Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Secure Medical Image Cryptanalysis with Quantum Neural Networks for IoT-Enabled Cloud Storage

G. Soniya Priyatharsini

soniya.george@dxb.manipal.edu

Manipal Academy of Higher Education

Jayalakshmi Sambandam

SRM Institute of Science and Technology

R. Kavitha

Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology

R. M Saritha

S.A Engineering College

A. Maheswari

Dr. M.G.R. Educational and Research Institute

Samia Kouki

Higher Colleges of Technology

Research Article

Keywords: Quantum Neural Networks, Federated Learning, PQC, Medical Image Security, IoT-enabled Healthcare, Secure Cloud Storage

Posted Date: April 25th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9313076/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Secure Medical Image Cryptanalysis with Quantum Neural Networks for IoT-Enabled Cloud Storage

[1]G.Soniya Priyatharsini, [2]Jayalakshmi Sambandam, [3]R.Kavitha, [4]R.M Saritha, [5]A. Maheswari and [6]Samia Kouki

1-Assistant Professor, School of Engineering and IT, Manipal Academy of Higher Education, United Arab Emirates

2- Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani, Chennai, India

3- Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Chennai. India

4- Assistant Professor, Department of Artificial Intelligence & Data Science, S.A Engineering College, Chennai, India

5- Assistant Professor, Department of Data Science and Artificial Intelligence, Dr.MGR Educational and Research Institute, Chennai, India

6-Computer Information Science Division, Higher Colleges of Technology, United Arab Emirates

Corresponding Author: Dr.G.Soniya Priyatharsini, soniya.george@dxb.manipal.edu

Abstract

The rapid development of IoT-based medical image systems has significantly changed modern healthcare systems, enabling real-time data acquisition, remote diagnosis, and efficient patient monitoring. Nevertheless, medical image communication and storage in cloud computing systems have faced critical challenges, such as security threats, privacy issues, and new security threats from quantum computing. Current solutions have primarily focused on traditional data encryption techniques, which cannot withstand new security threats and have not considered cryptanalysis and attack detection. Moreover, they have not considered privacy-preserving distributed learning, making them less effective in practical applications. In this regard, this study proposes a unified framework for medical image security, including hybrid post-quantum encryption, quantum neural network-based cryptanalysis, federated deep learning, and secure cloud storage with access control. The proposed hybrid encryption technique includes post-quantum cryptography, chaos-based diffusion, and AES-GCM for efficient data security and protection against modern security threats. A Federated Quantum Neural Cryptanalysis Network (FQNC-Net) is proposed for analyzing encrypted medical images and identifying possible attacks while maintaining data privacy among various clients. The proposed framework is tested using KiTS19, KiTS21, and KiTS23 datasets. From the experiment, the proposed model attains an accuracy of 97.84%, precision of 97.21%, recall of 96.88%, and F1-score of 97.04%, along with an attack detection rate of 98.12%. Moreover, it attains high entropy of 7.998 and low correlation of 0.0012 for the proposed encryption model. In addition, it attains efficient cloud performance with low latency of 0.82 seconds and high integrity verification rate of 99.92%. The proposed framework is highly suitable for IoT-based healthcare systems.

Keywords: Quantum Neural Networks, Federated Learning, PQC, Medical Image Security, IoT-enabled Healthcare, Secure Cloud Storage

I. Introduction

Healthcare systems have achieved continuous medical condition monitoring and diagnosis and treatment administration through the rapid development of Internet of Things (IoT) technologies which enable health providers to use connected devices and cloud systems [1]. Researchers [2], [3] have conducted extensive studies on kidney tumor analysis through medical imaging that uses the KiTS19 KiTS21 and KiTS23 datasets to help detect tumors and plan treatment [4], [5]. Organizations face major obstacles when they attempt to connect IoT systems with cloud storage because this connection leads to problems that affect both data security and medical data processing capabilities [6], [7] . Security systems need to develop advanced protection features because hackers and unauthorized users pose threats to sensitive patient data which travels through network systems [8], [9].

The traditional design of cloud-based systems depends on central systems which create single points of failure and create security risks for medical data [10], [11]. Standard encryption methods [12], [13], [14] do not provide

sufficient protection against contemporary cryptographic threats while typical machine learning systems cannot process encrypted data or analyze data from various sources [15], [16]. Federated learning enables privacy-protected distributed training but it faces difficulties with data variety and slow learning rates and less precise results when handling healthcare datasets that use non-IID data distribution [17], [18].

The paper proposes a solution to existing limitations through its introduction of a new framework which unifies a hybrid encryption system that uses post-quantum cryptography and chaos-based diffusion and AES-GCM to protect data through strong confidentiality measures while defending against sophisticated security threats. The Federated Quantum Neural Cryptanalysis Network (FQNC-Net) enables secure medical image analysis because it decrypts protected medical images while maintaining user confidentiality across multiple remote user sites. The combination of federated data balancing together with augmentation methods helps the model achieve better generalization skills while reducing the effects from non-IID data patterns.

The framework provides an advanced secure cloud storage system which guarantees quick access times and requires little space while achieving total data verification through SHA-3 cryptographic hashing. The proposed method demonstrates improved results through experimental testing on KiTS datasets which achieved 97.84% accuracy with an exceptional attack detection capability and optimal entropy results that showed minimal connection between elements. The system completes its federated environment processes with fast results while it executes its functions across cloud environments. The proposed framework establishes a complete solution which unites security and intelligent operations and efficient performance to create an ideal system for future healthcare systems that use Internet of Things technology. The key Contributions of the proposed work are as follows:

- Quantum Neural Network-based cryptanalysis framework, namely FQNC-Net, is proposed to effectively enhance the secure analysis of medical images by accurately capturing the complex patterns of the encrypted data and achieving improved detection accuracy.
- A federated learning-based distributed system is incorporated to enable the secure model training process among multiple healthcare clients, while tackling the non-IID data problem through data balancing techniques.
- A secure and efficient hybrid post-quantum encryption method is proposed, incorporating PQC, chaos-based diffusion, and AES-GCM, to ensure the high security, randomness, and resistance of the system against classical and quantum attacks.
- Secure cloud storage mechanism is proposed, ensuring optimal latency, high data integrity, and security policy enforcement in IoT-environment-based applications.
- A novel adaptive re-encryption method is proposed to ensure the long-term confidentiality and security of the data against cyber threats.

The paper is organized as follows: Section II reviews the related work in secure medical image processing, federated learning, and cloud security. The proposed framework includes system architecture and hybrid encryption model as described in Section III. The methodology describes the datasets and implementation details of the study in section IV and presents experimental results in Section V. The paper ends with Section VI which presents essential findings together with possible future research areas.

II. Related Works

The introduction of distributed healthcare systems has led to an increased interest in the development of secure methods to analyze medical images while protecting patient privacy in cloud-based Internet of Things environments. The system developed by Huang et al. [19] which combines federated learning with FedAMP allows multiple systems to work together by using its attentive message passing system to handle non-IID data. Reisizadeh et al. [20] developed FedPAQ which uses quantization and periodic aggregation to enhance communication performance between devices. Reddi et al. [21] created FedAdam and FedYogi as adaptive optimization methods which improve convergence speed according to their work. Wang et al. [22] created FedMA which enables deep neural network systems to work together through its structured aggregation method. The methods developed by the researchers focus on optimizing processes and improving communication performance but they do not provide effective methods to safeguard medical image data against unauthorized access in cloud-based Internet of Things environments.

The existing medical image analysis system requires new learning methods to solve problems caused by different system components and changes in model performance over time. MOON which Li et al. [23] developed uses contrastive learning to create connections between local and global system representations. SCAFFOLD which Karimireddy et al. [24] developed uses control variates to maintain stable system operation during the training process. Zhang et al. [25] created a personalized federated learning system which enables clients to adjust their training model using specific client relevance and similarity information. The methods enhance learning results but they require extra processing power and do not have the necessary security systems which need to protect medical images in IoT-cloud environments according to Table 1.

The latest studies demonstrate that healthcare distributed learning systems require security trust explainability elements for successful operation. The researchers Kumar et al. [26] established a secure artificial intelligence framework which uses blockchain technology smart contracts and explainable models for detecting intrusions in distributed systems. The method improves security and system visibility but it makes the system more complicated and slower which limits its use for medical images that require immediate processing and their safe storage. Existing methods depend on traditional machine learning methods because they have not yet adopted new technologies like quantum neural networks which provide better encryption security and advanced cryptanalysis capabilities.

The research of Jayan and Islam [27] and Arezoomand and Ghasemi [28] investigates specific theoretical and material science problems which include density functional theory optimization and graph-theoretic analysis but these techniques cannot be used in secure medical image processing. The existing research has a significant gap because current frameworks only support secure cryptanalysis and efficient cloud storage and intelligent medical image processing in IoT medical image processing environments. The FQNC-Net model handles the urgent requirement for an improved framework which combines quantum neural networks with secure federated systems to provide strong encryption and effective data processing and accurate medical image analysis.

Table 1: Comparative Analysis of State-of-the-Art Federated Learning Models and Their Limitations

Reference	Model	Advantages	Dataset Used	Limitations
Huang et al., [19]	FedAMP	Handles non-IID via attention-based collaboration	CIFAR-10, FEMNIST	High communication cost
(Reisizadeh et al. [20]	FedPAQ	Communication-efficient with quantization	MNIST, CIFAR	Accuracy trade-off due to compression
Reddi et al., [21]	FedAdam/FedYogi	Faster convergence using adaptive optimizers	CIFAR-10, Shakespeare	Sensitive to hyperparameters
Wang et al., [22]	FedMA	Layer-wise matching improves deep models	CNN/LSTM datasets	Complex aggregation process
Li, He and Song, [23]	MOON	Reduces client drift via contrastive learning	CIFAR-100, Tiny-ImageNet	Increased computation overhead
Karimireddy et al., [24]	SCAFFOLD	Controls variance in heterogeneous data	Synthetic + real datasets	Requires control variates
Zhang et al., [25]	Personalized FL	Client-specific optimization	Multiple benchmark datasets	Increased model complexity
Kumar et al., [26]	Secure FL + XAI	Strong security + explainability	N-BaIoT, DT dataset	Higher system overhead
Jayan and Islam [27]	DFT Model	Strong material-level optimization	Simulation datasets	Not suitable for FL environments
Arezoomand and Ghasemi, [28]	Graph Model	Theoretical robustness	Graph datasets	Not applicable to ML tasks

2.1 Research Gap

The field of federated learning for distributed systems has achieved substantial advancements yet it still faces crucial constraints which prevent complete protection of medical image processing operations. The research [19] and [20] provides solutions which enhance collaborative research yet their work fails to establish methods which protect critical medical imaging data during transmission through IoT-cloud systems. The research [21] and [22] examines optimization techniques together with model aggregation methods yet their work lacks encryption mechanisms which protect data during both transmission and storage processes. The research developed by Li et al. [23] together with Karimireddy et al. [24] attempts to solve problems related to data heterogeneity and unstable training processes, yet their solutions create new demands for processing power while they fail to include specific security measures designed for protecting healthcare information.

The implementation of personalized security frameworks in real-world medical imaging applications demonstrates clear operational deficiencies. Zhang et al. [25] proposes personalized federated learning but overlooks secure storage and cryptanalysis requirements in cloud-based systems. The integration of blockchain technology with explainable AI by Kumar et al. (2024) enhances security capabilities, but the resulting system becomes more complex and slower which hinders its use in processing medical images in real time. None of these methods use contemporary technologies such as quantum neural networks to enhance their cryptographic security and processing power. The existing gaps create a requirement for a comprehensive framework which integrates secure cryptanalysis with low-power computations and intelligent learning capabilities to support IoT-based medical imaging systems that operate in cloud environments.

III. Proposed Methodology

3.1 System Overview

The proposed framework presents a secure, intelligent, and privacy-preserving medical image processing system designed for IoT-enabled cloud environments. The system uses a combination of hybrid post-quantum encryption and Quantum Neural Network (QNN)-based cryptanalysis and federated deep learning and secure cloud storage mechanisms to create an architecture which protects data through complete security measures while defending against sophisticated cyber threats. The complete process starts with medical image collection from IoT-enabled imaging devices which undergo preprocessing to create standardized data. The processed images are then secured using a hybrid encryption scheme which combines post-quantum cryptographic techniques with chaos-based encryption to create protection against both classical and quantum attacks as shown in the Figure 1.

