to analyze healthcare data securely and together. [8-12] The process consists of three important parts: training a local model, safeguarding gradients, and collecting and averaging gradients with blockchain. Using this sequence, medical information stays safe and secure on each node but can also take part in worldwide information exchange.

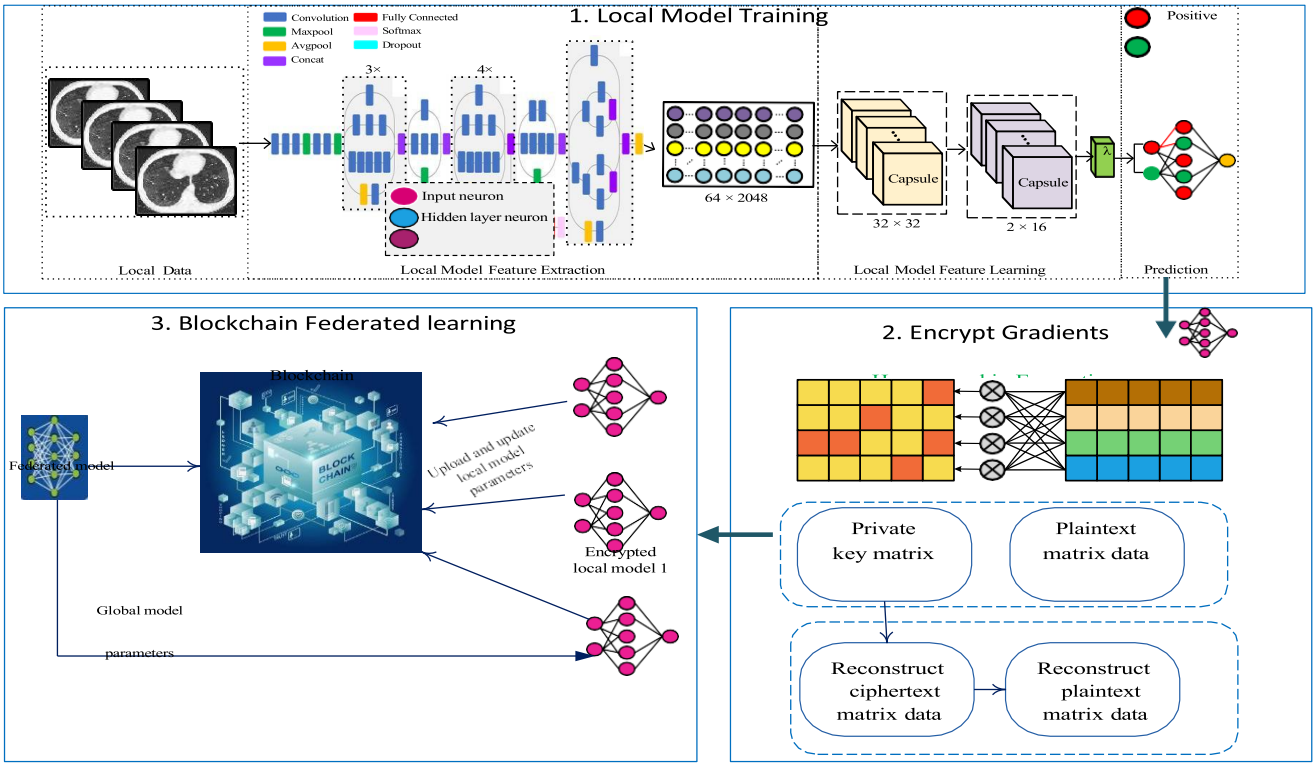

FIGURE 1 Overview of blockchain-assisted federated learning framework

Each medical center or device trains its own deep neural network model using patient data like CT scans, different blood markers, or pictures of vital signs. Convolutional and dense layers are used in training, and afterwards, the output is used for classification. Information from the environment remains there, and only the gradients of the model are allowed to be shared after training. It is necessary to make sure this component follows privacy rules such as HIPAA and GDPR. In the second stage, an important step is added with gradient encryption. Homomorphic encryption or matrix-based private key encoding is one of the main approaches for data masking of the parameters before any transfer. The picture demonstrates how key matrices turn ordinary gradient data into a protected version.

Ensuring information security, it stops any data leakage or unauthorized control attempts during either the storing or the transferring process, even if there is a security issue with the channel or the node handling the data. After that, encrypted changes to the model are sent through a blockchain network to guarantee secure aggregation and open collaboration. Every local node uploads its encrypted information to the blockchain, and a set of rules checks and connects those details with the global model. The blockchain provides legitimate trust throughout the network, so anything can be checked, and major failures are avoided. When the global model is updated, it is sent to all locations for further training, finishing the federated learning process.

