E-ISSN 2586-9027
Homepage : https://tci-thaijo.org/index.php/SciTechAsia Science & Technology Asia
Vol.31 No.3 July - September 2026 Page: [259-277]
Original research article

Blockchain-Based Quantum-Secure Federated Learning with Hybrid Qkd-Pqc Encryption and Multi-Party Secure Aggregation for Healthcare Systems

Sandeep H.[1], Renukaradhya P.C.[2], Ranganatha H.R.[3,*], Rashmi B.C.[4]

[1]*Department of Artificial Intelligence & Data Science, Global Academy of Technology, Bangalore 560002, India*
[2]*Department of CS&E , Sapthagiri NPS University, Bangalore, Karnataka 560057, India*
[3]*Department of Computer Science and Engineering, Sapthagiri NPS University, Bangalore, Karnataka 560057, India*
[4]*Department of CSE (AI&ML), RNS Institute of Technology, Bangalore 560098, India*

Received 10 February 2026; Received in revised form 18 August 2026
Accepted 25 August 2026; Available online 30 September 2026

ABSTRACT

Predictive modelling of brain and critical care conditions requires accuracy, speed, and privacy, yet sensitive clinical data and fragmented healthcare systems hinder AI implementation. Existing Federated Learning frameworks struggle to balance performance, scalability, security, and privacy in real-world medical environments and deployment. This work proposes a fully encrypted federated learning architecture integrating locally trained models, enhanced by Adaptive Differential Privacy (ADP), with MIMIC-III/IV clinical datasets, ensuring hospital-level data locality while maintaining model accuracy. Post-Quantum Secure Communication is enabled through a Hybrid Obfuscated Quantum Key Distribution–Post-Quantum Cryptography (QKD-PQC) system, providing secure key exchange, dynamic obfuscation, and quantum-resistant encryption. AI-driven smart contracts on a Permissioned Blockchain verify PQC signatures, monitor node reputation, coordinate aggregation, and reward reliable participants. During global model synthesis, a Secure Aggregation Layer using Multi-Party Computation (MPC) and Shamir's Secret Sharing protects encrypted model updates, ensuring privacy and immutability.

Keywords: Artificial Intelligence (AI); Adaptive Differential Privacy (ADP); Multi-Party Computation (MPC); Quantum Key Distribution (QKD)

***Corresponding author:** ranganathahr@snpsu.edu.in **doi:**

1. Introduction

The rapid growth of digital healthcare has resulted in an exponential increase in clinical data generated from wearable technology, medical imaging, remote monitoring systems, and electronic health records. Such data holds immense promise for enhancing disease prediction, diagnosis, treatment planning, and overall patient outcomes if analyzed with state-of-the-art artificial intelligence algorithms [1, 2]. As healthcare systems globally embrace data-driven decision-making, there is an increasing requirement for safe, dependable, and compatible AI solutions. This shift has raised demand for computational frameworks that are capable of securely and ethically leveraging the value drawn from distributed medical data [3-5].

Traditional consolidated learning systems have several advantages, but they pose significant risks when used in healthcare settings. The gathering of patient data in centralized repositories creates potential security breaches, illegal access, and mass privacy violations. Stringent laws dictate the exchange of data and the security of patient data in healthcare organizations [6-8]. These limitations weaken the scope and quality of AI models developed on isolated datasets and make it difficult for effective collaboration among hospitals and healthcare centers. There is an emerging need for collaborative artificial intelligence models among healthcare providers that learn from diverse and geographically dispersed datasets without the transfer of sensitive data to meet contemporary therapeutic requirements [9, 10].

Federated collaboration is one of the most promising avenues, as this will allow institutions to collaborate on shared learning without requiring them to share local data. However, with the increasing volume and value of healthcare data, participant dependability, communication security, and defense against sophisticated attacks become a concern [11-13]. Real-world adoption requires resilience, trust, and transparency in such distributed contexts. Healthcare systems also need to be prepared for the imminent future of quantum computing, which poses serious threats to traditional cryptographic techniques that are widely used today to protect digital communication [14, 15]. Long-term privacy of transmitted medical data is at risk unless defenses are developed to prevent adversaries with quantum capabilities from breaking widely used encryption and signature systems [16].

This novel threat emphasizes the critical need for quantum-resistant measures to provide security for healthcare data in the present and the future. As such, the integration of distributed systems, secure communication frameworks, and AI must consider quantum-era dangers. Blockchain technology is gaining popularity in the healthcare sector due to its capabilities in decentralized trust, unchangeable records, and transparent processes for validation [17].

Permissioned versions allow only recognized institutions to take part in it, thus enabling clinical collaboration in a controlled and tamper-resistant environment. By mixing visibility with strong access control, blockchain can help improve confidence between hospitals that do not have full faith in each other. It becomes imperative to uphold such trust in order to maintain the integrity of the contributions and cooperation among various players in large-scale medical ecosystems [18-20].

The fast growth of digital healthcare has created an increased need for AI models that can learn from a variety of clinical data without jeopardizing patient privacy

or breaching legal restrictions. Traditional centralized AI systems, especially with quantum computing closing in on cracking conventional cryptography, have sensitive medical data at significant risk of breaches, unauthorized entry, and long-term confidentiality issues. Federated Learning introduces a viable alternative by enabling hospitals to collaboratively train models while keeping data resident within their local environments. However, it still requires strong assurances that any shared model updates cannot be intercepted, altered, or deanonymized. It is blockchain's contribution of adding trust, transparency, and tamper-resistance that guarantees only authenticated players contribute to the learning process. Even with blockchain, however, the aggregation process must ensure that no private model updates can be reconstructed by anyone. In fact, it is the strong defense afforded by quantum-secure cryptographic and secure aggregation that finally allows health organizations to collaborate securely and confidently. This integrated approach is necessary in creating robust, future-proof AI systems in healthcare.

- A federated learning system that leverages the MIMICIII/IV clinical datasets in a manner that ensures full data locality with strict compliance to healthcare-related privacy laws.
- To establish a local training system with enhanced Adaptive Differential Privacy, so that the model accuracy-privacy protection balance is dynamically adapted at every participating hospital.
- To protect the model updates against current and future quantum-capable adversaries, a hybrid obfuscated QKD-PQC system was integrated into a proposed Post-Quantum Secure Communication layer.
- AI-powered smart contracts were combined with a Permissioned Blockchain to handle incentive distribution, coordination of aggregation, reputation management, and authentication in a way that is both transparent and impenetrable.
- Designed a secure aggregation layer which combines Shamir's Secret Sharing with MPC, enabling globally private and integrity-preserving model updates without the disclosure of any sensitive client parameters.

The remainder of this paper is organized as follows: Section 2 reviews the fundamental works on safe aggregation, federated learning, and cryptographic techniques for healthcare systems. Section 3 describes the proposed safe aggregation framework on healthcare, which includes its architecture, threat model, and the encryption techniques used. Section 4 covers the experimental setup, the performance measures, and makes a comparison with existing methods. Finally, Section 5 summarizes all the major contributions of the work and presents directions for future work.

2. Related Work

Mijwil et al. [21] suggested a post-quantum safe blockchain-based federated learning system to improve the security of smart grids in 2025. Their solution combined quantum-resistant cryptography with decentralized learning to assure the security and integrity of grid data transferred between dispersed nodes. According to their results, including PQC methods protects

communication and reduces the vulnerability of upcoming quantum attacks. However, there were limiting factors for this work: the large computational burden and scalability over larger smart grid infrastructures remain restricted.