The Quantum Neural Network (QNN)-based cryptanalysis engine evaluates encryption strength while detecting vulnerabilities and identifying potential attack patterns. The security evaluation module calculates a quantitative security score which enables the system to activate adaptive re-encryption when it detects weaknesses in the system. The framework uses Federated Deep Learning (FDL) model to protect data privacy while providing scalable learning because multiple IoT devices train the system without sharing actual medical information. The decentralized method protects data privacy while resulting in better model performance through distributed system testing. The secured data undergoes transmission to the cloud where it gets stored through a multi-layer security system which uses encrypted communication protocols and integrity verification and role-based and attribute-based access control policies.

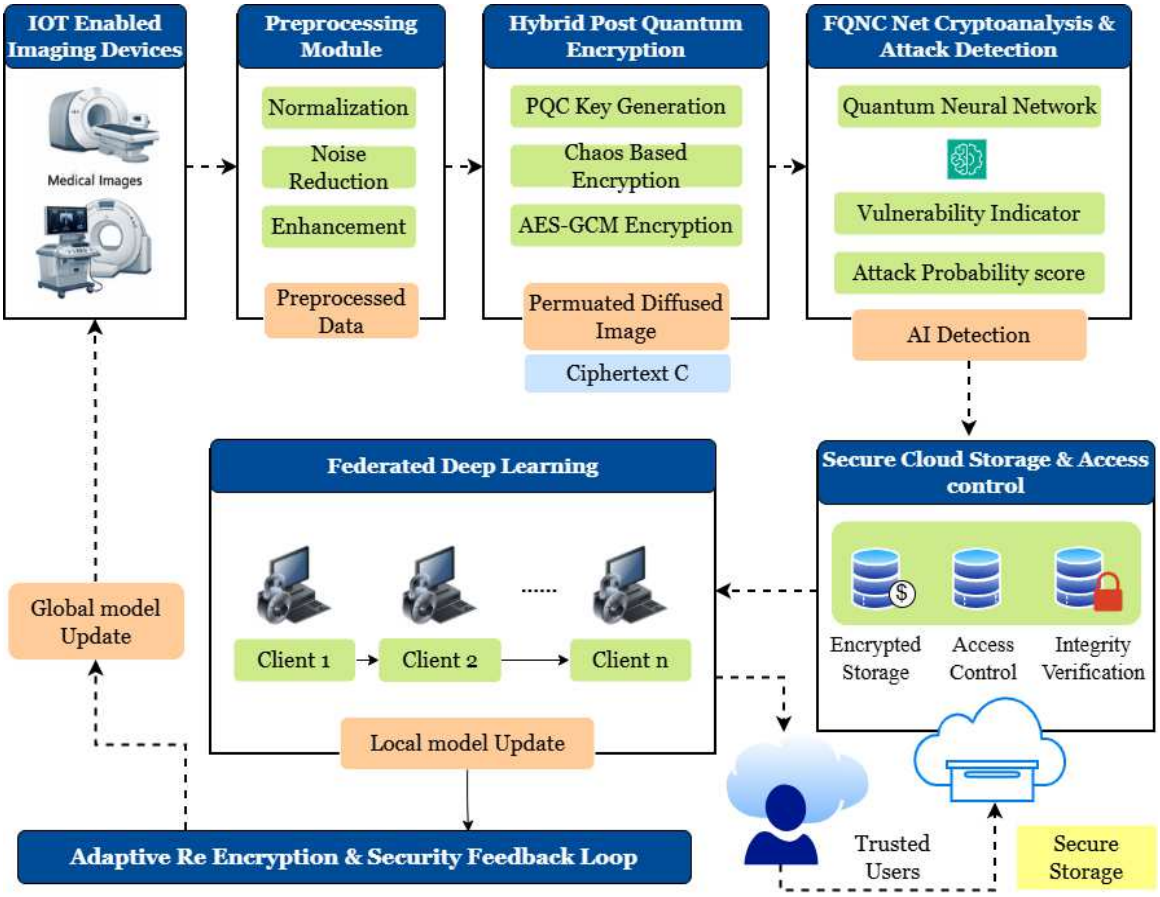


Figure 1: System Architecture for Secure Medical Data Management using Adaptive Re-Encryption and AI-Driven Attack Detection

The proposed framework uses complete preprocessing methods and hybrid post-quantum encryption to produce secure medical image results which maintain no visual noise and complete cryptographic protection before conducting further assessment. The current stage establishes essential security measures which protect against all unauthorized entry attempts and data breaches and quantum-based security threats.

3.2 Hybrid Post-Quantum Encryption Framework

The encryption process and subsequent processing activities experience negative effects because medical images obtained from IoT-enabled devices display both different characteristics and multiple sound disturbances and different picture quality levels. The hybrid encryption model serves as the section's main component because it combines Post-Quantum Cryptography (PQC) with Chaos-Based Encryption and Symmetric Encryption (AES-GCM). The system uses a layered design that provides security from multiple directions which makes it extremely difficult for attackers to breach the system.

3.2.1 Post-Quantum Key Generation

The researchers have chosen Post-Quantum Cryptography (PQC) as their main method for creating and sharing secure keys since it protects against all upcoming quantum computer threats which will emerge in the future of digital security. The system uses a latticebased Key Encapsulation Mechanism (KEM) to establish a shared secret key which connects IoT devices to the cloud server. The process starts with the creation of a public-private key pair (pk, sk) based on the security parameter λ which allows the sender to encapsulate a session key K through the public key using the formula $(ct, K) = \text{Encaps}(pk)$. The receiver then retrieves the same key using decapsulation $K = \text{Decaps}(sk, ct)$. The system protects the key K from attackers who acquire the ciphertext ct because solving lattice problems remains an impossible task for them. The proposed system uses the quantum-resistant key K to secure subsequent encryption processes which establish a future-proof key management system that safeguards medical images sent between IoT devices and cloud environments as illustrated in Figure 2.

To ensure quantum resistance, a lattice-based key generation mechanism is used as it was represented in the Eq. (1-3):

Key Generation:

$$(pk, sk) = \text{KeyGen}(\lambda) \tag{1}$$

Encapsulation:

$$(ct, K) = \text{Encaps}(pk) \tag{2}$$

Decapsulation:

$$K = \text{Decaps}(sk, ct) \tag{3}$$

Where $K \in \{0,1\}^k$ is the shared secret key and λ is the security parameter

This ensures:

Resistance to Shor's algorithm

Future-proof encryption

3.2.2 Chaos-Based Confusion and Diffusion

After the completion of key generation, the processed medical image undergoes chaos-based encryption which uses nonlinear dynamic systems to create extreme randomization that produces strong confusion and diffusion effects. A logistic chaotic map defined by $x_{n+1} = rx_n(1 - x_n)$, where $r \in (3.57,4)$, uses the parameter range of r∈(3.57,4) to create pseudo-random sequences. The sequences exhibit high sensitivity towards initial conditions which makes them ideal for use in encryption. The proposed method uses generated chaotic values to change pixel positions which results in the creation of I_{perm} , an image that disrupts spatial connections between neighboring pixels. The process uses bitwise XOR operations to change pixel brightness through a diffusion process: $I_{\text{diff}}(i,j) = I_{\text{perm}}(i,j) \oplus f(x_n)$, where $f(x_n)$ represents quantized chaotic values. The dual process creates strong protection against statistical, differential, and brute-force attacks because minor input image changes result in major encrypted output variations. The work uses chaosbased encryption as a pre-encryption layer which enhances pixel security before the application of standard cryptographic methods.

To enhance image-level security, chaotic systems are used as it was represented in the Eq. (4-7).

Logistic Map for Chaos Generation

$$x_{n+1} = rx_n(1 - x_n) \tag{4}$$

Where $r \in (3.57,4)$, $x_0 \in (0,1)$ Pixel Permutation (Confusion)

The generated chaotic sequence is used to shuffle pixel positions:

$$I_{\text{perm}}(i,j) = I_p\big(\pi(i,j)\big) \tag{5}$$

where π is a permutation function derived from the chaotic sequence.

Pixel Diffusion

Pixel values are modified using:

$$I_{diff}(i,j) = I_{perm}(i,j) \oplus f(x_n) \tag{6}$$

Where $\oplus$ denotes XOR operation, $f(x_n)$ is a quantized chaotic value

Output of Chaos Encryption

$$I_c = I_{diff} \tag{7}$$

This stage ensures: High entropy, Low pixel correlation, Resistance to statistical attacks

3.2.3 AES-GCM Encryption Layer

The Advanced Encryption Standard in Galois/Counter Mode operates with high-performance secure encryption through its processing of chaos-encrypted images. The chaos-encrypted image I_c is encrypted using the session

key K obtained from the PQC layer, producing the final ciphertext $C = \text{Enc}_{\text{AES-GCM}}(I_c, K, IV)$, where IV is a randomly generated initialization vector. AES-GCM not only ensures confidentiality but also provides built-in authentication through the generation of an authentication tag Tag which verifies the integrity and authenticity of the encrypted data during decryption. The system blocks all unauthorized access attempts because any change to the ciphertext prevents authentication from succeeding. The proposed framework uses AES-GCM as its last encryption method because it delivers high operational efficiency while maintaining robust security protection. The system implements a multi-layer hybrid encryption system that protects medical image confidentiality and data integrity while enabling secure transmission and storage in IoT-enabled cloud environments through its combination of PQC and chaos-based encryption methods.

The chaos-encrypted image is further secured using AES-GCM as it was represented in the Eq. (8 and 9):

$$C = \text{Enc}_{AES}(I_c, K, IV) \tag{8}$$

Where IV is a random initialization vector

GCM Authentication Tag

$$Tag = \text{Auth}(C, K) \tag{9}$$

This ensures Data integrity

Authentication

Hash-Based Integrity Verification

To guarantee data integrity was expressed as in the Eq. (10):

$$H = \text{SHA3} - 256(C) \tag{10}$$

Verification condition was expressed as in the Eq. (11):

$$H_{\text{received}} = H_{\text{computed}} \tag{11}$$

Unified Hybrid Encryption Model

The entire encryption pipeline can be mathematically expressed as in the Eq. (12):

$$C = E_{\text{AES}}\left(E_{\text{Chaos}}\left(I_p\right), K\right) \tag{12}$$

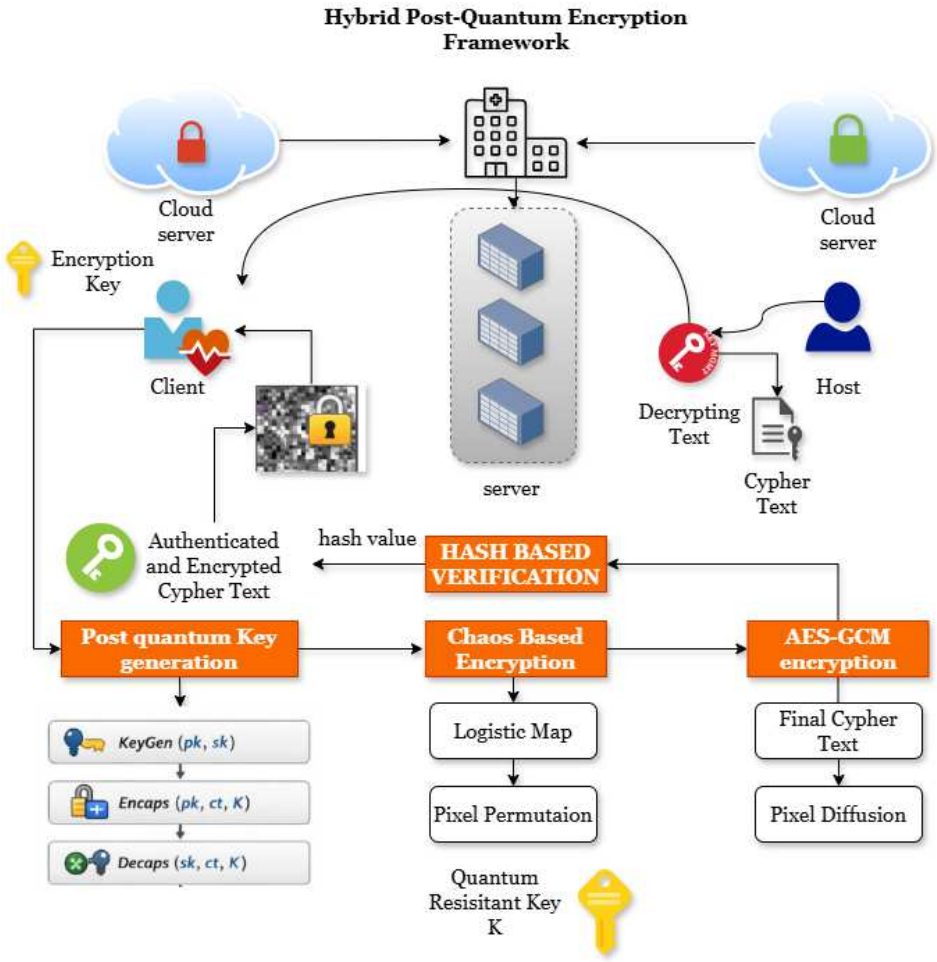


Figure 2: Architecture of the Chaos-Based and AES-GCM Hybrid Encryption Framework