3.1. COMPONENTS AND LAYERS

3.1.1. DATA OWNERS (HOSPITALS, DEVICES)

The data owners play the main role in forming a blockchain-based FL system for healthcare. Hospitals, clinics, research organizations, and an increase in IoMT gadgets like wearable devices and home monitoring are all part of these entities. Those who handle patients' data make sure it is always kept safe by not transferring the original data from their server. Instead of sharing their data, they adjust machine learning models by using their own data locally, which allows them to pass on updates to the models that hold their knowledge within them. Using this approach not only saves patient privacy but also allows doctors to benefit from the diversity of medical data that would be hard to collect in one place. It is the duty of data owners to ensure accuracy and preprocess their data, and make certain that their computational tools fulfill the network's requirements. When IoMT devices are integrated into healthcare systems, edge nodes play a larger role in collecting and processing data in

real time. Such data processing extends analytics to a wide variety of situations, allowing for continual and aware monitoring of patients' health.

3.1.2. FEDERATED LEARNING SERVER

The federated learning server leads the process of training models together with other devices. The main purpose is to arrange for the model to be trained by giving the model to every data owner and merging their newly calculated updates. Usually, the server governs everything in traditional FL, but in blockchain versions, the server functions can be managed by various nodes to reduce the risk and provide more trust. The server makes sure everyone's information is updated properly, guides the training steps, and can use approaches like differential privacy or secure multi-party computation to better keep private information secure during updates. Furthermore, it takes care of registering users, verifying them, and giving access to the needed resources only to approved entities taking part. When blockchain technology is used, the server's processes can be audited, as all modification transactions are added to the permanent ledger. Doing this helps organizations keep track of every action and contribution, and this is very important for meeting regulations and combining efforts in multi-institutional healthcare.

3.1.3. BLOCKCHAIN NETWORK (SMART CONTRACTS, LEDGER NODES)

Federated learning is secured, transparent, and accurate because of the blockchain network supporting it. The system stores all updates, activities by participants, and events of the system in decentralized distributed ledger nodes. Smart contracts help automate important operations such as combining many financial models, verifying each participant, distributing incentives, and ensuring models are shared. The blockchain removes the need for humans to monitor the system, which makes the entire network secure from various dangers. Every node in the ledger system checks and saves each transaction independently to maintain consensus and stop anyone from making illegal changes. This architecture is very important in healthcare because it helps different institutions trust one another, as every action can be checked and is in line with the rules. Key management, access control, and keeping track of track provenance can be ensured by blockchain technologies.

3.1.4. AGGREGATOR AND MODEL VERIFIER

The aggregator and model verifier are important parts that combine local changes into a single model and make sure the learning process is correct. The aggregator takes encrypted updates provided by the data owners and calculates an average or another type of aggregation according to the needs of the application and fairness concerns. In blockchain-supported FL, the process of aggregating data is typically carried out by smart contracts that ensure all activities are both transparent and secure. At the same time, the model verifier thoroughly scans for unusual behaviors, unapproved updates, or poisoning attempts prior to allowing updates to be added to the global model. Some verification methods rely on cryptography, on statistical checks, or on comparing with reference collections of records. When the blockchain is used, it is easy for the verifier to track each change in the model and confirm participants' contributions. Federated learning can be trusted in healthcare with this approach because it prevents any mistakes, injustices, or vulnerabilities that could come from attackers.

3.1.5. Applications

The new hybrid quantum-classical network is designed to help with high-efficiency processing of signals in bioinformatics. The approach connects a variety of biological data with advanced neural networks and scientific simulation tools to ensure strong and adjusted bioinformatics analysis. Data is sourced, preprocessed, filtered through hybrid learning, simulated by quantum computers, and the results are given in ways suitable for the application. In the beginning, bioinformatics takes gene expression data, DNA/RNA sequence information, and proteomics from a secure database. Data is handed to a preprocessing layer where several modules work to remove noise and extract new information, so the data becomes suitable for the next stages of modeling. Subsequent to processing, the signals are delivered to both classical and quantum-related computational routes in the hybrid core. Hybrid cores have two separate computing methods.

Deep learning models, FNN, CNN, and RNN are part of the classical branch and are intended for tasks like prediction, learning patterns over time, and finding meaningful data features. At the same time, the quantum-inspired branch depends on quantum encoding and quantum operators to model the behavior and relationships of quantum neurons. The results from both computational paths are given to a fusion and output layer, where a fusion module blends traditional and quantum concepts. An anomaly detection engine draws attention to unusual events, predicts risk, and assists in making key decisions. The intelligence learnt by machine learning is used to help the app's modules locate signs of disease and advise personalized care. It reflects a blending of biology, classical artificial intelligence, and quantum computing, made for large-scale, secure, and understandable bioinformatics processing.