Ar-Reyouchi et al. [22] presented a secure-by-design framework for next-generation IoMT systems based on a hybrid quantum-blockchain and AI-based framework suitable for 6G healthcare networks. Encouraging outcomes were depicted for future remote diagnostics and telemedicine. However, this work faced issues in that there was little empirical validation of system functionality and no real-world implementation whatsoever.

Prajapat et al. [23] developed a generative AI-enabled quantum encryption technique for the protection of blockchain-based IoT-based healthcare applications. Performance measures regarding IoT contexts showed enhanced encryption strength with tolerable latency. Nevertheless, this work faced the issue of excessive resource consumption by generative models and their limited application in light-weight health care Internet of Things devices.

Alandjani [24] introduced a quantum-secure, blockchain-based, and MARL-federated framework to improve trust leadership in IIoT networks. This paradigm showed promise for the improvement of decision-making in large-scale industrial ecosystems. However, the algorithmic complexity and the long training times of MARL systems in dynamic IIoT contexts were challenges to the work.

Ali et al. [25] developed a post-quantum secure blockchain-based FL system to enhance the cybersecurity of smart grid infrastructures. Their work focused on integrating decentralized model updates with PQC algorithms to ensure long-term protection against quantum attacks. However, they faced challenges related to significant communication overhead, network latency, and dependence on sophisticated cryptographic techniques. Table 1 shows the related work comparison of existing techniques.

Table 1. Related work comparison.

Author	Techniques	Advantages	Dis-advantages
Mijwil et al. [21]	PQC, BFL	Enhanced security against quantum adversaries forsmart-grid infra-structure.	Scalability evaluation is limited.
Ar-Reyouchi et al. [22]	QKD, AI-based anomaly detection.	Enables cross-institutional collabora-tion with data locality.	Limited empirical throughput/ latency measure-ments on realistic 6G/IoMT testbeds.
Prajapat et al. [23]	Generative-AI-driven quantum-resistant encryption integrated with Blockchain.	Provides confiden-tiality gains and provenance/ access control for healthcare IoT.	High computa-tional cost on resource-constrained IoT devices.
Alandjani [24]	Multi-Agent Reinforcement Learning (MARL)	Improved robustness to Byzantine actors.	Limited performance evaluation at industrial scale.
Ali et al. [25]	Post-Quantum Signature Schemes combined with Blockchain-backed Federated Learning, Aggregation optimizations.	Provides compre-hensive bench-marking of PQC schemes for signing model updates.	Limited exploration of key-rotation policies under realistic operational constraints.

While modern healthcare systems generate large volumes of sensitive clinical data, strict privacy laws and security concerns prevent hospitals from sharing this data for collaborative AI research. Although adversarial manipulation is already a risk in current federated learning

frameworks, long-term cryptographic risks also pose great threats. Traditional centralized learning leaves patient records open to breaches, while an urgent need exists for quantum-resistant security in dispersed medical environments due to the rise of quantum computing, which puts conventional encryption at far greater risk. Present aggregation algorithms cannot offer confidentiality when several untrusted nodes participate, and trust management across institutions often lacks transparency. A safe, privacy-preserving, and quantum-resilient federated learning architecture is required to enable trustworthy multi-hospital collaboration without risking the integrity or confidentiality of patient data.

3. Proposed Methodology

First, the proposed methodology will utilize MIMIC-III/IV health datasets that contain real clinical data, including vital signs, lab results, prescription drugs, and critical care notes. For complete data localization and privacy requirements, each participating hospital shall access only that portion of this dataset allocated to it. Then, each node separately performs local model training using ADP. With dynamic variation injection into gradients or weights based on training behavior and data sensitivity, ADP enables each institution to maintain tight anonymity while still generating high-quality model updates during training. These are privacy-ensuring upgrades, ready to be securely transmitted across the federated learning environment. Fig. 1 shows the architecture of the proposed study.

It combines a Hybrid Obfuscated QKD-PQC system that provides ultra-secure key exchange with improved resistance against new quantum threats with PQC-based encryption and signatures to offer a Post-Quantum Secure Communication layer that protects model updates during transmission. The encrypted updates are then sent to a Permissioned Blockchain server where AI-driven smart contracts govern node reputation, ensure authenticity, manage aggregation, and fairly distribute rewards. Last but not least, a Secure Aggregation Layer using Shamir's Secret Sharing and Multi-Party Computation ensures that no single entity will recover local parameter values while still enabling the accurate global model synthesis. Put together, these elements offer a trusted, quantum-resilient, privacy-preserving federated learning system for modern healthcare environments.

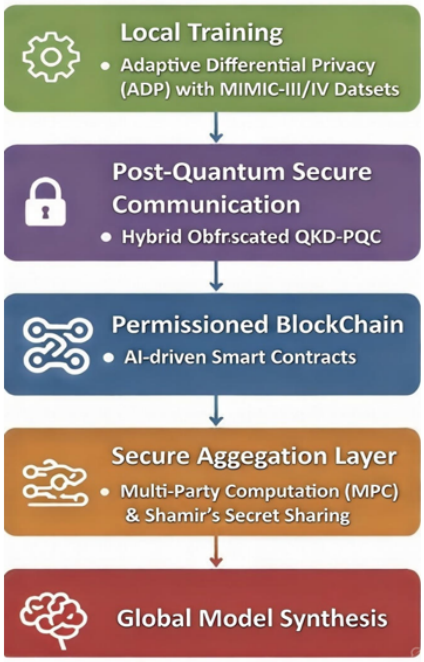

Fig. 1. Proposed architecture..

3.1 Data collection

MIMIC-IV dataset: Medical Information Mart for Intensive Care, version 4: MIMIC-IV is a freely available, de-identified, large clinical dataset, which col-

lects comprehensive health records of patients admitted to Beth Israel Deaconess Medical Center between the years 2008 and 2019. It includes demographics, vital signs, lab measures, diagnoses, treatments, prescription drugs, imaging reports, and summaries of the ICU stay. Structured modules of the dataset-hosp (hospital-level interactions), icu (ICU-level detailed measures), and ed (emergency department data)-enable researchers to examine a wide array of clinical prediction tasks. Mortality prediction-alive vs. deceased-length-of-stay classification, readmission risk, sepsis detection (sepsis vs. non-sepsis), classification of diseases like heart failure, pneumonia, diabetes, intervention prediction categories such as the requirement for mechanical ventilation or vasopressor use are all target classes derived.

3.2 Local model training with adaptive differential privacy

In the proposed system, every hospital node uses private patient data to independently train a local model, ensuring sensitive clinical data never leaves the premises. The model gradients go through Adaptive Differential Privacy before being sent to the federated learning server to ensure secrecy during training. ADP adds precisely calibrated noise that dynamically changes with the iteration of training, gradient magnitude, and data sensitivity. This adaptive method balances privacy and accuracy by not allowing excessive noise addition while ensuring robust privacy.

The updating of the gradient using ADP has the following expression:

$$\tilde{g}t = gt + N(0, \sigma^2 tI), \qquad (3.1)$$

where σt is the adaptive noise scale and gt is the raw gradient at iteration t.