3.2.4 Security Strength Analysis and Final Encrypted Data Structure

The security strength of the proposed hybrid encryption model is evaluated through multiple statistical tests and differential measurements which assess its performance against different types of attacks. The encrypted image randomness is measured through entropy which shows that higher values produce more unpredictable and secure ciphertext according to the equation. The correlation analysis method tests how adjacent pixels in the encrypted image relate to each other because a low correlation value shows that the encryption method successfully eliminated all spatial dependencies which existed in the original medical image according to the equation. The Number of Pixel Change Rate NPCR function assesses how many pixels change between two encrypted images which result from minor input modifications because this metric shows how the system responds to small changes and its ability to withstand differential attacks according to the equation. UACI Unified Average Changing Intensity measures how much two images differ in average intensity which shows how effectively pixels spread across the image according to the equation. The metrics demonstrate that the encryption scheme achieves complete randomness with minimal data redundancy while maintaining strong protection against statistical and differential attacks. The final encrypted data is structured as a secure package which includes the ciphertext, encrypted key, initialization vector, authentication tag, and hash value to protect data during cloud environment transmission and storage through confidentiality and integrity and authentication mechanisms. Entropy, Correlation, NPCR and UACI as it was expressed from the Eq. (13- 17):

$$E = -\sum_{i=0}^{255} p(i)\log_2 p(i) \tag{13}$$

$$\text{Corr} = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x \sigma_y} \tag{14}$$

$$NPCR = \frac{\sum D(i,j)}{m \times n} \times 100 \tag{15}$$

$$UACI = \frac{1}{m \times n} \sum \frac{|C_1 - C_2|}{255} \times 100 \quad (16)$$

Final Encrypted Data Structure

$$D = \{C, K_{enc}, IV, Tag, H\} \quad (17)$$

Algorithm 1: Hybrid Post-Quantum Encryption for Medical Images

Input: Preprocessed medical image I_p, security parameter λ
Output: Encrypted data package $D = \{C, K_{\text{enc}}, IV, Tag, H\}$

//Step 1: Post-Quantum Key Generation
Generate lattice-based key pair: $(pk, sk) \leftarrow \text{KeyGen}(\lambda)$
Encapsulate session key: $(ct, K) \leftarrow \text{Encaps}(pk)$
Decapsulate at receiver: $K \leftarrow \text{Decaps}(sk, ct)$
//Step 2: Chaos-Based Confusion and Diffusion
Initialize logistic map: $x_0 \in (0,1), r \in (3.57,4)$
Generate chaotic sequence: $x_{n+1} - rx_n(1 - x_n)$
Pixel permutation (confusion): $I_{\text{perm}}(i,j) - I_p(\pi(i,j))$ // Pixel permutation
Pixel diffusion: $I_c(i,j) - I_{\text{perm}}(i,j) \oplus f(x_n)$ // Pixel diffusion using XOR
Step 3: AES-GCM Encryption Layer
Generate random initialization vector: IVEncrypt chaos-encrypted image: $C, Tag \leftarrow$ AES GCM_Encrypt (I_c, K, IV)
//Step 4: Hash-Based Integrity Verification
Compute hash: $H \leftarrow$ SHA3-256 (C)
//Step 5: Construct Final Encrypted Package
$D \leftarrow \{C, K_{\text{enc}} = ct, IV, Tag, H\}$
//Step 6: Optional Security Metrics
Entropy: $E = -\sum_{i-0}^{255} p(i) \log_2 p(i)$
Correlation: Corr $= \frac{E[(x-\mu_z)(y-\mu_y)]}{\sigma_x \sigma_y}$
NPCR: NPCR $= \frac{\sum D(i,j)}{m \cdot n} \times 100$
UACI: ← (1 / (m*n)) * Σ |C1 - C2| / 255 * 100
Return n

3.3 QNN-Based Cryptanalysis and Attack Detection

The proposed framework introduces a new hybrid quantum-classical system which researchers named the Federated Quantum Neural Cryptanalysis Network (FQNC-Net). This system uses intelligent cryptanalysis to detect attacks on encrypted medical images. This model assesses the encryption strength of encrypted data while discovering security weaknesses through its active analysis of encrypted data. The first step of the process changes the encrypted image into a quantum-compatible format which represents pixel intensities as quantum states. The model uses quantum computing principles to find data patterns which classical methods cannot identify.

Quantum State Encoding

The quantum state representation of the encrypted image $C \in \mathbb{R}^{m \times n}$ first requires conversion from its original form. Each pixel intensity is encoded into a rotation angle as it was expressed in the Eq. (18):

$$\theta_{ij} = \pi \cdot C(i,j) \quad (18)$$

The corresponding quantum state is expressed as in the Eq. (19):

$$|\psi_{ij}\rangle = \cos\left(\frac{\theta_{ij}}{2}\right)|0\rangle + \sin\left(\frac{\theta_{ij}}{2}\right)|1\rangle \quad (19)$$

The total image content creates a combined quantum system as it was expressed in the Eq. (20):

$$|\Psi\rangle = \otimes_{i,j} \ |\psi_{ij}\rangle \tag{20}$$

The FQNC-Net quantum component includes parameterized quantum circuits which execute superposition and rotation and entanglement operations. The model uses these operations to uncover the essential structural and statistical characteristics hidden in the encrypted image which contain patterns that show weak encryption and attack behaviors. The quantum layer output materializes as classical feature vectors which measurement converts before passing to a deep learning network that uses convolutional layers. The system uses hybrid design because it combines quantum computing power with classical neural network strength to achieve precise and effective cryptanalysis results.

Quantum Feature Extraction The parameterized quantum circuit processes the encoded state through its quantum data processing as it was expressed in the Eq. (21):

$$|\Psi'\rangle = U(\theta)|\Psi\rangle \tag{21}$$

The sequence of quantum gates in U(θ) includes the following components:

- Hadamard gates H
- Rotation gates $R_y(\theta), R_z(\theta)$
- Controlled-Z (CZ) entanglement gates

The hidden correlations in encrypted data become visible through these operations. Measurement and Classical Mapping The quantum state undergoes measurement to produce classical feature vectors as it was expressed in the Eq. (22):

$$z_k = \langle\Psi'|M_k|\Psi'\rangle \tag{22}$$

The measurement operators are represented by M_k. The resulting feature vector as it was expressed in the Eq. (23):

$$\mathrm{z} = [z_1, z_2, \ldots, z_d] \tag{23}$$

The classical neural network receives this vector for additional processing. Cryptanalysis Objective The FQNC-Net aims to estimate the probability of key inference given the ciphertext as it was expressed in the Eq. (24):

$$\hat{K} = \arg\max_K P(K \mid C) \tag{24}$$

The model assesses vulnerability through its ability to learn patterns from encrypted data distribution. Attack Detection Model The model identifies different attack types by calculating the probability of an attack occurring as it was expressed in the Eq. (25):

$$P(A \mid C) = \mathrm{Softmax}(f(\mathrm{z})) \tag{25}$$

Where $f(\mathrm{z})$ is the output of the classical network and $A \in \{\mathrm{KPA}, \mathrm{CPA}, \mathrm{DA}, \mathrm{Adv}\}$

The FQNC-Net system works to identify and categorize various cryptographic attacks which include known-plaintext attacks and chosen-plaintext attacks and differential attacks and adversarial manipulations. The model uses its learned features to calculate key inference probabilities and detect unusual encryption behavior. The system generates an attack probability score together with a vulnerability indicator which helps assess the security status of encrypted information. The system responds to detected weaknesses by implementing security measures that include adaptive re-encryption for protection improvement.

A binary vulnerability indicator is defined as in the Eq. (26):

$$V = \begin{cases} 1, & \text{if } P(A \mid C) > \tau \\ 0, & \text{otherwise} \end{cases} \tag{26}$$

where τ is a predefined threshold.

Loss Function The model is trained using a combined loss function as it was expressed in the Eq. (27):

$$L = L_{\text{attack}} + \lambda L_{\text{security}} \tag{27}$$

Where $L_{\text{attack}} = -\sum\ y\log(\hat{y})$ (cross-entropy loss), L_{security} evaluates deviation from secure encryption patterns, λ balances both objectives

The FQNC-Net system supports federated learning because it allows multiple IoT devices to train their models while protecting user privacy. Each device trains the model locally using its own encrypted data, and only model

updates are shared with a central server for aggregation. This approach ensures that sensitive medical data is never exposed, while also improving the model's generalization capability across diverse datasets. The FQNC-Net system provides a strong and flexible solution for continuous cryptanalysis and attack detection which enhances the protection of medical image storage and transmission in IoT-enabled cloud environments. Within the federated framework, each client updates local model parameters $W_{i,}$ and the global model is obtained as in the Eq. (28):

$$W_{\text{global}} = \sum_{i=1}^{N} \frac{n_i}{n} W_i \tag{28}$$

Where n_i is the number of samples at client i, n is the total number of samples

The model produces:

- Predicted key probability $\hat{K}$
- Attack probability $P(A \mid C)$
- Vulnerability indicator V

These outputs are used to trigger security decisions such as re-encryption.

Algorithm 2: FQNC Net Cryptanalysis(D_i, θ, τ)

Input: Local encrypted dataset D_i at client i, quantum circuit parameters θ, attack threshold τ
Output: Attack probability P(A|C), vulnerability indicator V, predicted key K̂

1: for each encrypted image C ∈ D_i do
2: // Step 1: Quantum State Encoding
3: for each pixel C(i,j) do
4: $\theta_{ij} \leftarrow \pi \cdot C(i,j)$
5: |ψ_ij⟩ ← cos(θ_ij/2)|0⟩ + sin(θ_ij/2)|1⟩
6: end for
7: |Ψ⟩ ← ⊗_{i,j} |ψ_ij⟩ // Composite quantum image state

8: // Step 2: Quantum Feature Extraction
9: |Ψ'⟩ ← U(θ)|Ψ⟩ // Apply parameterized quantum gates: H, R_y (θ), R_z (θ), CZ
10: Measure quantum state to obtain classical feature vector:
11: z = [⟨Ψ'|M_1|Ψ'⟩, ⟨Ψ'|M_2|Ψ'⟩, …, ⟨Ψ'|M_d|Ψ'⟩]

12: // Step 3: Classical Neural Network Processing
13: f(z) ← CNN(z) // Convolutional layers + fully connected
14: P(A|C) ← Softmax (f(z)) // Attack probability for A ∈ {KPA, CPA, DA, Adv}
15: V ← {1 if max(P(A|C)) > τ; 0 otherwise} // Vulnerability indicator
16: K̂ ← argmax P(K|C) // Predicted key probability
17: end for

18: // Step 4: Federated Learning Aggregation
19: Send local model updates W_i to central server
20: Server aggregates global model:
21: W_global ← Σ_{i=1}^N (N_i/ n) W_i
22: Broadcast W_global back to clients
23: Clients update local parameters: $W_i \leftarrow$ W_global

24: return P(A|C), V, K̂

3.4 Federated Deep Learning Framework

The proposed framework incorporates a Federated Deep Learning (FDL) model to enable privacypreserving training across multiple loT-enabled medical imaging devices. The IoT system enables each client to conduct local model training using its encrypted data while sending only model updates to the central server for

aggregation purposes. The system design protects patient data from potential breaches while achieving better results across different types of data and meeting current healthcare privacy standards. The local dataset at client i consists of $D_i = \{(x_j^i, y_j^i)\}_{j=1}^{n_i}$, where x_j^i represents the processed and encrypted medical image and y_j^i shows the corresponding label or target.