3.2. WORKFLOW AND DATA FLOW

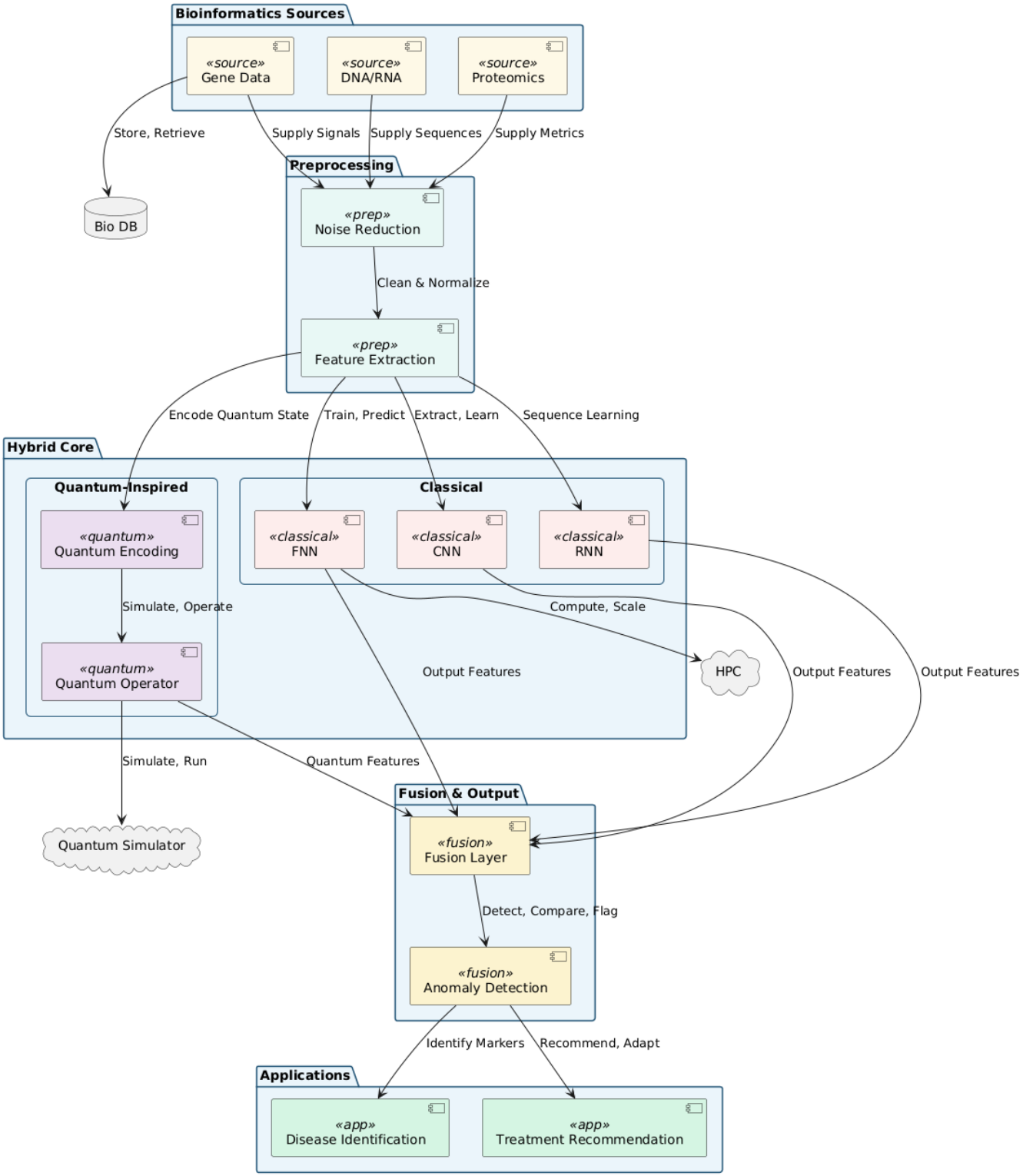

FIGURE 2 Architecture of a hybrid quantum-inspired neural framework for signal processing in bioinformatics

4. METHODOLOGY

4.1. FEDERATED LEARNING MODEL DESIGN

4.1.1. MODEL SELECTION AND TRAINING PROCESS

The design of an FL model requires choosing a machine learning framework and architecture that is best suited for the healthcare task you wish to tackle. [13-16] Frameworks like PyTorch and TensorFlow offer full support for federated learning, and extra libraries such as PySyft and Flower come with important functions for distributed model training and communication. Whether to use a neural network, a decision tree, or a recurrent model depends on what area is being looked

at, the structure of the data, and the expertise found at each institution. Each data owner (hospital or device) prepares the chosen model using its own patient records, so private data is always protected within the institution. Usually, local training runs through multiple epochs after which the computed updates (such as gradients or weights) are transmitted safely to a main server or aggregator. Using an unstructured approach maintains privacy and combines the data from several sources, which improves and generalizes learning from healthcare data. It is important to handle different kinds of data, guarantee smooth communication between parties, and adopt privacy methods like differential privacy and secure multi-party computation to decrease the chances of leaking data.