Thus, the ultimate local model update is

$$\omega_{t+1} = \omega_t - \eta \tilde{g}t. \qquad (3.2)$$

This ensures that all nodes of the federated learning network provide relevant and privacy-preserving updates for safe global aggregation.

3.3 Post-quantum secure communication

In particular, the proposed scheme places strong emphasis on ensuring secure, quantum-resistant communication in federated learning systems with IoT and healthcare applications. These are distributed systems where local model updates are exchanged between a central server and nodes (e.g., hospitals or IoT devices). It is important to provide assurance over the confidentiality, integrity, and validity of these updates, especially against a threat model contemplating quantum attack that could render conventional cryptographic schemes vulnerable. Our solution integrates QKD, PQC, and advanced obfuscation and reactive parameter-shifting mechanisms into a robust multilayer security architecture.

3.3.1 Local model update and preprocessing

Each node i has a private dataset Di to train a local model $Mi.\Delta Wi$ represents the gradients or local model parameters which are ready for safe transmission. To support adjustable encryption strength, a normalisation and sensitivity evaluation is implemented before encryption.

$$Si =_j^{max} |\Delta W_j^i|, \; j = 1, 2, ..., n, \qquad (3.3)$$

where n is the total number of parameters and Si is the sensitivity of the model update of the i-th node. Afterwards, the sensitivity will determine the adaptive noise as well as encryption parameters.

3.3.2 Post-quantum cryptographic encryption

First, every update in the model is encrypted with a PQC system such as Kyber for lattice-based key encapsulation or Dilithium for lattice-based digital signature, to prevent quantum attacks. The following explains the encryption process:

$$C_i = PQC_ENC_{ki}(\Delta Wi). \quad (3.4)$$

In this case, C_i represents the encrypted models update, and K_i is the symmetric key obtained by PQC-based key exchange function f and a hybrid Quantum Key Distribution. Model sensitivity is integrated into the adaptive key derivation in order to improve resilience over targeted attacks on extremely sensitive updates.

3.3.3 Hybrid QKD-PQC key exchange

Here, the New Hybrid Obfuscated QKD-PQC system in order to improve key distribution. In the proposed system, quantum keys KQ are first generated through QKD between the central server and the node.

$$KQ = QKD(Ai, S), \quad (3.5)$$

where S denotes the central server and Ai denotes the node. QKD offers information-theoretic security against eavesdropping. Then, the quantum key is combined with a PQC-derived key KP in order to enhance the security for a longer term and thus prevent side-channel attacks:

$$Ki = Hash(KQ \oplus KP). \quad (3.6)$$

This hybrid key, Ki inherits the advantages of both quantum and post-quantum cryptography, enabling forward secrecy and providing defense against quantum and classical attacks.

3.3.4 Obfuscation and adaptive parameter shifting

Both encryption and signing are obfuscated and, in addition, adaptively parameter-shifted to enhance the security. Obfuscated PQC encryption with adaptive parameters $\theta = (\theta 1, \theta 2, ..., \theta m)$ is denoted as $E\theta$.

$$E\theta(\Delta Wi) = PQC_ENC_{ki}(\Delta Wi + \eta(\theta)). \quad (3.7)$$

We give a mathematical definition to describe the obfuscation as follows: $\eta(\theta)$ is a perturbation vector generated dynamically from time, network state, and system parameters. Adaptive parameter-shifting can guarantee that cryptographic procedures will change over time:

$$\theta(t+1) = \theta(t) + \alpha \cdot \nabla F(\theta(t)). \quad (3.8)$$

In this case, $F(\theta)$ represents a feedback function assessing the security strength of the current configuration, and α is the learning rate controlling the adaptation pace.

To ensure validity, each encrypted model update is signed by a PQC-based digital signature system, like Dilithium. This confirms that the updates are unmodified from transmission and indeed were transmitted from a valid node. Each node sends the final secure payload to a central server. Before running federated aggregation, the server decrypts the structure version using the hybrid key Ki and verifies the signature.

$$W_{global}^{(t+1)} = \sum_{i=1}^{N} \frac{|Di|}{\sum_j |Dj|} \Delta Wi, \quad (3.9)$$

where N is the total number of nodes participating, and Di is the size of the local dataset for weight aggregation. Therefore, this strategy gives a robust, post-quantum

safe interactions layer for FL, providing protection to sensible dispersed data while preserving system effectiveness.

The corrupt model is assumed to be fixed in every training round, and the number of colluding nodes is assumed to be less than the Shamir secret-sharing threshold (T), which means that an update of any model cannot be reconstructed from the colluding nodes. The federated server is honored but not trusted and it is up to the individual clients to use secure aggregation to prevent it from accessing any of their updates; the federated server aggregates them properly. Within the system, only hospitals and blockchain validators with valid authentication can be involved; and as in a standard permissioned blockchain, there is the assumption that blockchain validators will adhere to the consensus protocol, but a bounded fraction may be malicious. Moreover, the adversary is supposed to be able to use the communication channel, and it could try to intercept or replay an attack, but hybrid QKD-PQC communication security and post-quantum digital signatures are applied to prevent these attacks for communication security and authentication/integrity. The model also assumes that a future adversary might be quantum capable but that the primitives used in the post-quantum cryptography and the mechanisms based on QKD will be secure with respect to their security assumptions, thus preventing attacks on the model leakage, message tampering, impersonation, and reconstruction of individual updates without authorization.

3.4 Permissioned blockchain integration

It is suggested that the approach integrates a Permissioned Blockchain network into the collaborative learning process to provide safe, verified, and impenetrable transmission of encrypted model updates across approved healthcare facilities. This approach improves the dependability, equity, and auditability of cooperative model training by utilizing decentralized trust mechanisms, AI-driven smart contracts, and Post-Quantum Cryptography signatures.

3.4.1 Secure transmission and PQC-protected model updates

Each participating hospital Hi, having trained a local model on its own dataset, receives a parameter update vector ΔWi. In order to resist impersonation, replay crimes, and quantum-enabled forgery attempts, updates are digitally signed using PQC techniques such as CRYSTALS-Dilithium and encrypted with hybrid quantum-resistant keys prior to transmission.

$$Ci = Enc_{ki}(\Delta Wi), \tag{3.10}$$

$$\sigma i = PQC_Sign_{SKi}(Ci). \tag{3.11}$$

In this case, Ci is the encoded model update, Ki is a symmetric key shared through PQC-based key transfer, and σi is the digital signature attesting to validity. To preserve patient privacy and institutional identity, changes can only be submitted by approved hospitals in the permissioned network.

3.4.2 Permissioned blockchain validation and smart contract verification

Signed and encrypted updates are then sent as transactions to the approved blockchain, where a consensus is reached by only reliable healthcare nodes. A smart contract S powered by AI performs automated verification:

$$S(Ci, \sigma i, PKi) = \begin{cases} 1, & \text{if } PQC_Verify_{PKi}(Ci, \sigma i \\ 0, & \text{Otherwise.} \end{cases} \tag{3.12}$$

The changes included in the blockchain ledger are only those that return

1 (valid). Since the blockchain ensures all the submissions are immutable, forensic tracking is possible and model manipulation is impossible. Since the network is permissioned, consensus latency and storage overhead are kept optimum for real-time collaboration in healthcare.