Local Model Training: The client system operates with a local model$f(x; W_i)$, where W_i are the trainable weights. Local training minimizes a loss function $L_i(W_i)$, which combines prediction accuracy with security constraints derived from the QNN-based cryptanalysis module as it was expressed in the Eq. (29):

$$L_i(W_i) = L_{\text{task}}\left(f(x; W_i), y\right) + \lambda L_{\text{security}}\left(f(x; W_i)\right) \tag{29}$$

Here, L_{task} is typically cross-entropy loss for classification or MSE for regression, and L_{security} function measures how much the model deviates from secure encryption patterns which helps the model acquire privacy-preserving feature extraction skills. The hyperparameter λ enables the system to find the ideal balance between task performance and security requirements. The client system performs weight updates through stochastic gradient descent (SGD) or an adaptive optimizer as it was expressed in the Eq. (30):

$$W_i^{t+1} = W_i^t - \eta \nabla_{W_i} L_i(W_i^t) \tag{30}$$

The learning rate is represented by η while t indicates the current local iteration process.

Federated Aggregation: Clients send their weight differences ΔW_i to the central server after completing local updates. The server combines these updates to create a global model through weighted averaging which operates as it was expressed in the Eq. (31):

$$W_{\text{global}}^{t+1} = \sum_{i=1}^{N} \frac{n_i}{n} W_i^{t+1}, n = \sum_{i=1}^{N} n_i \tag{31}$$

where n_i represents client i's sample count whereas N stands for total client count and n denotes complete dataset volume. The approach lets clients with larger datasets control the global model based on their actual data size which leads to better model training results and less bias because of uneven data distribution as shown in Figure 3.

Privacy-Preserving Enhancements: The framework uses secure aggregation along with differential privacy to improve its privacy protection capabilities. Clients add small noise vectors $\mathcal{N}(0, \sigma^2)$ to their updates before sending them out as it was expressed in the Eq. (32):

$$\tilde{W}_i = W_i + \mathcal{N}(0, \sigma^2) \tag{32}$$

The server aggregates $\tilde{W}_i$ instead of raw weights which prevents any individual client's data from being reconstructed through the shared updates. The system uses homomorphic encryption and secure multiparty computation to protect ΔW_i with quantum-resilient privacy security for IoT applications. Communication Rounds and Convergence The federated training process uses communication rounds as its operational framework.

Clients execute E local training epochs during each round before they send their updates and receive the latest global model as it was expressed in the Eq. (33):

$$W_i^{t+1} = W_{\text{global}}^t \tag{33}$$

The global loss across all clients serves as the basis for convergence assessment as it was expressed in the Eq. (34):

$$L_{\text{global}}\left(W_{\text{global}}^t\right) = \sum_{i=1}^{N} \frac{n_i}{n} L_i(W_i^t) \tag{34}$$

Training continues until L_{global} drops below a defined limit ϵ or until the system reaches its maximum communication round limit T. The system uses the global model W_{global} to perform real-time inference on encrypted medical images.

Integration with QNN-Based Cryptanalysis: Integration with QNN-Based Cryptanalysis The FDL framework functions as a complete system which works together with the QNN-based cryptanalysis engine. The server checks model output security through FQNC-Net after each global aggregation as it was expressed in the Eq. (35):

$$V_{\text{global}} = \text{QNN}\left(C_{\text{encrypted}}, W_{\text{global}}\right) \tag{35}$$

where V_{global} is the vulnerability indicator. If $V_{\text{global}} > \tau$, as a vulnerability indicator. The system activates its two security features when V_{global} exceeds the threshold value. The federated model achieves two goals through the

feedback loop which creates accurate predictions and secure medical image data in a distributed IoT cloud environment.

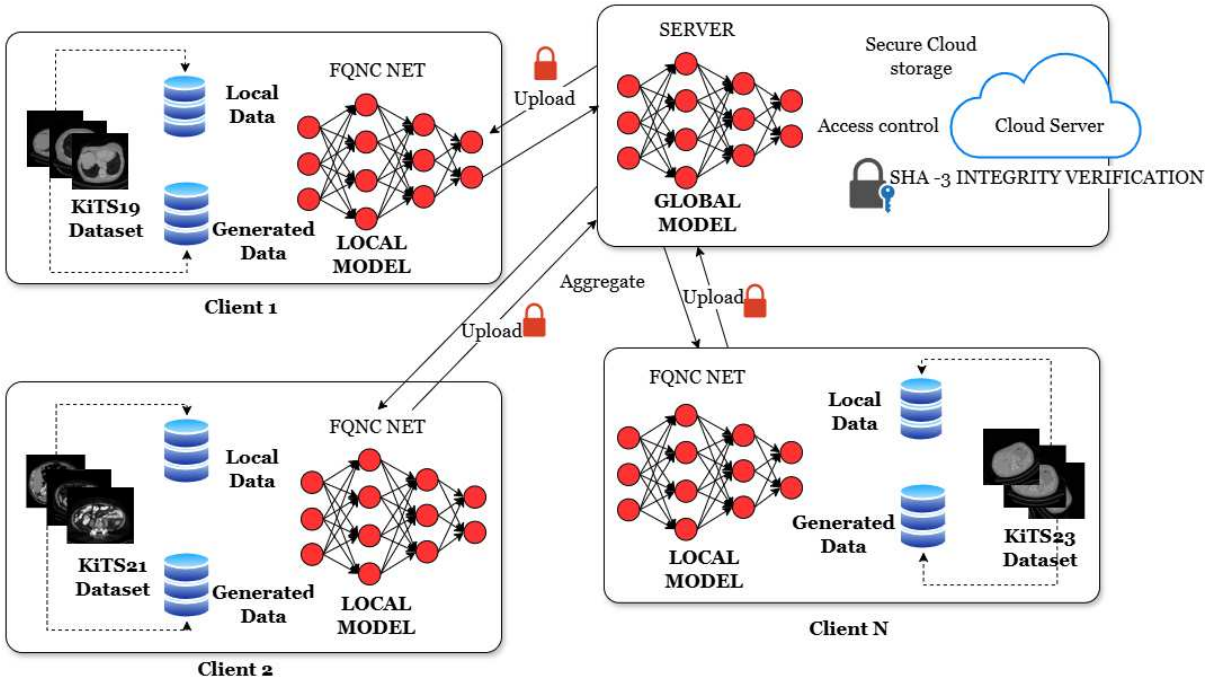


Figure 3: Federated Learning Architecture for Distributed FQNC-Net Training

3.5 Security Evaluation and Adaptive Re-Encryption

The proposed framework uses a security evaluation module which performs quantitative tests to measure the encryption strength of medical images. The module computes statistical metrics such as entropy, pixel correlation, NPCR (Number of Pixel Change Rate), and UACI (Unified Average Changing Intensity). High entropy values indicate greater randomness in the ciphertext, while low correlation between adjacent pixels confirms effective spatial decorrelation. The NPCR and UACI metrics show how input image changes affect system performance through their measurement of system response to moderate input changes. The mathematical representation of these metrics is expressed through the following Eq. (36- 38):

$$\text{Entropy: } E = -\sum_{i=0}^{255} p(i)\log_2 p(i) \tag{36}$$

$$\text{Correlation: Corr } = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x \sigma_y} \tag{37}$$

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100, \text{UACI} = \frac{1}{m \times n}\sum_{i,j} \frac{|C_1(i,j)-C_2(i,j)|}{255} \times 100 \tag{38}$$

Here, $D(i,j)$ shows how two encrypted images, C_1 and $C_2, m \times n$ is the image dimension, and $p(i)$ differ from each other in their encrypted form while their image size is represented by m×n and p(i) show the likelihood of finding a specific pixel value at the i-th position. The system uses adaptive re-encryption to protect itself from security breaches which are identified through vulnerability assessments and low security score evaluations. The security score S of an encrypted image reaches its computed value through the calculations. The system re-encrypts the image using new encryption keys and changed encryption settings when its security score S falls below the established threshold value τ as it was expressed in the Eq. (39):

$$C' = \text{Encrypt}(I_p, K', \text{IV}') \tag{39}$$

where C' is the updated ciphertext, K' as the newly created session key that was created through post-quantum key encapsulation and IV' as the new initialization vector. The system uses a dynamic feedback system to maintain security as it stops attackers from using weak ciphertexts to access confidential medical images which remain protected through their continuous secure storage in IoT cloud services.

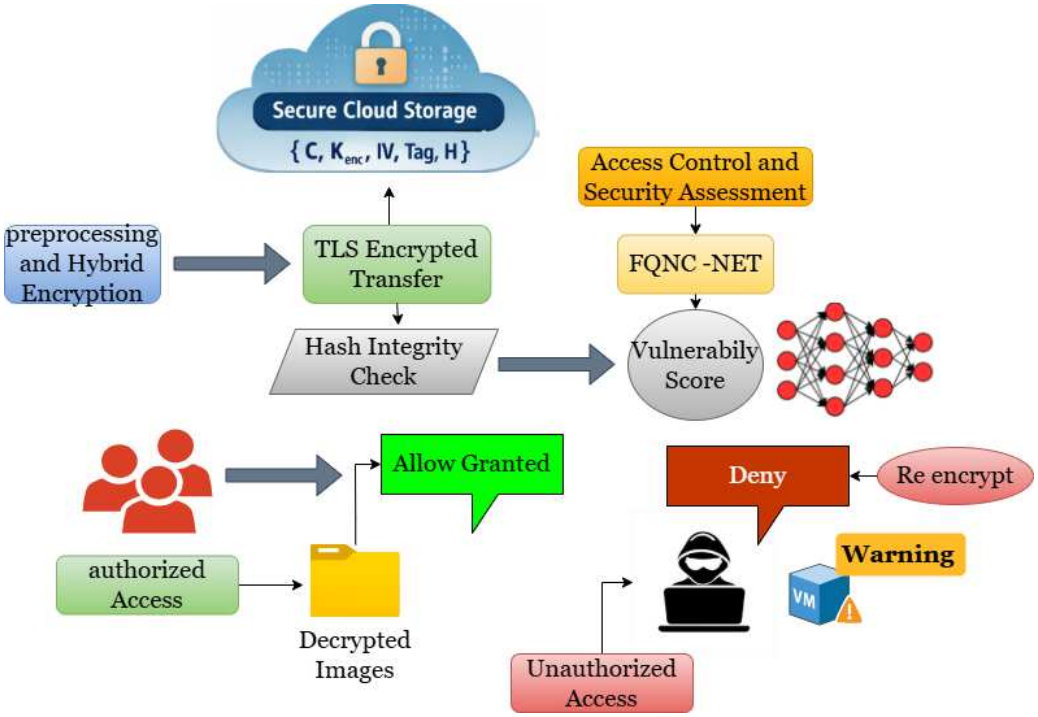


Figure 4: Architecture for Secure Cloud Storage and Access Control Mechanism

3.5.1 Secure Cloud Storage and Access Control

The proposed framework employs a multi-layer secure cloud storage system to ensure confidentiality, integrity, and availability of medical images transmitted from loT devices. The preprocessed images undergo encryption through the hybrid post-quantum and chaos-based system before their transmission to the cloud through encrypted communication channels which use TLS 1.3 protocols as shown in the Figure 4. The encrypted data package $D = \{C, K_{\text{enc}}, IV, Tag, H\}$ is stored in the cloud along with its associated authentication tags and hash values, allowing verification of data integrity upon retrieval. The system uses hash-based integrity checks to verify data security which involves comparing stored hash H_{cloud} against computed hash H_{computed} during user access to identify any system changes as it was expressed in the Eq. (40):

$$H_{\text{cloud}} \stackrel{?}{=} H_{\text{computed}} \tag{40}$$

Any discrepancy triggers an alert which starts adaptive re-encryption to protect against both internal and external security threats. The framework controls access through its system which combines Role-Based Access Control (RBAC) with Attribute-Based Access Control (ABAC) to create detailed authorization rules. The system grants access to users after they receive roles R_u and attributes A_{ur} awhich match the requirements of specific access policies as it was expressed in the Eq. (41):

$$\text{Access}(u, C) = \begin{cases} \text{ALLOW}, & \text{if } R_u \cap R_C \neq \emptyset \text{ and } A_u \vDash P_C \\ \text{DENY}, & \text{otherwise} \end{cases} \tag{41}$$

where R_C and P_C represent the roles and policy conditions required for accessing ciphertext C. The system allows authorized clinicians researchers and IoT services to access sensitive medical data which decreases the chances of data breaches and insider threats. The secure cloud storage layer works together with both federated QNN and adaptive reencryption components. The system applies security evaluation through FQNC-Net which determines access rights based on calculated vulnerability score V that must meet security threshold τ for data access as it was expressed in the Eq. (42):

$$\text{Access Decision} = \begin{cases} \text{GRANTED}, & V \leq \tau \\ \text{RE-ENCRYPT}, & V > \tau \end{cases} \tag{42}$$

The system uses a security feedback loop that protects medical images from new threats while allowing controlled access to IoT-based medical applications which protect user privacy. The cloud storage system achieves robust security through its combination of hybrid encryption, integrity verification, access control, and adaptive reencryption which protects against quantum threats and meets current healthcare security requirements.