4.1.2. UPDATE AGGREGATION STRATEGY

Federated learning relies heavily on update aggregation, since it directly influences the accuracy, fairness, and safety of the shared model. FedAvg is used most often, with the central server adding up the local updates from all data owners and giving them appropriate weights. The weighting commonly depends on the amount of data in each local dataset, allowing big institutions to take part in developing the model in their own areas. Sophisticated methods of aggregation could handle data that is not IID, find outliers, and jump to be robust even when updates are hacked. Blockchain makes it possible to develop smart contracts for aggregation in FL, so the process remains clear and open for inspection. At this point, checks may be done to make sure updates are harmonious and meet fairness or privacy requirements before they are added to the global model. Applying aggregation can improve the model's performance and earn the trust of participants because the process is clear, can be checked, and can't be easily tampered with.

4.2. BLOCKCHAIN INTEGRATION

4.2.1. SMART CONTRACT DESIGN

Smart contracts are computer programs placed on the blockchain that run and enforce necessary steps in federated learning. Using smart contracts in healthcare FL, registration can be managed, models can be combined, and participants are given rewards as soon as their actions are confirmed. These rules guarantee that data access, data privacy, and updates follow standards so all actions stay open to review, uniform, and cannot be modified. Using smart contracts automates the described processes, eliminates a lot of paperwork, makes errors less likely, and offers solid support for relationships between multiple organizations working together. They can also address disputes because all transactions and decisions saved using smart contracts are permanent and can be checked by regulators.

4.2.2. CONSENSUS MECHANISM

The security of the federated learning system depends on the basic consensus mechanism used in its blockchain network. It makes sure that members of the network gather and agree on the correct order and authenticity of transactions, as well as any updates made to the model. Some of the more common consensus protocols are Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), each differing in how much they can manage, how much energy they use, and how resilient they are to malicious individuals. In healthcare FL, because latency and throughput are very important, most users choose lightweight consensus techniques such as PBFT or delegated PoS. With these protocols, decisions and smart contract actions are approved fast, and people can conduct many transactions without delays. Since the consensus process prevents one entity from making unilateral blockchain changes, it makes the federated learning ecosystem trustworthy and transparent.

4.2.3. TRANSACTION AND MODEL LOGGING

A blockchain version of transaction and model tracking ensures all activity in the federated learning system can be looked up and trusted. The distributed ledger records all events in the process: registration, updates, collecting results, and giving out prizes. Because of this detailed logging, anyone can look at how the global model was developed and what has happened in it since. In the healthcare field, where being accountable and following rules is necessary, blockchain logging helps trace the access, use, and decision-making behind every healthcare model. If needed, the use of blockchain can help analyze disputes or incidents since every action is permanently and openly recorded. Because transaction and model logging are included with both smart contracts and consensus mechanisms, the system becomes highly trustworthy, transparent, secure, and dependable, establishing a solid basis for confidential and trusted healthcare data analysis.

4.3. SECURITY AND PRIVACY TECHNIQUES

4.3.1. DATA ANONYMIZATION/ENCRYPTION

Most federated learning systems depend on anonymizing and encrypting data when working with sensitive topics, such as healthcare. Data anonymization disguises personal information in data so that no one can find out who individuals are, even if another person accesses the data without permission. The usual approach is to remove or mask information such as names and social security numbers, and also handle dates of birth or zip codes by making them general or adding random elements to them. Improving privacy by removing personal information may affect the value of the data if not well traded off with the data's use.

Encryption directly helps keep the information safe while using federated learning. In this case, the raw patient data stays where it is located, and what's shared are only model updates, for example, the gradients or weights. Encryption is used to offer more protection for the updates before they are sent. Homomorphic encryption makes it possible for the server or aggregator to combine updates without ever looking at the actual information. This means the sensitive data will be secured even if someone manages to access the messages. Secure Multi-Party Computation (SMPC) helps several parties to find a common answer, such as an aggregated model, without disclosing their own details to each other or to the central computer. Using blockchain, each update and the activity of aggregating models occur on a distributed ledger where they are publicly visible, unchangeable, and traceable. Using anonymization and encryption in federated learning allows healthcare partners to work more securely, follow privacy laws, and rely on each other.

4.3.2. DIFFERENTIAL PRIVACY OR HOMOMORPHIC ENCRYPTION

Differential privacy and homomorphic encryption ensure strong protection of data being shared in federated learning.

Differential privacy uses random noise to modify the data or model changes before they are released. As a result, having or leaving out any one person's data is unlikely to play a major role in the final result, which protects privacy. In federated learning, you can include random noise in your local model updates before sending them, meaning your privacy is still maintained even if the aggregator or others are attacked. Differential privacy is especially important when studies require analysis of massive health data because there is a serious threat of re-identification from the model's predictions.