Smart contracts ensure secure model aggregation through the computation of a blockchain-recorded global model and selection of approved updates. In order to ensure equity across hospitals, a weighted contribution score is utilized,

$$W_{global}^{(t+1)} = \sum_{i=1}^{N} ri.\Delta Wi, \tag{3.13}$$

where ri is a blockchain-maintained reputation value representing node dependability, historical accuracy, and contribution consistency.

Next come updates of reputation estimates:

$$r_i^{(t+1)} = r_i^{(t)} + \beta.Qi, \tag{3.14}$$

where β is a learning factor and Qi is a quality metric obtained from anomaly detection, gradient verification, or accuracy improvement. Furthermore, smart contracts automate incentive allocation and promote the occurrence of frequent high-quality updates by the hospitals. This method encourages sincere involvement, strengthens confidence across institutions, and deters dishonest or careless inputs. The proposed method will ensure quantum-resilient, transparent, and fair federated learning across healthcare institutions by incorporating PQC-secured update transmission, blockchain-facilitated authentication, and AI-driven smart contracts for approval, reputation, and incentives. This approach ensures model updates are tamper-proof, protects private clinical data, and fosters trustworthy collaboration in a secure, decentralized environment.

3.5 Secure aggregation

The Secure Aggregation Layer is a fundamental privacy-preserving technique in Federated Learning where multiple clients can jointly train a global model without revealing their raw model updates to anyone. This layer leverages Shamir's Secret Sharing along with the Novel Multi-Party Computation protocol to keep sensitive model parameters away f rom any single aggregate node. Each client encrypts its local modeling update ΔWi and splits it into several secret shares before transmission. These shares are distributed among a group of authorized aggregating nodes in such a way that no single node can recover the original update on its own. This architecture ensures secrecy even if one or more of these aggregating nodes get compromised. Fig. 2 shows the architecture of secure aggregation.

3.5.1 Secret sharing by clients

First, each client, C_i computes its local modeling update, ΔWi. Instead of directly transmitting ΔWi, the client employs Shamir's Secret Sharing to divide its update into N different shares or polynomials, where N was the number of authorized aggregate nodes. This guarantees that at least an initial threshold of shares will be needed to re-construct the update in its original form ΔWi.

Shamir's Secret Sharing (Polynomial Generation): The secret, ΔWi, is the constant term in a polynomial $P_i(x)$ of degree T-1 generated by the client C_i:

$$P_i(x) = \Delta Wi + a_1 x + a_2 x^2 + ...a_{T-1} x^{T-1}. \tag{3.15}$$

Then the client evaluates the polynomial in various places x_j for every aggrega-

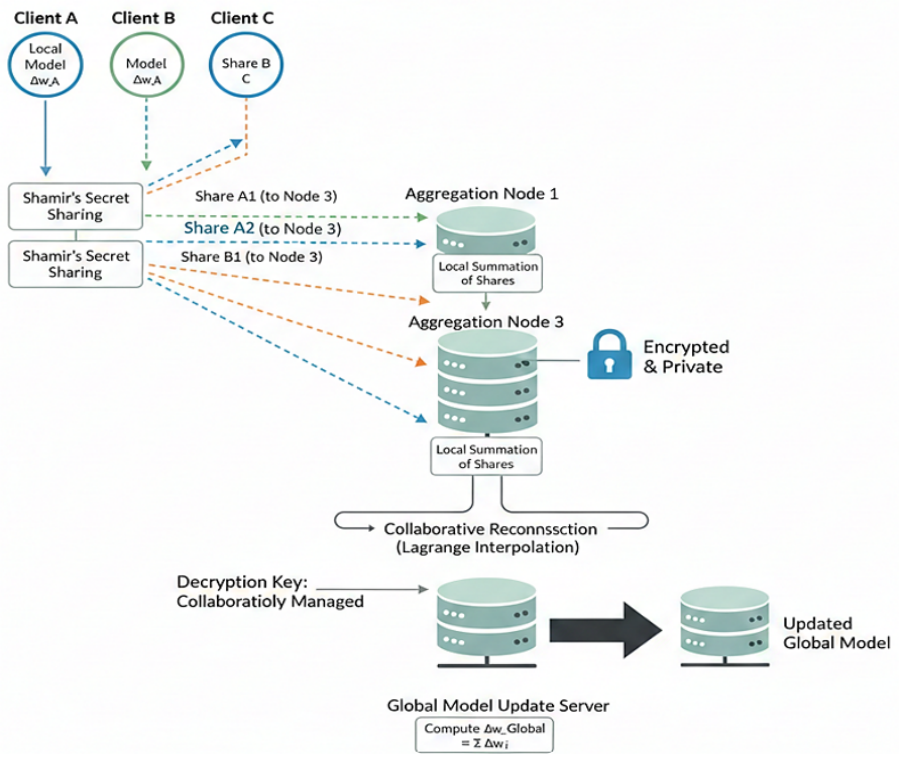

Fig. 2. Architecture of secure aggregation.

tion node $j = 1, ..N, N$ to obtain Nshares. This is the share s_{ij} for node j.

$$s_{ij} = P_i(x_j). \tag{3.16}$$

These shares s_{ij} are subsequently distributed to the N aggregation nodes. Importantly, no single node knows enough to reconstruct the original updateΔWi, since no node possesses more than T shares.

3.5.2 Secure aggregation by nodes (MPC)

The aggregation nodes receive shares across all active clients. In every node, the local sum of the shares that it received from all clients can be computed without decrypting every single contribution individually since summing shares equates to summing the underlying secrets due to a Shamir's Secret Sharing characteristic. Let S_j denote the sum of shares that the aggregation node j received from all the M active clients:

$$S_j = \sum_{i=1}^{M} s_{ij} = \sum_{i=1}^{M} P_i(x_j). \tag{3.17}$$

3.5.3 Global model update

The aggregation nodes then jointly aggregate their sums s_{ij} to reconstruct the aggregation global update $\sum_{i=1}^{M} \Delta Wi$. This is done using the Lagrange Interpolation formula, that is the reconstruction phase of Shamir's Secret Sharing, but applied on the summed values s_j. The ultimate aggregation update,$\Delta WGlobal$, is the constant term of the patched polynomial $\sum_{i=1}^{M} P_i(x)$, which is equal to the sum of the original secrets:

$$\Delta WGlobal = \sum_{i=1}^{M} \Delta Wi. \tag{3.18}$$

While the raw updates to the models (ΔWi) are never exposed in plaintext to any one entity, including the server and the aggregation nodes, this whole process ensures the correct computation of the global model update. The confidentiality of the system is preserved even when up to $T-1$ aggregation nodes are compromised. Up to $(T-1)$ colluding aggregation nodes cannot reconstruct an individual client update from their available shares. If (T) or more aggregation nodes collude, this confidentiality guarantee no longer holds, which is an explicit limitation of the proposed threshold-based design.

The Secure Aggregation Layer creates a strong, cryptographically protected environment by which model contributions stay confidential, unlawful reconstruction is statistically infeasible, and collaborative learning can take place without any direct communication of information between participants. Algorithm 1 shows the proposed work flow:

Algoritm 1: The proposed work flow.