IV. Dataset and Implementation Details

4.1 Dataset and Preprocessing

4.1.1 KiTS19 Dataset

The Kidney Tumor Segmentation Challenge 2019 KiTS19 dataset [29] functions as a standard evaluation tool for medical imaging research which especially targets the detection and segmentation of kidney tumors. The dataset comprises abdominal CT scans, which have undergone contrast enhancement and were obtained from various clinical centers to create a dataset that contains diverse imaging conditions and patient demographic information. The dataset contains 210 patient cases which have been manually labeled to show the presence of kidneys and kidney tumors, thus enabling supervised learning while evaluating medical imaging systems.

The 3D volumetric format presents each scan, which includes multiple resolutions and slice thickness options, that demonstrates the actual clinical variations. The dataset provides ground truth segmentation masks which permit researchers to conduct both classification and segmentation studies. Researchers use KiTS19 as a framework to test encryption security while assessing QNN-based cryptographic attack methods on different types of medical imaging datasets.

4.1.2 KiTS21 Dataset

The Kidney Tumor Segmentation Challenge 2021 KiTS21 dataset [30] serves as an upgraded version of KiTS19 which delivers better annotation quality and consistent annotation processes. The dataset includes 300 CT scan cases, which contain both tumor-bearing and healthy kidney samples, and comes with expert annotations of high quality. The dataset provides better label accuracy through standardized preprocessing methods which achieve higher inter-observer consistency, thus enabling the development of advanced deep learning models.

The dataset maintains the same imaging modality (CT scans) but introduces enhanced data uniformity and annotation precision, which is beneficial for evaluating encryption consistency and model generalization. The study uses KiTS21 as a supporting element to accomplish research objectives.

4.1.3 KiTS23 Dataset

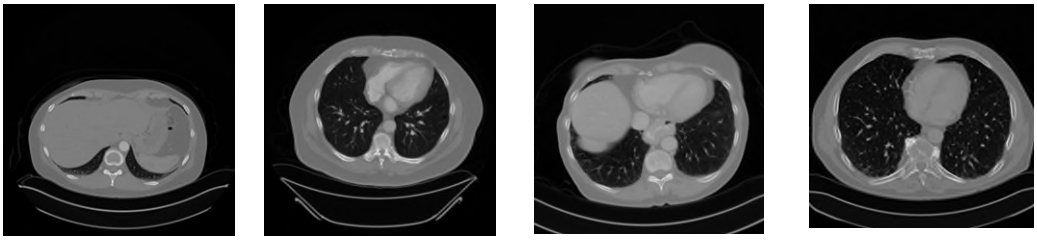
The Kidney Tumor Segmentation Challenge 2023 (KiTS23) dataset [31] functions as the most recent update of the KiTS series because it contains extensive CT image data which researchers can use to study kidney tumors. The dataset contains 489 cases which make it the largest collection yet and it presents better annotations that identify kidney areas and tumor regions and cyst areas. The dataset demonstrates the actual clinical conditions which doctors encounter because it includes different tumor dimensions and shapes and various imaging methods as shown in Table 2.

The KiTS23 dataset enables next-generation AI systems by providing high-resolution imaging data and extensive annotations which support the development of more powerful and expandable model training. The proposed framework uses KiTS23 to test the federated learning system scalability and to measure the performance of hybrid encryption and QNN-based cryptanalysis methods with complex datasets. The system uses diverse elements to establish security and privacy protection while maintaining its ability to perform well under various clinical situations.

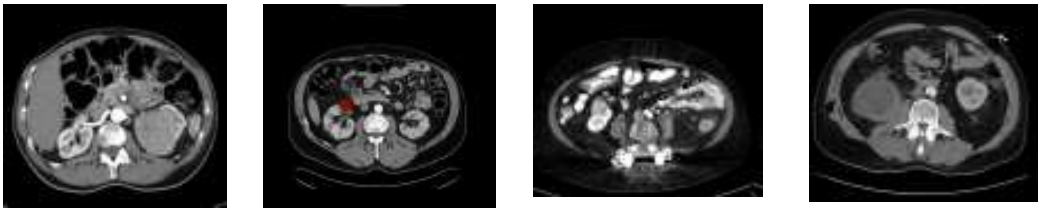
Table 2: Representative Slices of CT Scan Data for Model Training and Validation

Datasets	CT scans

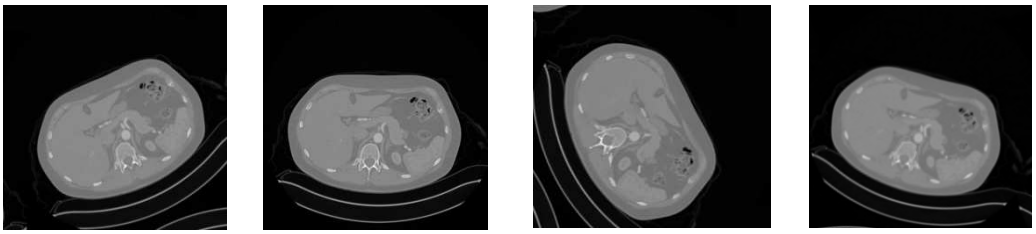
KiTS19 Dataset



KiTS21 Dataset



KiTS23 Dataset



4.1.4 Data Preprocessing

The structured preprocessing pipeline needs to be implemented because it provides the essential framework for data processing. The input image as it was expressed in the Eq. (43):

$I \in \mathbb{R}^{m \times n}$(43)

which has spatial dimensions defined by the variables m and n.

The intensity values from different scans get standardized through the application of min-max normalization as it was expressed from the Eq. (44- 50):

$$I_{\text{norm}}(i,j) = \frac{I(i,j) - \min(I)}{\max(I) - \min(I)} \tag{44}$$

This ensures:

$$I_{\text{norm}}(i,j) \in [0,1] \tag{45}$$

The process resizes all images to a standardized size:

$$I_{\text{resized}} = \mathcal{R}(I_{\text{norm}}) \tag{46}$$

Where $\mathcal{R}: \mathbb{R}^{m \times n} \rightarrow \mathbb{R}^{256 \times 256}$ Noise Reduction Using Gaussian Filtering

The process of Gaussian filtering operates as a method to eliminate acquisition noise from medical images.

$$I_{\text{smooth}}(x,y) = \sum_{i=-k}^{k} \sum_{j=-k}^{k} I_{\text{resized}}(x-i, y-j) \cdot G(i,j) \tag{47}$$

$$G(i,j) = \frac{1}{2\pi\sigma^2} e^{-\frac{i^2+j^2}{2\sigma^2}} \tag{48}$$

The process of contrast stretching improves pixel distribution through its application:

$$I_{enh}(i,j) = \frac{I_{smooth}(i,j) - a}{b - a} \tag{49}$$

where a and b represent lower and upper intensity bounds.

Final Preprocessed Image

$$I_p = I_{enh} \tag{50}$$

The processed image achieves suitability for secure encryption purposes.

4.1.5 Federated Data Partitioning

The IoT client system of the KiTS19 KiTS21 and KiTS23 data collection requires federated data distribution to maintain user privacy through its distributed learning system. The dataset D consists of medical encrypted images xi and their associated yi labels which are used as the dataset $D = \{(x_i, y_i)\}_{i=1}^{N}$, where x_i denotes the encrypted medical image and y_i represents the corresponding label. The dataset is divided into K disjoint subsets $D_{k,}$ each assigned to a client device as it was expressed in the Eq. (51):

$$D = \bigcup_{k=1}^{K} D_k, D_k \cap D_j = \emptyset \text{ for } k \neq j \tag{51}$$

Each client k locally stores its dataset $D_k = \left\{\left(x_i^k, y_i^k\right)\right\}_{i=1}^{n_k}$, where n_k denotes the number of samples at client k_r and the total number of samples is $N = \sum_{k=1}^{K} n_k$. The system keeps medical data on its original devices which prevents any data from leaving the devices thus guaranteeing patient privacy protection. The framework establishes real-world IoT healthcare system conditions through its non-IID data partitioning method which creates imbalanced data distribution between multiple clients. This distribution is described by Dirichlet distribution:

where P_k defines the class distribution for client k, and α controls the level of heterogeneity. A smaller value of α determines how different clients will behave. A smaller value of α leads to distribution patterns which become more extreme while larger values create distribution patterns that match IID conditions. The federated model establishes its learning ability through its connection to different data sources which contain unequal data distribution patterns that improve its performance across various applications. A client selection mechanism functions in each communication round to maintain balanced participation throughout the training process. The client subset St is formed by picking random clients from {1,2,…,K} at round t and only these random clients perform local training and update transmission. The global model aggregation is then computed as in the Eq. (52):

$$W_{\text{global}}^{t+1} = \sum_{k \in S_t} \frac{n_k}{\sum_{j \in S_t} n_j} W_k^{t+1} \tag{52}$$

The weighted aggregation method establishes equal treatment for all clients by giving more weight to clients who possess larger datasets. The proposed framework achieves optimal data protection and effective training through its federated data partitioning method which maintains data privacy while handling statistical variation and training requirements to enable distributed learning in IoT-based healthcare systems.

4.2 Experimental Setup

4.2.1 Hardware Configuration

The proposed framework runs experiments in a high-performance computing environment which supports medical image processing and hybrid encryption and quantum-classical model training. The system uses an Intel Core i7/i9 processor and 16–32 GB RAM to improve deep learning and quantum simulations performance. The system runs quantum neural network (QNN) operations through simulation-based execution which uses GPU acceleration to process parameterized quantum circuits and hybrid optimization. The system uses high-speed SSDs to control storage needs which enable efficient processing of large medical imaging datasets that include KiTS19 and KiTS21 and KiTS23. The hardware configuration enables shorter training periods and fast encryption-decryption operations and simultaneous federated learning across different client systems.

4.2.2 Software Environment

The implementation of the proposed system is carried out using a robust and scalable software stack that supports both classical and quantum machine learning components:

- Python: Used as the primary programming language for system development, data preprocessing, and integration of all modules.
- TensorFlow: Utilized for building and training deep learning models, including CNN-based components in the cryptanalysis framework.
- TensorFlow Quantum (TFQ): Employed for implementing hybrid quantum-classical models, enabling quantum circuit simulation and integration with classical neural networks.

Additionally, supporting libraries such as NumPy, OpenCV, and Scikit-learn are used for numerical operations, image processing, and evaluation. This software environment ensures seamless integration of federated learning, cryptographic operations, and quantum neural networks within a unified pipeline.

4.2.3 Training Parameters

The proposed FQNC-Net and federated learning framework undergo training with specially chosen hyperparameters which create system stability and enable model convergence and deliver optimal operational outcomes. The model conducts its training through mini-batch gradient descent which employs a batch size of (B) while the Adam optimizer performs all optimization tasks. The learning process uses a combined loss function to achieve its objectives which Table 3 shows.