Data encryption by means of homomorphic encryption makes it possible to compute numbers while keeping the encrypted information intact. As a result, models can be updated on each participant's device and distributed in the form of encrypted data to the central aggregator. The aggregator can operate on the encrypted updates and show the result as a decrypted value to only the authorized persons. With this technique, information is kept private at every step of the computation, so data exposure is not possible during the aggregation stage. In healthcare federated learning systems, you can choose to use differential privacy, homomorphic encryption, or both, based on what is needed in terms of security and performance. Incorporating them into federated learning helps offer reliable data confidentiality, satisfies laws and regulations, and promotes teamwork between sensitive data users.

5. IMPLEMENTATION DETAILS

5.1. DEVELOPMENT ENVIRONMENT

Engineers typically set up a blockchain-assisted federated learning framework in healthcare using powerful programming languages, IDEs, and libraries meant for distributed machine learning and blockchain tasks. Python is preferred mainly because it supports many tools, is simple to use, and is teamed with renowned libraries for machine learning and data science. The majority of projects choose Python 3.7 or above since these versions are dependable and contain the latest updates required for developing both federated learning and blockchain systems. PyCharm, Visual Studio Code, and Jupyter Notebook are some of the well-known IDEs used by developers, and they make prototyping, visualization, and teamwork easier than before.

Typically, the environment also has version control with Git to handle source code and Docker to easily reuse and scale projects running on various computers. Truffle, Hyperledger Fabric SDKs, and Ganache are some of the favourite development frameworks for setting up blockchain networks. Developers use these tools to make and review smart contracts and decentralized applications. Healthcare federated learning often involves processing a large amount of data; therefore, adding cloud-based resources or strong computing clusters to the existing setting may help enhance the development environment.

5.2. FRAMEWORKS AND TOOLS USED

Launching a federated learning system with blockchain support needs all three elements: machine learning, federated learning, and blockchain frameworks. Most people in the field use TensorFlow Federated, PySyft, and Flower libraries for federated learning. The frameworks let users organize distributed training, send information between nodes, and apply privacy-protecting methods. TensorFlow Federated makes it simple to add TensorFlow models to federated activities, and PySyft guarantees privacy by processing data with encryption and differential privacy.

Smart contracts and decentralized ledgers are mainly developed and managed on Ethereum and Hyperledger Fabric on the blockchain. Developers use Truffle Suite, Remix IDE, and Solidity (for Ethereum) or Hyperledger Composer and Chaincode (for Hyperledger Fabric) to develop, test, and launch smart contracts that take care of model aggregation, dealing with participants, and managing payments. REST APIs, web3 libraries, or custom middleware are usually used to help blockchain and federated learning systems exchange data securely. Monitoring, auditing, and visualization platforms, such as Grafana or Kibana, can be installed to supervise system performance and check blockchain transactions.

5.3. DATASETS AND PREPROCESSING

Data in blockchain-assisted federated learning for healthcare usually comes from various hospitals, clinics, or medical devices, showing how medical data is spread out and types in the real world. Data types found in healthcare include EHRs, medical

scans such as those from an MRI or CT, test results, and data obtained by wearable devices. Every institution keeps its own data and uses it only for building models on its premises.

Preprocessing makes sure that the data is high-quality, uniform, and works well at all locations. For this, it is important to clear duplicates, manage anything that is missing, normalize or standardize the data, transform categorical variables, and protect by removing personal data. Some imaging data require preprocessing using actions such as resizing, normalization, and data augmentation to boost the model's skills. Feature engineering and selection are implemented where data is collected to fit the data for each task. It is vital that the steps in preprocessing data be similar at each site to prevent the model from performing poorly or from becoming divided. Using partitioning techniques can make datasets like the aggregated one less IID, which helps verify how well the federated learning framework works.

5.4. DEPLOYMENT SETUP (E.G., SIMULATION, CLOUD, EDGE DEVICES)

A blockchain-based federated learning framework can be used in a wide range of environments based on factors such as size, security requirements, and the infrastructure that's available. A local cluster or virtual machines can often be used to recreate numerous data owners, database networks, and blockchain nodes at the beginning of the development phase. Studies in the simulation environment make it possible to create, identify errors, and measure how the system works before launching it for live use.

Services such as AWS, Google Cloud, and Microsoft Azure in the cloud are useful for deploying federated learning as well as blockchain servers and storage for large-scale uses. Cloud deployment makes it easy to allocate resources, ensure constant access to healthcare systems, and protect data, which are important for large health projects. More and more, smart healthcare systems are choosing edge deployment with IoMT devices and local servers, which makes it possible to receive real-time data, perform quick processing, and rapidly update models. Edge devices, in these situations, own the data, join federated learning events, and communicate using safe methods with central aggregators and blockchain networks.

Most organizations use hybrid setups that mix cloud computing and edge computers, which helps them regulate power, privacy, and the stability of their systems. Security of networks, encrypted communications, and constant monitoring are applied, no matter what, to maintain the integrity and confidentiality of federated learning and blockchain in the system.