Input:	Local healthcare datasets, initial global model, privacy parameters, QKD-PQC security parameters, blockchain network, and aggregation threshold.
Output:	Updated global model MG
1.	Initialize the global model MG and register all authorized hospitals in the permissioned blockchain network.
2.	**For each federated learning round** $r = 1, 2, \ldots R$**:**
3.	The central server distributes the current global model to all participating hospitals.
4.	For each participating hospital Hi: • Keep the private healthcare dataset Di within the hospital. • Preprocess the local dataset and initialize the local model using MG. • Train the local model using the private dataset. • Calculate the local model gradients/update. • Evaluate the gradient magnitude, training stage, and data sensitivity. • Determine the adaptive privacy level. • Add calibrated differential-privacy noise to the local update.
5.	Evaluate the sensitivity to determine the Ui required communication security level.
6.	Generate a QKD key between hospital and the central server.
7.	Generate a post-quantum cryptographic key using the selected PQC mechanism.
8.	Combine the QKD and PQC keys to establish a hybrid quantum-resistant session key.
9.	Encrypt the privacy-preserving update using the hybrid session key.
10.	Apply the proposed obfuscation and adaptive parameter-shifting mechanism to the encrypted update.
11.	Generate a post-quantum digital signature for the protected update.
12.	Transmit the encrypted and signed update to the permissioned blockchain network.
13.	The blockchain verifies the hospital identity and validates the digital signature.
14.	Reject updates from unauthorized, invalid, or suspicious participants.
15.	Record valid model updates as blockchain transactions.
16.	Use smart contracts to perform update verification, contribution assessment, reputation management, and incentive allocation.
17.	Forward the approved model updates to the secure aggregation layer.
18.	Each participating hospital divides its approved update into multiple secret shares using Shamir's Secret Sharing.
19.	Distribute the secret shares among the authorized aggregation nodes.
20.	The aggregation nodes jointly process the received shares using Multi-Party Computation (MPC) without revealing individual hospital updates.
21.	Combine the secret shares according to the predefined aggregation threshold.
22.	Reconstruct only the aggregated global update without recovering any individual hospital update.
23.	Update the global model using the securely aggregated update.
24.	**End For**
25.	Check the global model performance against the predefined stopping criterion.
26.	If the stopping criterion is not satisfied, start the next federated learning round.
27.	Otherwise, return the final trained global model MG.
End Algorithm	

4. Result and Discussion

The proposed approach shows better decryption accuracy and computational efficiency, with more entropy, and lower key generation and latency in encryption/decryption, compared with AES-256, ECDSA, Salsa20, ECC-256, and Twofish. Also, compared with FedMA, FedAvgM, FedOpt, FedPAQ, and FedBN, the proposed model attains improved precision, recall, accuracy, specificity, F1-score, and MCC with minimized MSE, MAE, and energy consumption in the evaluation of federated learning. This enables safe and effective distributed clinical intelligence.

4.1 Evaluation metrics

The proposed method is evaluated on a number of measures that determine its effectiveness, including precision, accuracy, sensitivity, RMSE, MSE, and MAE. Table 2 summarizes the effectiveness of the proposed approach and also provides the relevant evaluation results.

Table 2. Evaluation metrics.

Metrics	Formula
Accuracy	$ACC = \frac{T_{po}+T_{ne}}{T_{po}+T_{ne}+F_{po}+F_{ne}}$
Sensitivity	$SENS = \frac{T_{po}}{T_{po}+F_{ne}}$
Precision	$PRE = \frac{T_{po}}{T_{po}+F_{po}}$
Specificity	$SPEC = \frac{T_{ne}}{T_{ne}+F_{po}}$
F1 score	$F1 = 2 \cdot \frac{PRE \cdot REC}{PRE+REC}$
MAE	$MAE = \frac{1}{M}\sum_{j=1}^{M} \lvert x_j - \hat{x} \rvert$
MSE	$MSE = \frac{1}{M}\sum_{j=1}^{M} (x_j - \hat{x})^2$

4.2 Performance analysis

The proposed framework is suitable to provide safe, reliable, yet computationally efficient distributed clinical intelligence for large-scale healthcare systems. Fig. 3 shows the accuracy and loss validation for the proposed study by varying epoch value.

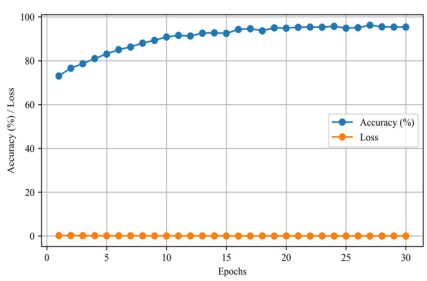

Fig. 3. Accuracy and Loss curve.

The figure shows the trend of accuracy and loss regarding the training performance of a machine learning model over 30 epochs. The y-axis represents accuracy as a percentage and loss values, while the x-axis shows the total number of training epochs. During further training, the model's accuracy gradually increases from its initial value of 73%. Accuracy reaches approximately 95–96% toward the last epochs, which constitutes efficient learning and improvement in the ability of a model to make predictions. The prediction errors are gradually reduced, as evidenced by the loss curve simultaneously falling rapidly in the early epochs and eventually stabilizing close to zero. The increase in accuracy and decrease in loss both show an inverse relationship, which indicates stable model convergence. Altogether, there are no obvious indications of overfitting, and this figure shows successful training with steadily improving performance. Fig. 4 shows the confusion matrix for the proposed study.

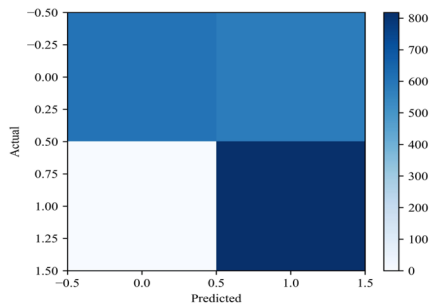

Fig. 4. Confusion matrix.

This figure shows a confusion matrix used to evaluate the performance of a binary classification model. The y-axis represents actual class labels, while the x-axis represents expected class labels. According to the color bar, each cell depicts the number of samples that fell into a specific actual-predicted pairing; darker shades reflect larger values. The top-left and bottom-right cells, respectively, correspond to the true negatives and true positives, reflecting accurate predictions. The darkened bottom-right cell reflects a large number of posi-

tive samples classified correctly. The top-right cell represents false positives, whereas very few false negatives are reflected by the light-colored cell in the bottom left. Strong classification with high accuracy and little misclassification is suggested in general by the matrix. Fig. 5 shows various encryption techniques, focusing on latency measurements.

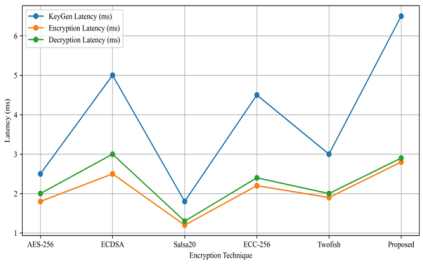

Fig. 5. Cryptographic performance.