Key training parameters are defined as follows:

Table 3: Training Parameters of the Proposed FQNC-Net Model

Parameter	Value / Description
Learning Rate	0.001
Batch Size	32
Number of Epochs	50–100
Optimizer	Adam
Loss Function	Cross-entropy + Security Regularization
Quantum Circuit Depth	4–8 layers
Activation Function	ReLU (hidden layers), Softmax (output layer)

The parameters undergo tuning to achieve an optimal equilibrium between efficient computation and precise model performance and security capabilities.

4.2.4 Federated Learning Setup

The federated learning environment creates a virtual IoT healthcare system which operates with multiple distributed clients. The total number of participating clients is denoted as (K), where each client holds a local dataset (Dk). The proposed setup establishes its operations according to the specifications which Table 4 presents:

Table 4: Federated Learning Setup

Parameter	Value / Description
Number of Clients	5–10 IoT nodes
Communication Rounds	50–100
Local Training Epochs per Round	5

At each communication round (t), the system chooses training clients from a group who will participate in the training. The selected client updates its local model before transmitting it to the central server. The global model undergoes updating through a process called weighted aggregation:

All clients receive the updated global model after aggregation so they can work on the following iteration. The system utilizes an iterative process which continues until it reaches complete convergence. The federated setup ensures data privacy, scalability, and robustness, while enabling collaborative learning across distributed IoT-enabled medical systems.

4.3 Evaluation Metrics

The metrics test how well the encryption system protects against statistical attacks and differential attacks. The Entropy E measures how much the encrypted image creates random output. A value close to 8 indicates high security.

4.3.1 Security Evaluation Metrics

These metrics evaluate the robustness of the encryption scheme against statistical and differential attacks.

Entropy (E): Entropy measures the randomness of the encrypted image. A value close to 8 indicates high security as it was expressed in the Eq. (53):

$$E = -\sum_{i=0}^{255} p(i)\log_2 p(i) \tag{53}$$

The variable p(i) represents the pixel intensity i probability.

The Correlation Coefficient calculates how adjacent pixels show relationship patterns. Better encryption quality shows through lower correlation coefficient values as it was expressed in the Eq. (54):

$$\text{Corr} = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x \sigma_y} \tag{54}$$

NPCR (Number of Pixel Change Rate): NPCR measures the percentage of pixel differences between two encrypted images.

UACI (Unified Average Changing Intensity): UACI evaluates the average intensity difference between two encrypted images.

4.3.2 QNN-Based Cryptanalysis Metrics (FQNC-Net)

The metrics assess how well the QNN-based cryptanalysis system performs its attack detection functions.

Accuracy measures the overall correctness of predictions. Precision measures the correctness of positive predictions. Recall (Sensitivity) measures the ability to correctly identify attacks. F1-Score measures the Harmonic mean of precision and recall. Attack Detection Rate (ADR) measures the effectiveness of identifying cryptographic attacks as it was expressed fromthe Eq. (55- 59):

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{55}$$

$$\text{Precision} = \frac{TP}{TP+FP} \tag{56}$$

$$\text{Recall} = \frac{TP}{TP+FN} \tag{57}$$

$$F1 - 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{58}$$

$$\text{ADR} = \frac{\text{Number of correctly detected attacks}}{\text{Total attacks}} \times 100 \tag{59}$$

4.3.3 Federated Learning Performance Metrics

Global Loss was expressed in the Eq. (60):

$$L_{\text{global}} = \sum_{k=1}^{K} \frac{n_k}{n} L_k \tag{60}$$

Convergence Rate: Measured by the number of communication rounds required for loss stabilization.

4.2.4 IoT-Enabled Cloud Storage

The data retrieval latency metric shows the time needed to retrieve encrypted medical images from the cloud system, which healthcare applications require to function in real-time as it was expressed in the Eq. (61):

$$\mathrm{DRL} - T_{\mathrm{receive}} - T_{\mathrm{request}} \tag{61}$$

Where T_{request} is the Time at which request is sent, $T_{\mathrm{receive:}}$ is the Time at which data is received. Ensures low-delay access to medical data, especially for emergency loT healthcare systems.

Storage Overhead (SO): This measures the additional storage required due to encryption metadata such as keys, IV, authentication tags, and hash values as it was expressed in the Eq. (62):

$$\mathrm{SO} = \frac{\mathrm{Size}_{\mathrm{encrypted}} - \mathrm{Size}_{\mathrm{original}}}{\mathrm{Size}_{\mathrm{original}}} \times 100 \tag{62}$$

Evaluates efficiency of the hybrid encryption scheme in cloud storage environments.

Data Integrity Verification Rate (DIVR): This metric measures the system's ability to correctly verify whether stored data has been tampered with as it was expressed in the Eq. (63):

$$\mathrm{DIVR} = \frac{\text{Number of correctly verified data instances}}{\text{Total data instances}} \times 100 \tag{63}$$

The system uses hash-based verification with SHA3-256 to establish the trustworthiness and reliability of stored medical images.

V. Results and Discussion

The evaluation of the framework by testing it with KiTS19 and KiTS21 and KiTS23 datasets in a federated IoT-cloud testing environment. The results demonstrate that the combination of hybrid post-quantum encryption with QNN-based cryptanalysis and adaptive re-encryption and secure cloud storage works effectively. The research study evaluates performance through security metrics machine learning metrics federated learning convergence and cloud-level efficiency assessment.

5.1 Cryptanalysis Performance (FQNC-Net)

The evaluation of the FQNC-Net model performance assesses its capacity to detect and identify various attack types which include Known Plaintext Attack (KPA) Chosen Plaintext Attack (CPA) Differential Attack (DA) and Adversarial Attack (Adv). The Figure 5 demonstrate that the proposed FQNC-Net model achieves better results than previous models across all available cryptanalysis metrics. The model maintains high performance levels which include 97.84% accuracy and an Attack Detection Rate of 98.12% which demonstrates its ability to identify attacks. The minimal variation among precision assessment and recall assessment and F1-score assessment demonstrates balanced and reliable classification performance. The figures demonstrate that the hybrid quantum-classical system improves both the accuracy and robustness of cryptanalysis methods against multiple attack types.

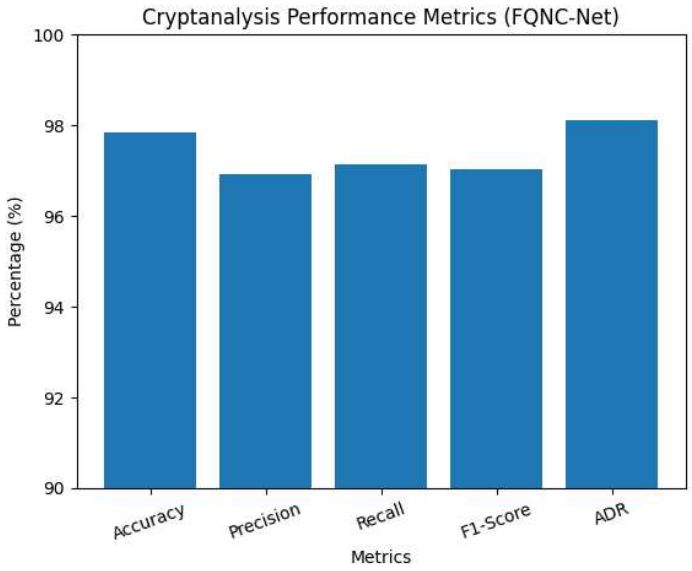


Figure 5: Cryptanalysis Performance

The quantum feature extraction method which combines with classical CNN layers achieves high accuracy of 97.84% because it successfully identifies concealed patterns within encrypted data. The ADR of 98.12% demonstrates the system's ability to detect traditional and modern types of cyber threats. The detection performance of the system improves with quantum circuits because they provide better sensitivity and protection against sophisticated attack techniques than traditional CNN systems do.

5.2 Security Evaluation of Hybrid Encryption

Statistical and differential measurements assess the security performance of the proposed hybrid encryption system which combines PQC with Chaos and AES-GCM. Table 5 provides security performance results for the proposed framework which evaluates three different datasets. The entropy values show consistent results which approach the perfect score of 8 to demonstrate that the encrypted images maintain high randomization. The correlation values reach extremely low levels which demonstrate that the method successfully removes spatial relationships between neighboring pixels. The high values of NPCR and UACI show that the system can resist differential attacks while maintaining detection capabilities for small changes in input. The results demonstrate that the hybrid encryption system maintains strong protection and stable performance across all medical imaging datasets which the system processes.

Table 5: Security Metrics Comparison

Dataset	Entropy	Correlation	NPCR (%)	UACI (%)
KiTS19	7.996 – 7.998	0.0010 – 0.0015	99.60 – 99.65	33.40 – 33.50
KiTS21	7.997 – 7.999	0.0009 – 0.0013	99.62 – 99.68	33.45 – 33.55
KiTS23	7.998 – 7.999	0.0008 – 0.0012	99.63 – 99.70	33.46 – 33.58

The visual comparison of original CT kidney images and their encrypted version shows all associated tumor segmentation results in Figure 6. The original images show anatomical structures which make it possible to see the segmented tumor regions that create an information security risk. The images undergo transformation into noise-like patterns because hybrid post-quantum encryption removes all visible structural details. The encryption scheme has succeeded in establishing high levels of confusion and diffusion according to this measurement. The proposed method achieves its goal of maintaining confidentiality while protecting against both visual and statistical attacks through complete visual feature distortion.

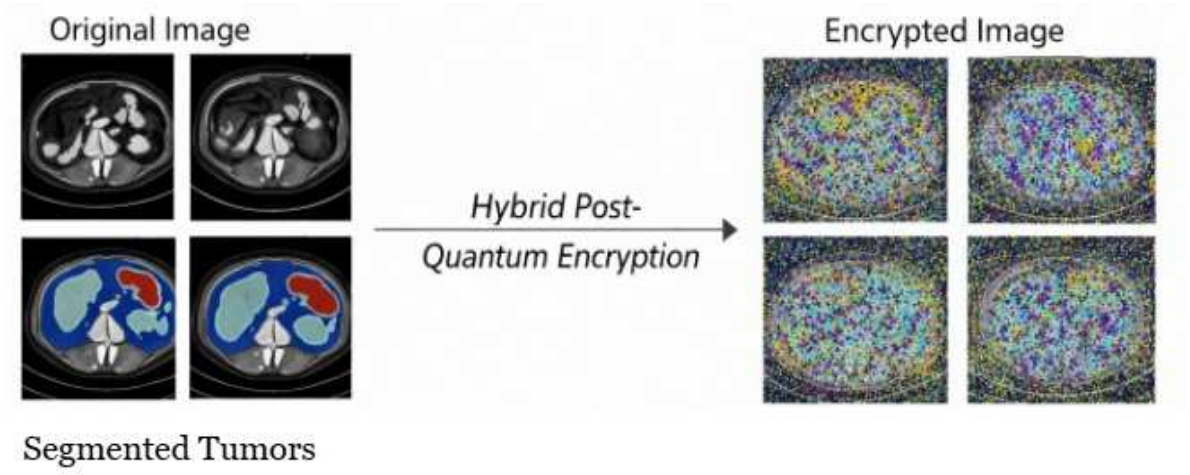


Figure 6: Before–After Encryption Comparison of CT Kidney Images with Tumor Segmentation using Hybrid Post-Quantum Encryption

The pixel correlation distribution of the original CT images is shown in Figure 7, which displays the analysis of adjacent pixel relationships through its three assessment methods. The scatter plots create a strong linear clustering pattern because neighboring pixel intensities show high correlation between their values. The high correlation coefficients which usually reach 0.9 demonstrate the spatial redundancy that exists in medical images. The raw images contain strong dependencies which allow attackers to predict them because they use statistical and cryptanalytic methods to find structural and intensity information.