6. EXPERIMENTAL EVALUATION

6.1. EVALUATION METRICS

In healthcare, it is necessary for evaluation in blockchain-assisted federated learning to look at both model performance and features like efficiency, privacy, and scalability. Major factors to watch are:

- **Accuracy**: The precision of the model is shown by looking at how it does when applied to new, unseen data, usually using terms like classification accuracy or mean squared error.
- **Latency**: Latency means how fast the system completes training, showing its overall reaction speed.
- **Communication Cost**: Describes the quantity of data traded between users and servers (or throughout the blockchain network), a factor that matters a lot in federated settings where bandwidth and energy are limited.
- **Privacy Leakage**: Refers to how much confidential data might be discovered based on shared information, and is often checked by running tests or using formal rules for privacy.
- **Blockchain Overhead**: Users experience extra delays and extra resource use due to blockchain processes such as consensus and logging transactions.

Metrics are checked using both main evaluation strategies and federated ones, allowing personalization and fairness to be checked on data owners' devices.

TABLE 1 Overall performance metrics of the proposed blockchain-assisted FL framework

Metric	Value (Example)
Accuracy (%)	91.2
Latency (s/round)	3.5
Communication Cost (MB/round)	5.2
Privacy Leakage (%)	<1
Blockchain Overhead (s/round)	0.8

6.2. BASELINE COMPARISONS

To evaluate how useful the proposed framework is, experimental findings are studied against several already existing frameworks.

- **Centralized Learning**: A traditional approach method where everyone shares their data, which helps to achieve the highest accuracy without any privacy protections.

- **Vanilla Federated Learning**: Federated Learning without blockchain, demonstrating the difference made by decentralized management and new aspects of security.
- **Personalized Federated Learning**: Federated Learning techniques that adjust the model for single users, which are used to assess both fairness and adaptation functionality.
- **Clustered Federated Learning**: Approaches that arrange similar clients together to tackle varying data and assist in the learning process.

People mainly compare baselines based on how accurate they are, the cost to operate them, and their security features. Usually, when blockchain is added to FL, the resulting model is slightly less accurate but more private and checks for transparency in comparison to FL alone.

TABLE 2 Comparison of learning approaches by accuracy, communication cost, and privacy

Method	Accuracy (%)	Comm. Cost (MB/round)	Privacy Leakage (%)
Centralized Learning	93.5	0	High
Vanilla Federated Learning	90.8	4.7	Moderate
Blockchain-Assisted FL	91.2	5.2	<1

6.3. PERFORMANCE ANALYSIS

6.3.1. MODEL PERFORMANCE

Blockchain in federated learning keeps the chosen model highly effective at predicting, almost the same as its counterpart in centralized learning models, but ensures no private data is exposed. Using privacy protection measures and recording data on the blockchain does not negatively impact how effective the model is, as its performance remains stable. Such personalized methods can lead to further performance gains for various groups of clients through adapting to their local data.

6.3.2. SCALABILITY

Scalability is measured by adding more data owners and checking how it influences the performance of the system. When the network is scaled, delays and communication expenses go up just a bit, and the framework is still efficient. Because blockchain uses a decentralized way to reach agreement and manages the participation of users, the system works well for large healthcare collaborations.

TABLE 3 Impact of number of clients on system performance

# Clients	Accuracy (%)	Latency (s/round)	Comm. Cost (MB/round)
10	91.5	2.8	3.1
50	91.2	3.5	5.2
100	90.9	4.7	8.3

6.3.3. Blockchain Overhead

Using blockchain increases the overhead because every node checks the consensus, transactions, and smart contract execution. Still, especially when consensus is efficient and smart contracts are updated, these drawbacks are not serious, as each round takes less than a second and there is only a slight boost in the cost of communication. It is deemed acceptable since it brings greater transparency, makes audits easier, and offers greater security.

TABLE 4 Overhead introduced by blockchain integration

Operation	Added Latency (s/round)	Added Comm. Cost (MB/round)
Without Blockchain	0	0
With Blockchain	0.8	0.5

7. DISCUSSION

7.1. INTERPRETATION OF RESULTS

Using a blockchain-based federated learning method in healthcare shows that a satisfactory level of privacy, model performance, and efficiency can be maintained. Distributed training often gets results that are as accurate as those using all the data together, proving it works even with data remaining inside the organization. Latency and the expenses involved in communication have increased only slightly as a result of adding blockchain to the system. Privacy is much safer in the proposed method, as shown by the metrics derived from testing attacks and measurable values, than it is in conventional federated learning, thanks to differential privacy and homomorphic encryption. Blockchain takes up little system resources but ensures security and transparency. Individual tests show that the framework can offer the same services to a higher number of people by using minor amounts of added resources. All these findings prove that the system satisfies both technical standards and regulatory policies, and it supports the development of credible and verifiable AI solutions in healthcare.

7.2. ADVANTAGES OF THE PROPOSED FRAMEWORK

This new blockchain-aided federated learning framework provides better advantages than standard and simple approaches.