This graph compares the cryptographic performance of various encryption techniques, focusing on latency measurements. AES-256, ECDSA, Salsa20, ECC-256, Twofish, and the proposed method are some of the encryption techniques displayed along the x-axis, while latency in milliseconds is displayed along the y-axis. Three performance parameters are shown: encryption latency, decryption latency, and key generation latency. Salsa20 has the lowest latency across all three categories, indicating a high degree of computational efficiency. On the contrary, because of their higher computational complexity, ECDSA and the proposed technique have higher key generation latency. The proposed technique presents moderate values for encryption and decryption latencies, which remain relatively similar across methods. The figure shows how cryptographic algorithms trade off computational efficiency against security strength. Fig. 6 indicates entropy level for proposed and existing studies.

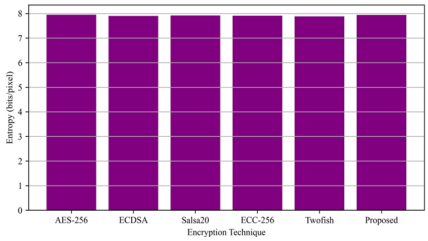

Fig. 6. Entropy level.

The following figure presents a bar chart showing the entropy level for some encryption methods, namely AES-256, ECDSA, Salsa20, ECC-256, Twofish, and the proposed technique. Entropy is in bits per pixel on the y-axis, and encryption techniques are on the x-axis. In fact, all techniques have entropy values very close to the optimum value for encrypted data, which is almost 8 bits per pixel. This indicates strong resistance against statistical attacks, with a high degree of randomness. The entropy of the suggested technique is comparable to well-established techniques, hence implying strong cryptography. Basically, the picture shows that all the evaluated methods—including the proposed strategy—result in secure, well randomized encryption outputs suitable for sensitive data protection. Fig. 7 shows the correlation coefficients for the existing and proposed method.

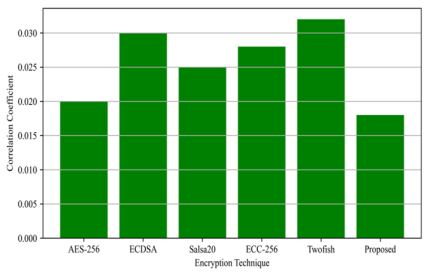

Fig. 7. Correlation coefficient.

The figure shows a bar chart representing correlation coefficients for various encryption methods such as AES-256,

ECDSA, Salsa20, ECC-256, Twofish, and the proposed approach. The y-axis represents values of the correlation coefficient, while the x-axis represents the encryption approaches. Since lower correlation depicts less statistical similarity between the original and encrypted data, it is considered a sign of higher encryption quality. The proposed strategy, among those tested, has the lowest correlation coefficient, indicating that it is more resistant to statistical and differential attacks. Other techniques, while still within reasonable bounds regarding security, have somewhat higher correlation values. In general, the graph depicts an increase in decorrelation by the proposed approach, enhancing the robustness of encryption and data confidentiality. Fig. 8 shows the accuracy for various existing and proposed encryption techniques.

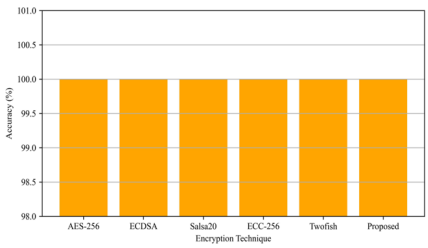

Fig. 8. Accuracy for encryption technique's.

A bar graph is presented that compares the correctness percentages of various encryption methods, such as AES-256, ECDSA, Salsa20, ECC-256, Twofish, and the proposed approach. The x-axis represents the encryption methods and the y-axis represents correctness percentage. Each approach yields 100% accuracy, which represents perfect or near-perfect performance of the test under consideration. It means that all the schemes are equally effective regarding the integrity of data and accuracy in encryption and decryption. However, consistency in accuracy level across the approaches stipulates that measurements such as latency, entropy, or correlation could be more helpful regarding distinguishing performance differences among these techniques compared to accuracy alone. Fig. 9 indicates the throughput performance for both existing and proposed techniques.

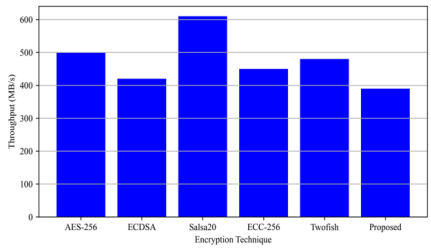

Fig. 9. Throughput.

The figure depicts a bar graph representing throughput performance of various encryption methods in terms of MB/s. Different encryption techniques are shown along the x-axis, including AES-256, ECDSA, Salsa20, ECC-256, Twofish, and the Proposed Method, while throughput is shown on the y. Salsa20 achieves the highest throughput, reflecting particularly good processing speed and efficiency for large quantities of data. Very high throughput performance is also reflected in AES-256 and Twofish, but ECC-256 and ECDSA reveal slightly lower numbers due to their higher computational overhead. The proposed method strikes a balance between efficiency and security, recording a moderate throughput. The depicts performance trade-offs among encryption techniques for high-throughput data environments. Fig. 10 shows the normalized score for federated learning performance.

The graphical representation shows a normalized bar chart of various federated learning algorithms such as FedMA, FedAvgM, FedOpt, FedPAQ, FedBN, and proposed algorithms. The X-axis shows

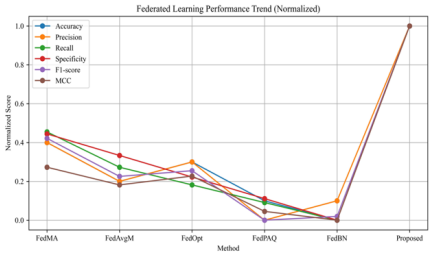

Fig. 10. Federated learning performance.

the different algorithms, while the y-axis shows normalized scores of various evaluation metrics such as MCC, precision, recall, specificity, and F1-score. The existing algorithms are just mildly good; rather, they are fluctuating because FedPAQ and FedBN algorithms show a marked degradation in performance. However, the proposed algorithm shows peak points and acquires maximum normalized scores for all evaluation parameters, which represent superb class performance. Hence, this graph shows that this federated learning algorithm is more reliable and effective than existing algorithms. Fig. 11 shows performance comparison of proposed and existing federated learning techniques.

Ten parameters are used to compare the Proposed Federated Learning technique with five existing methods, which are presented in bar charts. In nearly all parameters concerning the efficacy and efficiency of models, the proposed technique performs outstandingly. For instance, all positive parameters including Accuracy, F1-score, Precision, Recall, Specificity, and MCC show the highest values for the proposed technique. On the other hand, the worst performances in negative parameters such as RMSE with a value of approximately 0.035, and Energy with a magnitude of approximately 250 J, indicate enhanced capability in error minimization and energy usage, respectively. Therefore, this thorough evaluation confirms without doubts that Proposed Federated Learning performs better than existing methods in both efficacy and efficiency. Fig. 12 shows the processing time for both existing and proposed approaches.

The bar chart shows six Federated Learning methods in relation to their run times in seconds, with a total scale measured around 250–360 seconds. The leading player in this case is ”Proposed,” completing in approximately 250 seconds, making it far more efficient than other methods. FedMA takes the longest time, approximately 360 seconds. The next is FedOpt, which takes about 350 seconds, followed by FedAvgM with 340 seconds, then FedBN with 330 seconds, all above 300 seconds. FedPAQ takes approximately 300 seconds, a moderate pace. In summary, the above results show that ”Proposed” is the quickest technique among all tested benchmarks. Table 3 shows the comparison analysis of proposed and existing approaches. Fig. 13 shows the ROC curve comparison for the proposed method.