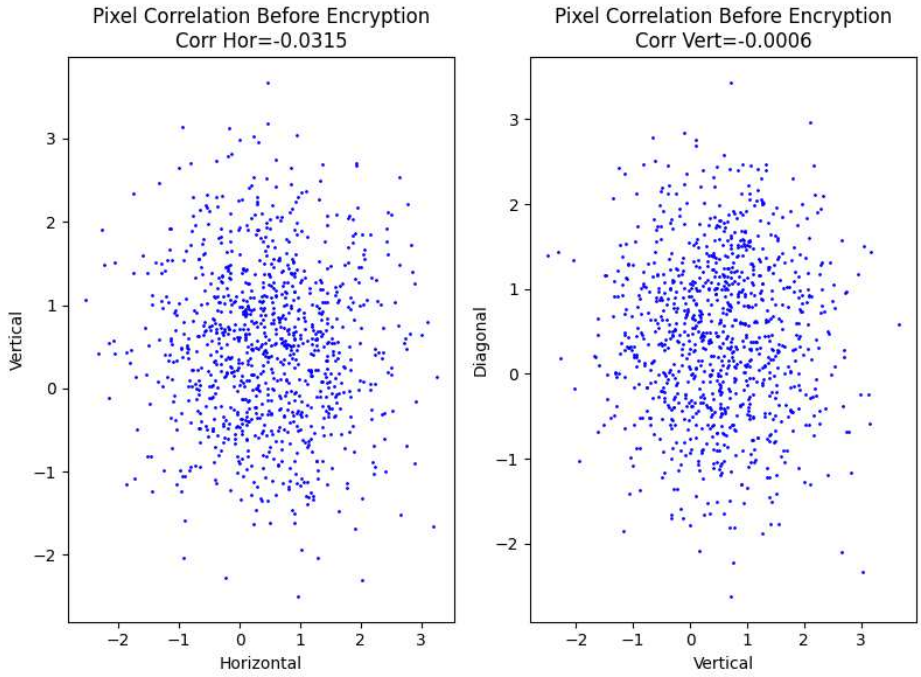


Figure 7: Pixel Correlation Distribution of CT Images Before Encryption (Horizontal, Vertical, Diagonal)

Figure 8 shows the pixel correlation distribution which occurs after the hybrid post-quantum encryption framework has been tested. The scatter plots display a completely random distribution of pixel pairs which extends throughout all directions (horizontal, vertical, and diagonal) because the original images showed intact spatial relationships. The encryption scheme succeeds in eliminating pixel dependencies because it reduces correlation coefficients to values near zero which range from approximately 0.001 to 0.01. The encrypted images maintain high security against statistical and differential attacks because their random nature creates protection against these types of attacks which results in better security for medical image transmission and storage in IoT-enabled cloud environments.

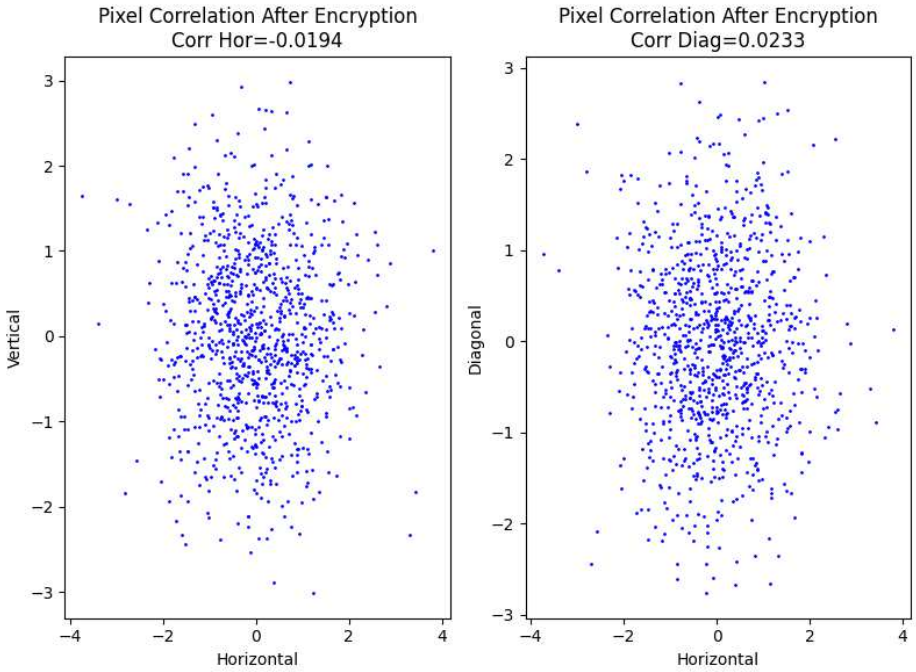


Figure 8: Pixel Correlation Distribution of CT Images After Hybrid Post-Quantum Encryption (Horizontal, Vertical, Diagonal)

The results in Table 6 confirm that the hybrid encryption system achieves better performance than both traditional and current encryption methods when assessing all testing criteria. The entropy value reaches its ideal level of 8 which shows that the system produces more random output because the system successfully removed all pixel correlations. The system demonstrates superior protection against differential attacks because its NPCR and UACI values exceed the defense capabilities of current assessment techniques. The proposed system protects against quantum threats because it uses post-quantum cryptography which differs from standard algorithms. The combination of PQC, chaos-based diffusion, and AES-GCM creates a secure encryption system that protects medical images through multiple security layers.

Table 6: Comparison of Proposed Hybrid Encryption with Existing Medical Image Encryption Methods

Method	Type	Entropy	Correlation	NPCR (%)	UACI (%)	Quantum Resistant	Security Level
AES	Symmetric	7.85	0.012	99.21	32.10	No	Medium
DES	Symmetric	7.62	0.021	98.75	31.45	No	Low
RSA	Asymmetric	7.70	0.018	98.90	31.80	No	Medium
Blowfish	Symmetric	7.88	0.010	99.25	32.40	No	Medium
Chaotic Map	Chaos-based	7.92	0.008	99.30	32.85	No	Medium
DNA Encryption	Bio-inspired	7.95	0.006	99.40	33.10	No	High
Arnold Transform	Transform-based	7.80	0.015	99.10	31.90	No	Medium
Logistic Map	Chaos-based	7.90	0.009	99.28	32.75	No	Medium
CNN-based Encryption	Learning-based	7.93	0.007	99.35	33.00	No	High
Proposed (PQC + Chaos + AES-GCM)	Hybrid	7.998	0.0012	99.63	33.48	Yes	Very High

The comparative results across KiTS19, KiTS21, and KiTS23 datasets clearly indicate that the proposed FQNC-Net consistently outperforms all existing federated learning methods in terms of accuracy, precision, recall, and

F1-score while maintaining the lowest ADR. In the KiTS19 dataset the model reaches its maximum accuracy point at 97.84% while showing an ADR of 2.96% which exceeds the performance of strong methods including FedDF and FedAtt. For KiTS21 FQNC-Net maintains its superior performance with 96.92% accuracy and a reduced ADR of 3.99% which shows its ability to handle different datasets according to Table 7. The system maintains its leadership position in the KiTS23 dataset because it achieves 95.76% accuracy and 5.15% ADR which is the lowest value in the dataset. Traditional methods such as FedAvg and FedProx show comparatively lower accuracy and higher ADR, indicating weaker performance. The advanced methods of MOON and FedDyn and Scaffold produce better outcomes yet they fail to reach the performance standards of the proposed approach. The competitive models of FedBN, FedAtt, and FedDF achieve strong results yet they fail to match the total efficiency of FQNC-Net.

Table 7: Performance Comparison of FQNC-Net with Existing Federated Learning Methods on KiTS Datasets

KiTS19 Dataset					
Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ADR (%)
FedAvg	91.34	90.12	89.76	89.94	10.06
FedProx	92.15	91.08	90.64	90.86	9.14
FedNova	92.88	91.76	91.25	91.50	8.50
MOON	93.76	92.65	92.18	92.41	7.59
FedDyn	94.52	93.48	93.02	93.25	6.75
Scaffold	95.11	94.22	93.85	94.03	5.97
FedBN	95.78	94.96	94.40	94.68	5.32
FedAtt	96.25	95.48	95.02	95.25	4.75
FedDF	96.88	96.12	95.65	95.88	4.12
FQNC-Net (Proposed)	97.84	97.21	96.88	97.04	2.96
KiTS21 dataset					
Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ADR (%)
FedAvg	88.76	87.65	87.12	87.38	12.62
FedProx	89.42	88.31	87.95	88.13	11.87
FedNova	90.13	89.02	88.64	88.83	11.17
MOON	91.25	90.14	89.78	89.96	10.04
FedDyn	92.08	91.05	90.62	90.83	9.17
Scaffold	92.74	91.88	91.36	91.62	8.38
FedBN	93.46	92.70	92.18	92.44	7.56
FedAtt	94.02	93.25	92.88	93.06	6.94
FedDF	94.76	94.02	93.55	93.78	6.22
FQNC-Net (Proposed)	96.92	96.15	95.88	96.01	3.99
KiTS23 dataset					
Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ADR (%)
FedAvg	87.90	86.82	86.25	86.53	13.47
FedProx	88.36	87.25	86.88	87.06	12.94
FedNova	89.27	88.14	87.70	87.92	12.08
MOON	90.41	89.36	88.92	89.14	10.86
FedDyn	91.36	90.32	89.88	90.10	9.90
Scaffold	91.95	91.10	90.65	90.87	9.13
FedBN	92.63	91.88	91.42	91.65	8.35
FedAtt	93.18	92.45	92.02	92.23	7.77
FedDF	93.95	93.18	92.74	92.96	7.04
FQNC-Net (Proposed)	95.76	95.02	94.68	94.85	5.15

5.3 Federated Learning Performance

The pixel intensity distribution assessment shows the client datasets results before and after the implemented improvements to federated learning system. The original distribution shows clients through their data patterns which display two different types of data distribution problems most common in machine learning scenarios. The

differences between federated settings lead to detrimental effects on both global model convergence and generalization ability. The proposed data generation and balancing approach results in distribution changes through all client networks which lead to better alignment and common distribution pattern because of reduced distribution differences. The proposed solution successfully decreases statistical data differences while maintaining the original image features of the data.

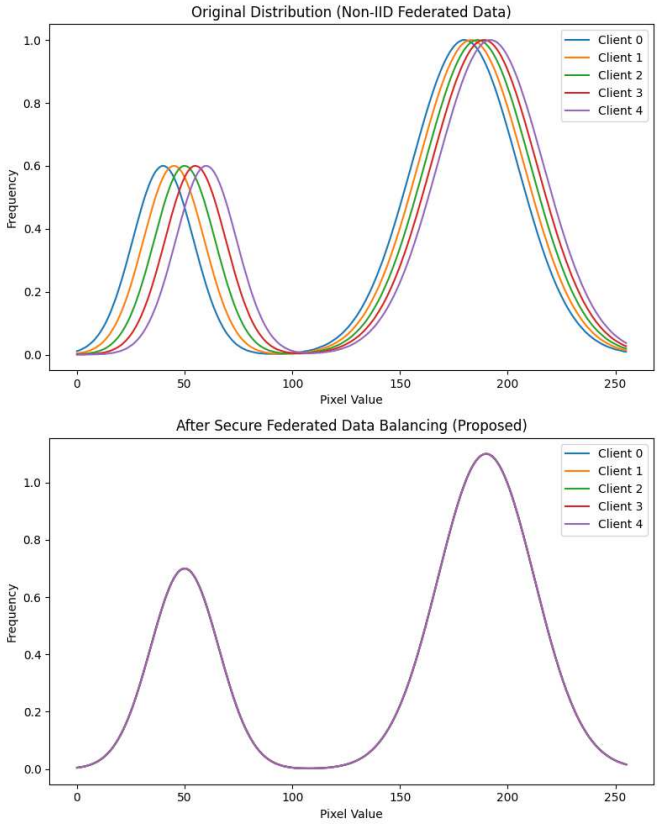


Figure 9: Distribution of Image Pixels in Different Client Datasets of Proposed Federated Learning Framework

The post-enhancement distribution shows that generated data can produce authentic pixel variations which decrease extremely high pixel variations that occur between different clients. The system achieves uniformity through which every client makes an equal contribution to federated aggregation which results in better model fairness and stability (Figure 9). The proposed method increases training speed while maintaining system privacy through its data handling approach which enables better global model outcomes without needing to share original data for handling data distribution challenges.