- **Enhanced Privacy and Security**: Patient privacy and security are ensured because federated learning, in conjunction with blockchain and strong encryption, is used. As a result, information is protected, and companies are following strong rules about privacy in healthcare.
- **Transparency and Auditability**: The ledger maintained by all computers on the blockchain shows every update, aggregation, and move by any participant, making the DS system trackable and accountable. It is important to put confidence in your partners and those in charge of regulatory checks.
- **Resilience and Fault Tolerance**: The absence of central nodes in decentralized structure ensures the stability of the system when nodes or entities are missing.
- **Scalability**: The framework makes it possible for many participants to engage, using blockchain consensus methods and smart contracts to ensure secure and versatile handling of participants.
- **Fairness and Incentivization**: Smart contracts ensure that those who contribute their resources are rewarded, motivating transparent and equal collaboration among institutions.
- **Flexibility**: Being modular, the design can handle healthcare data of many types, use machine learning models, and protect privacy, serving a lot of different clinical tasks.

7.3. CHALLENGES AND LIMITATIONS

Even though its strengths are clear, the proposed framework still has many challenges and limitations that must be handled for it to become common.

- **Blockchain Overhead**: Even though the integration is well-managed, it adds extra time to transactions and more communication costs, which can be important issues in already stretched and immediate services.
- **Complexity of Implementation**: Using federated learning, advanced cryptography, and blockchain together is not easy and may discourage small institutions from joining the system.
- **Data Heterogeneity**: When data from various institutions have different qualities and sources, it may lead to inconsistent results, so clever methods for consolidating and personalizing data are required.
- **Regulatory and Legal Uncertainty**: Because data privacy laws and intellectual property rights are always evolving, following them might be tough in international research.
- **Scalability of Blockchain**: Public blockchains run out of capacity as the number of transactions rises; still, scalability is better handled by permissioned or hybrid blockchains.
- **User Adoption and Trust**: End-user adoption can be achieved by clearly highlighting the value of the system, offering intuitive interfaces, and showing how the system boosts patient privacy and results.

8. CONCLUSION AND FUTURE WORK

The use of blockchain together with federated learning greatly improves how healthcare data can be analyzed without revealing individual details. The architectural framework developed in the study uses both FL and blockchain to handle important challenges in healthcare, such as privacy, security, fairness, and bias. The framework ensures patient information stays safe and encourages different hospitals to collaborate on more reliable and fair medical decision tools. The proposed system has been proven to provide accurate models, strong fairness, and privacy with very limited increases in overhead thanks to the blockchain platform. Blockchain does away with single points of failure and ensures open records are accessible that show why and how all model updates and participant actions occurred, therefore encouraging trust from everyone involved. Bias mitigation is an important part of the framework, making sure that no accidental bias increases existing issues in healthcare, leading to better and equal healthcare for patients.

Even so, various problems still exist in these countries. Applying advanced cryptography and blockchain technologies to products calls for experts and careful development of the system. Consensus and logging for transactions, acceptable in simulations, could make overheads more noticeable as a deployment becomes bigger or runs in real-time. Since healthcare data is not the same everywhere and regulations continue to change, the algorithms need to be tested regularly and in a number of clinical settings. Future improvements should include adding ways to motivate and support collaboration among healthcare providers and implementing better fairness measures, along with advanced means of ensuring privacy. To make the system more reliable, it needs to be evaluated on more extensive data and in practical healthcare environments, and possible innovations such as swarm learning, edge computing, and fog computing must be researched.

REFERENCES

[1] Teo, Z. L., Jin, L., Liu, N., Li, S., Miao, D., Zhang, X., ... & Ting, D. S. W. (2024). Federated machine learning in healthcare: A systematic review on clinical applications and technical architecture. Cell Reports Medicine, 5(2).

[2] Zhang, F., Kreuter, D., Chen, Y., Dittmer, S., Tull, S., Shadbahr, T., ... & Schönlieb, C. B. (2024). Recent methodological advances in federated learning for healthcare. Patterns, 5(6).

[3] Dhade, P., & Shirke, P. (2024). Federated learning for healthcare: A comprehensive review. Engineering Proceedings, 59(1), 230.

[4] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., ... & Cardoso, M. J. (2020). The future of digital health with federated learning. NPJ digital medicine, 3(1), 119.

[5] Wang, T., Du, Y., Gong, Y., Choo, K. K. R., & Guo, Y. (2023). Applications of federated learning in mobile health: Scoping review. Journal of Medical Internet Research, 25, e43006.

[6] Joshi, M., Pal, A., & Sankarasubbu, M. (2022). Federated learning for healthcare domain-pipeline, applications and challenges. ACM Transactions on Computing for Healthcare, 3(4), 1-36.

[7] Rauniyar, A., Hagos, D. H., Jha, D., Håkegård, J. E., Bagci, U., Rawat, D. B., & Vlassov, V. (2023). Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. IEEE Internet of Things Journal, 11(5), 7374-7398.