The graph above shows an ROC curve, which is a widely used technique for assessing the performance of a two-class classifier. The blue solid curve with a marked area corresponds to the proposed model, which shows Sensitivity against[TD2.1]. The ROC curve lies in the top left corner, which is a representation of a nearly perfect classifier. With an AUC of 0.999, the model is very efficient in classifying a positive and negative class.

The following table gives a comparison of current security solutions in distributed systems and healthcare systems using quantum and post-quantum technology. To improve the task of securing aggregated data, this research work focuses on a solution using hybrid QKD-

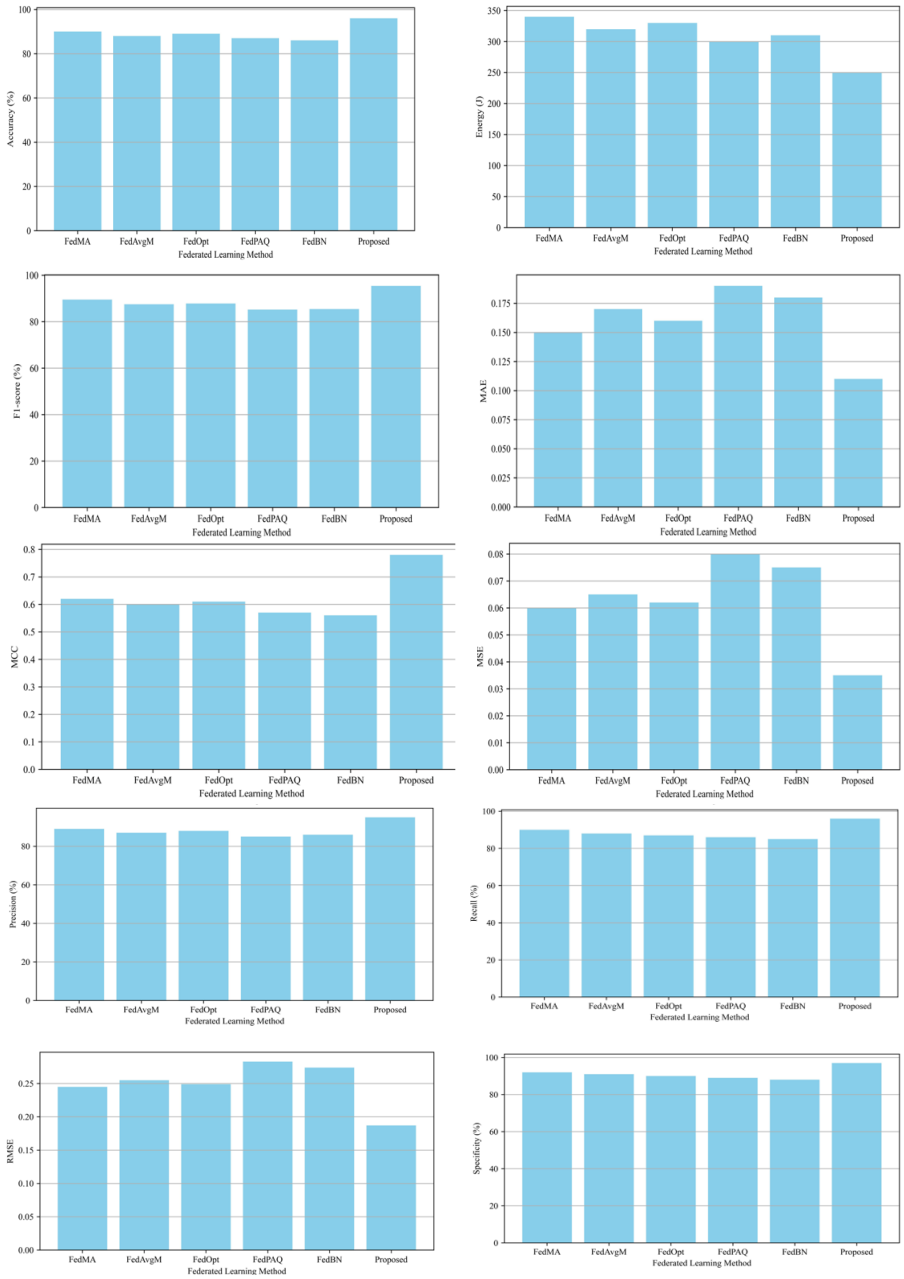

Fig. 11. Performance comparison for both existing and proposed technique.

PQC encryption and multi-party computation. The existing research shows great efficiency in performance: PQS-BFL, incorporating blockchain, federated learning, and lightweight post-quantum cryptography, attains a high accuracy level of fake data identification with fast detection speed of up to 95%. QBSF, with the combination of QKD, blockchain, and deep reinforcement learning, substantially improves security scores

Table 3. Comparison analysis of proposed and existing approaches.

Method	FedMA	FedAvgM	FedOpt	FedPAQ	FedBN	Proposed
Accuracy (%)	89	88	89	87	86	96
Energy (J)	340	320	330	300	310	250
F1-Score (%)	90	88	89	86	87	95
MAE	0.15	0.17	0.16	0.19	0.18	0.11
MCC	0.62	0.6	0.61	0.57	0.56	0.78
MSE	0.06	0.065	0.062	0.08	0.075	0.035
Precision (%)	90	88	89	85	86	94
Recall (%)	90	88	87	86	85	96
Time (s)	365	340	350	300	328	250
RMSE	0.245	0.255	0.25	0.28	0.27	0.185

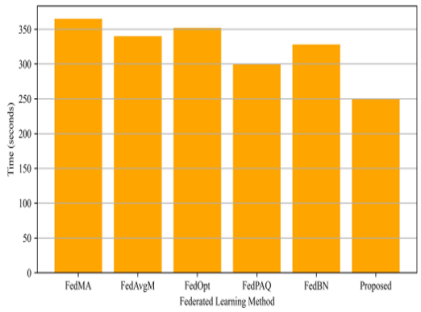

Fig. 12. Processing time.

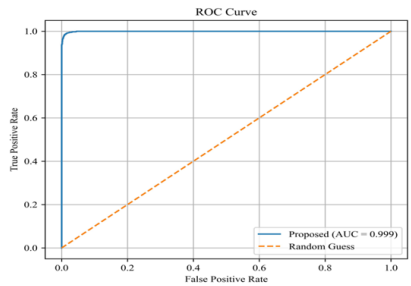

Fig. 13. ROC curve.

and decreases attack mistakes. Other research on generative AI, MARL, and PQC methods demonstrates great accuracy, precision, anomaly, and defense against poisonous attacks. Table 4 shows the state-of-art comparison for existing and proposed techniques.

5. Conclusion

This study proposed a privacy-preserving and quantum-resistant federated learning framework for critical healthcare and brain disease prediction by integrating adaptive differential privacy, MPC-based secure aggregation, permissioned blockchain, and hybrid QKD-PQC communication. The key lesson learned is that secure healthcare AI requires a multi-layered design where privacy, security, trust, and aggregation are jointly addressed rather than independently optimized. In practice, keeping data local, protecting model updates before transmission, and verifying participants through blockchain, significantly improves system reliability. However, stronger security inevitably introduces additional computational, communication, and storage overhead, highlighting an important trade-off between performance and protection. Therefore, careful configuration of privacy levels and cryptographic mechanisms is essential for real deployment. Overall, the framework provides a scalable and trustworthy foundation for collaborative healthcare learning, with future work focusing on efficiency optimization, edge deployment, and clinical interpretability for real-world adoption.

References

[1] Sahinbas K, Catak FO. Secure multi-party computation-based privacy-preserving data analysis in healthcare IoT systems.

Table 4. State-of-art comparison.

Authors	Techniques	Key Parameters	Accuracy Performance
Proposed	Hybrid QKD-PQC Encryption	Quantum Key Distribution (QKD), Multi-Party Computation (MPC)	Accuracy – 96%, Precision – 94%
[21]	PQS-BFL: Post-Quantum Secure Blockchain-based Federated Learning	Lightweight PQC protocols, Scalable Blockchain, Smart Grid architecture	95% probability in locating false data; Detection time <0.011s
[22]	QBSF: Quantum-Blockchain Secured Framework for IoMT	Quantum Key Distribution (QKD), Blockchain, Deep Reinforcement Learning (DRL)	137.5% security score improvement; 80% reduction in attack error rates
[23]	Generative AI-Enabled Quantum Encryption for Healthcare	Generative AI (GAI), Quantum Encryption, Dynamic Key Exchange, Hash functions	95% Accuracy; 95.1% Precision; 95.5% F1-score
[24]	MARL-Federated Blockchain: Quantum secure trust management	Multi-Agent Reinforcement Learning (MARL), Deep Q-Network, PQC (Kyber/NTRU)	94.3% Anomaly Detection Accuracy; 35% better poisoning defense
[25]	PQS-BFL	Smart Grid architecture	95% probability

In: Interpretable cognitive Internet of things for healthcare. Cham: Springer International Publishing; 2023. p. 57-72.

[2] 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):345.

[3] Zhou Y, Li L, Zuo X, Liu Y. A multi-party authentication scheme based on aggregate certificateless signature for smart healthcare. IEEE Internet Things J. 2025.

[4] Naresh VS, Venkata Raju A, Srinivasa Rao O. Secure multiparty computation for privacy-preserving machine learning in healthcare: a comprehensive survey. Wiley Interdiscip Rev Comput Stat. 2025;17(3):e70046.

[5] Liu D, Yu G, Zhong Z, Song Y. Secure multi-party computation with secret sharing for real-time data aggregation in IIoT. Comput Commun. 2024;224:159-68.

[6] Tan KL, Chi CH, Lam KY. Secure and privacy-preserving sharing of personal health records with multi-party preauthorization verification. Wireless Netw. 2024;30(6):4773-95.

[7] Wang C, Yang Q, Shen J, Wu QJ, He D. BM-PDA: blockchain based multifunctional private-preserving data aggregation for e-health systems. IEEE Trans Dependable Secure Comput. 2025.

[8] Khan S. Secure multi-party computation for privacy preservation in big data analytics. J Big Data Privacy Manag. 2024;2(2):168-79.

[9] Geng T, Liu J, Huang CT. A privacy-preserving federated learning framework for IoT environment based on secure multi-party computation. In: 2024 IEEE Annual Congress on Artificial Intelligence of Things (AIoT); 2024 Jul. p. 117-22.

[10] Dhinakaran D, Prabaharan G, Valarmathi K, Sankar SU, Sugumar R. Safeguarding privacy by utilizing SC-Dℓ DA algorithm in cloud-enabled multi party computation. KSII Trans Internet Inf Syst. 2025;19(2):635-56.

[11] Kaminaga H, Awaysheh FM, Alawadi S, Kamm L. MPCFL: towards multi-party computation for secure federated learning aggregation. In: Proceedings of the IEEE/ACM 16th International Conference on Utility and Cloud Computing; 2023 Dec. p. 1-10.

[12] Tamilselvi P, Lathika V, Jayachitra S, Arunkumar S, Balasubramani M, Kalaichelvi V. Secure multi-party computation for collaborative data analysis in network security. In: 2024 International Conference on Intelligent and Innovative

Technologies in Computing, Electrical and Electronics (IITCEE); 2024 Jan. p. 1-5.

[13] Nigam N, Goswami S, Agarwal M. Secure multi-party computation in distributed deep learning networks. In: 2023 IEEE International Conference on ICT in Business Industry & Government (ICT-BIG); 2023 Dec. p. 1-6.

[14] Siddique AA, Boulila W, Alshehri MS, Ahmed F, Gadekallu TR, Victor N, et al. Privacy-enhanced pneumonia diagnosis: IoT-enabled federated multi-party computation in Industry 5.0. IEEE Trans Consum Electron. 2024;70(1):1923-39.

[15] Sun L, Yeng P, Fauzi MA, Khatiwada P, Yang B. Multi-party privacy policy management in the context of health monitoring: an exploratory study. In: Proceedings of the 8th International Conference on Sustainable Information Engineering and Technology; 2023 Oct. p. 523-8.

[16] Tawfik AM, Al-Ahwal A, Eldien AST, Zayed HH. PriCollabAnalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation. Cluster Comput. 2025;28(3):191.

[17] Zhang H, Feng E, Lian H. A privacy-preserving federated learning framework for healthcare big data analytics in multi-cloud environments. Spectrum Res. 2024;4(1).

[18] Maurya A, Haripriya R, Pandey M, Choudhary J, Singh DP, Solanki S, et al. Federated learning for privacy-preserving severity classification in healthcare: a secure edge-aggregated approach. IEEE Access. 2025.

[19] Hosseingholizadeh A, Rahmati F, Ali M, Liu X. Homomorphic multi-party computation for Internet of Medical Things. Peer Peer Netw Appl. 2024;17(6):4049-69.

[20] Myalil Antony D, Shaik I, Vivek BS, MA R, Gubbi J, Lodha S. Decentralized inter-hospital motor imagery detection using robust multiparty model aggregation. In: Proceedings of the 8th International Conference on Data Science and Management of Data (12th ACM IKDD CODS and 30th COMAD); 2024 Dec. p. 1-9.

[21] Mijwil MM, Ali G, Peter KS, Dhoska K, Adamopoulos I. Post-quantum secure blockchain-based federated learning framework for enhancing smart grid security. Iraqi J Comput Inform. 2025;51(2):156-223.

[22] Ar-Reyouchi D, Benali H, Jihane B, Ghoumid K, Ar-Reyouchi EM. Secure-by-design IoMT networks: a quantum-blockchain and AI framework for 6G healthcare. In: 2025 International Conference on Communication, Computing, Networking, and Control in Cyber-Physical Systems (CCNCPS); 2025 Jun. p. 244-9.

[23] Prajapat S, Kumar P, Das AK, Muhammad G. Generative AI-enabled quantum encryption algorithm for securing IoT-based healthcare application using blockchain. IEEE Internet Things J. 2025.

[24] Alandjani G. A MARL-federated blockchain-based quantum secure framework for trust management in industrial Internet of Things. Sci Rep. 2025;15(1):39149.

[25] Ali G, Peter KS, Mijwil MM, Dhoska K, Adamopoulos I. Post-quantum secure blockchain-based federated learning framework for enhancing smart grid security. Iraqi J Comput Inform. 2025;51(2).