[8] Noman, A. A., Rahaman, M., Pranto, T. H., & Rahman, R. M. (2023). Blockchain for medical collaboration: A federated learning-based approach for multi-class respiratory disease classification. Healthcare Analytics, 3, 100135.

[9] Farooq, K., Syed, H. J., Alqahtani, S. O., Nagmeldin, W., Ibrahim, A. O., & Gani, A. (2022). Blockchain federated learning for in-home health monitoring. Electronics, 12(1), 136.

[10] Rani, S., Kataria, A., Kumar, S., & Tiwari, P. (2023). Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. Knowledge-based systems, 274, 110658.

[11] Ngoupayou Limbepe, Z., Gai, K., & Yu, J. (2025). Blockchain-Based Privacy-Enhancing Federated Learning in Smart Healthcare: A Survey. Blockchains, 3(1), 1.

[12] Yurdem, B., Kuzlu, M., Gullu, M. K., Catak, F. O., & Tabassum, M. (2024). Federated learning: Overview, strategies, applications, tools and future directions. Heliyon.

[13] Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., ... & Roselander, J. (2019). Towards federated learning at scale: System design. Proceedings of machine learning and systems, 1, 374-388.

[14] Lo, S. K., Lu, Q., Zhu, L., Paik, H. Y., Xu, X., & Wang, C. (2022). Architectural patterns for the design of federated learning systems. Journal of Systems and Software, 191, 111357.

[15] Lazaros, K., Koumadorakis, D. E., Vrahatis, A. G., & Kotsiantis, S. (2024). Federated Learning: Navigating the Landscape of Collaborative Intelligence. Electronics, 13(23), 4744.

[16] Li, Y., Ibrahim, J., Chen, H., Yuan, D., & Choo, K. K. R. (2024). Holistic Evaluation Metrics: Use Case Sensitive Evaluation Metrics for Federated Learning. arXiv preprint arXiv:2405.02360.

[17] B. C. C. Marella, G. C. Vegineni, S. Addanki, E. Ellahi, A. K. K and R. Mandal, "A Comparative Analysis of Artificial Intelligence and Business Intelligence Using Big Data Analytics," *2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)*, Bhimtal, Nainital, India, 2025, pp. 1139-1144, doi: 10.1109/CE2CT64011.2025.10939850.

[18] P. K. Maroju, "Empowering Data-Driven Decision Making: The Role of Self-Service Analytics and Data Analysts in Modern Organization Strategies," International Journal of Innovations in Applied Science and Engineering (IJIASE), vol. 7, Aug. 2021.

[19] Gopichand Vemulapalli Subash Banala,Lakshmi Narasimha Raju Mudunuri,Gopi Chand Vegineni,Sireesha Addanki,Padmaja Pulivarthy, 2025, “Enhancing Decision-Making: From Raw Data to Strategic Insights for Business Growth”, 2nd IEEE International Conference on Data Science And Business Systems.

[20] Lakshmi Narasimha Raju Mudunuri, “Risk Mitigation Through Data Analytics: A Proactive Approach to Sourcing”, Excel International Journal of Technology, Engineering and Management, vol. 10, no.4, pp. 159-170, 2023, https://doi.uk.com/7.000100/EIJTEM.

[21] Lakshmikanthan, G., & Nair, S. S. . (2024). Collaborative Shield: Strengthening Access Control with Federated Learning in Cybersecurity. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 5(4), 29-38. https://doi.org/10.63282/wa3nzy85

[22] B. C. C. Marella, “Streamlining Big Data Processing with Serverless Architectures for Efficient Analysis,” FMDB Transactions on Sustainable Intelligent Networks., vol.1, no.4, pp. 242–251, 2024.

[23] Noor, S., Awan, H.H., Hashmi, A.S. et al. “Optimizing performance of parallel computing platforms for large-scale genome data analysis”. Computing 107, 86 (2025). https://doi.org/10.1007/s00607-025-01441-y.

[24] Nair, S. S., & Lakshmikanthan, G. (2024). Digital Identity Architecture for Autonomous Mobility: A Blockchain and Federation Approach. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 5(2), 25-36. https://doi.org/10.63282/49s0p265

[25] Aragani, V. M. (2022). “Unveiling the magic of AI and data analytics: Revolutionizing risk assessment and underwriting in the insurance industry”. International Journal of Advances in Engineering Research (IJAER), 24(VI), 1–13.

[26] A Novel AI-Blockchain-Edge Framework for Fast and Secure Transient Stability Assessment in Smart Grids, Sree Lakshmi Vineetha Bitragunta, International Journal for Multidisciplinary Research (IJFMR), Volume 6, Issue 6, November-December 2024, PP-1-11.

[27] Venu Madhav Aragani, 2025, “Implementing Blockchain for Advanced Supply Chain Data Sharing with Practical Byzantine Fault Tolerance (PBFT) Alogorithem of Innovative Sytem for sharing Suppaly chain Data”, IEEE 3rd International Conference On Advances In Computing, Communication and Materials.