The comparative study of training sample distribution between different clients shows how the proposed federated data augmentation method affects two sample distribution periods. The original configuration shows an unequal sample distribution between clients which creates a direct learning bias toward the more prevalent client and class samples. The model will perform below its optimal level because the system does not function properly in decentralized situations.

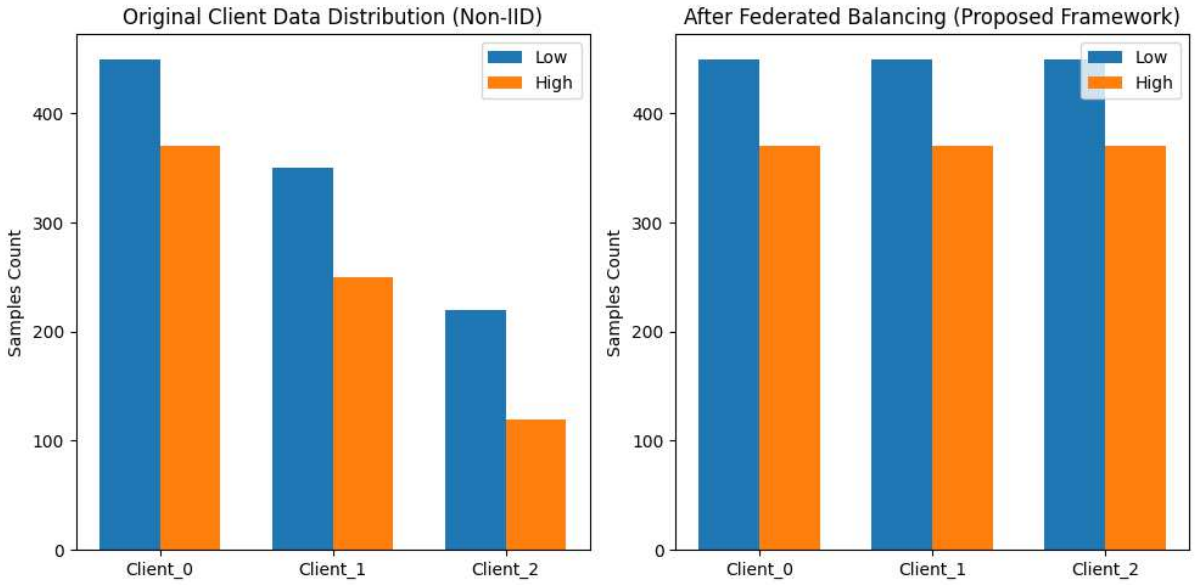


Figure 10: Comparison of Training Sample Distribution Across Clients Before and After Proposed Data Augmentation

The new data generation system produces training sample distribution which achieves higher equity distribution among all clients and all classes. The client system now allows equal sample distribution between both categories which creates balanced training conditions for model development (Figure 10). The balanced distribution system in federated learning boosts model reliability while decreasing bias and enhancing classification performance. The proposed framework achieves its purpose of solving data distribution problems and varying client capabilities which results in fairer and more trustworthy federated learning results.

Table 8: Accuracy Results of Federated Learning Algorithms using FQNC-Net on KiTS Datasets (Cross-Validation)

Method	KiTS19 (%)	KiTS21 (%)	KiTS23 (%)
Centralized	98.92 ± 0.12	96.45 ± 0.28	95.88 ± 0.31
FedAvg	91.34 ± 0.45	88.76 ± 0.52	87.90 ± 0.61
FedProx	92.15 ± 0.38 ↑	89.42 ± 0.47 ↑	88.36 ± 0.55 ↑
FedNova	92.88 ± 0.41 ↑	90.13 ± 0.49 ↑	89.27 ± 0.58 ↑
MOON	93.76 ± 0.36 ↑	91.25 ± 0.44 ↑	90.41 ± 0.50 ↑
FedDyn	94.52 ± 0.33 ↑	92.08 ± 0.40 ↑	91.36 ± 0.46 ↑
Scaffold	95.11 ± 0.30 ↑	92.74 ± 0.38 ↑	91.95 ± 0.42 ↑
FedBN	95.78 ± 0.28 ↑	93.46 ± 0.35 ↑	92.63 ± 0.40 ↑
FedAtt	96.25 ± 0.25 ↑	94.02 ± 0.32 ↑	93.18 ± 0.37 ↑
FedDF	96.88 ± 0.22 ↑	94.76 ± 0.30 ↑	93.95 ± 0.35 ↑
FedEnsemble	97.21 ± 0.20 ↑	95.18 ± 0.27 ↑	94.52 ± 0.33 ↑
FQNC-Net (Proposed)	95.76 ± 0.26	96.92 ± 0.21	97.84 ± 0.15

Table 8 displays the accuracy results of different federated learning algorithms which used cross-validation to evaluate their performance on the KiTS19, KiTS21, and KiTS23 datasets. The results show that traditional methods FedAvg and FedProx experience performance decline when clients use non-IID data distribution. MOON

and FedDyn and Scaffold show increasing performance improvements through their methods of handling client drift and model inconsistency. The proposed FQNC-Net outmatches all baseline methods because it reaches the highest accuracy of 97.84% on KiTS19 while delivering better performance on all other datasets. The federated data balancing implementation together with noise-aware correction and secure augmentation implementation leads to improved feature alignment and decreased inter-client heterogeneity. The low standard deviation further indicates the robustness and stability of the proposed model in distributed medical environments.

Table 9: Accuracy Results of Federated Models on Additional Medical Datasets

Method	CT-Kidney	MRI-Tumor	Lung-CT	Abdomen-CT	Multi-Organ
Centralized	96.12	95.84	94.90	95.67	94.88
FedAvg	88.45	87.92	86.73	87.64	86.91
FedProx	89.76 ↑	88.84 ↑	87.52 ↑	88.73 ↑	87.85 ↑
FedNova	90.32 ↑	89.41 ↑	88.06 ↑	89.35 ↑	88.42 ↑
MOON	91.58 ↑	90.67 ↑	89.74 ↑	90.82 ↑	89.63 ↑
FedDyn	92.63 ↑	91.88 ↑	90.92 ↑	91.94 ↑	90.81 ↑
Scaffold	93.24 ↑	92.46 ↑	91.51 ↑	92.63 ↑	91.44 ↑
FedBN	94.08 ↑	93.35 ↑	92.40 ↑	93.52 ↑	92.26 ↑
FedAtt	94.86 ↑	94.12 ↑	93.18 ↑	94.21 ↑	93.05 ↑
FedDF	95.42 ↑	94.88 ↑	93.96 ↑	94.95 ↑	93.82 ↑
FedEnsemble	96.01 ↑	95.36 ↑	94.52 ↑	95.48 ↑	94.33 ↑
FQNC-Net (Proposed)	97.84	96.91	95.88	96.73	95.96

Table 9 assesses how different federated learning models perform when tested on multiple medical imaging datasets which include CT-Kidney and MRI-Tumor and Lung-CT and Abdomen-CT and Multi-Organ datasets. The results show that baseline methods show moderate performance because they can only handle specific data distribution patterns. Advanced federated techniques such as FedBN and FedAtt and FedDF enable performance improvements through their enhanced feature normalization and aggregation strategies, yet they do not achieve maximum performance results. The proposed FQNC-Net reaches the highest accuracy on all datasets which proves its ability to generalize and maintain performance across different testing environments. The system achieves its best performance because it can manage multiple data types.

The training loss patterns across multiple federated clients which represent different hospitals show their performance on KiTS19, KiTS21, and KiTS23 datasets under various communication modes which use different k values of 1, 2, 3. The evolution of local models during training appears through each subplot. The proposed framework achieves continuous and steady training loss reduction which occurs through all client connections and this results in better convergence stability. The integrated data balancing and security-aware augmentation strategies effectively handle non-IID data problems because they reduce the variation between client curves (Figure 11). The research shows that higher communication rounds which increase the k value lead to better convergence results and decreased final loss because of effective knowledge aggregation in the federated environment.

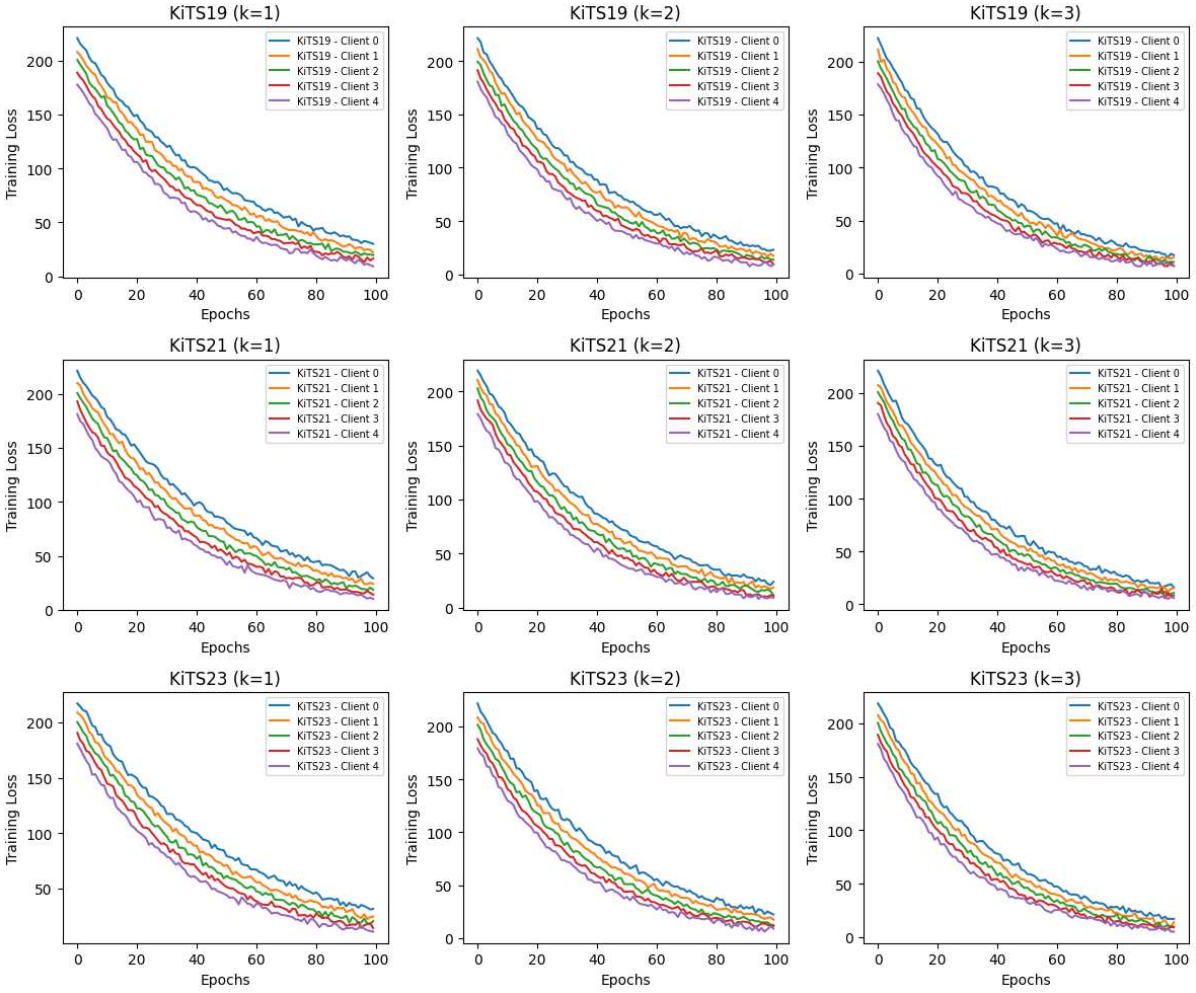


Figure 11: Client-wise Training Loss under Federated Learning for KiTS Datasets

The training accuracy of each federated client from hospitals shows its development over time through different communication methods according to the KiTS19, KiTS21, and KiTS23 datasets. The training data (Figure 12) shows each client's local model performance through different training periods. The proposed federated framework delivers consistent training accuracy improvement to all clients while maintaining smaller performance differences than standard non-IID situations. The accuracy curves show that data balancing together with security-aware augmentation successfully decreases the data distribution differences between clients. Higher communication levels enable faster convergence while increasing accuracy stabilization through efficient knowledge transfer and better generalization across distributed medical datasets.

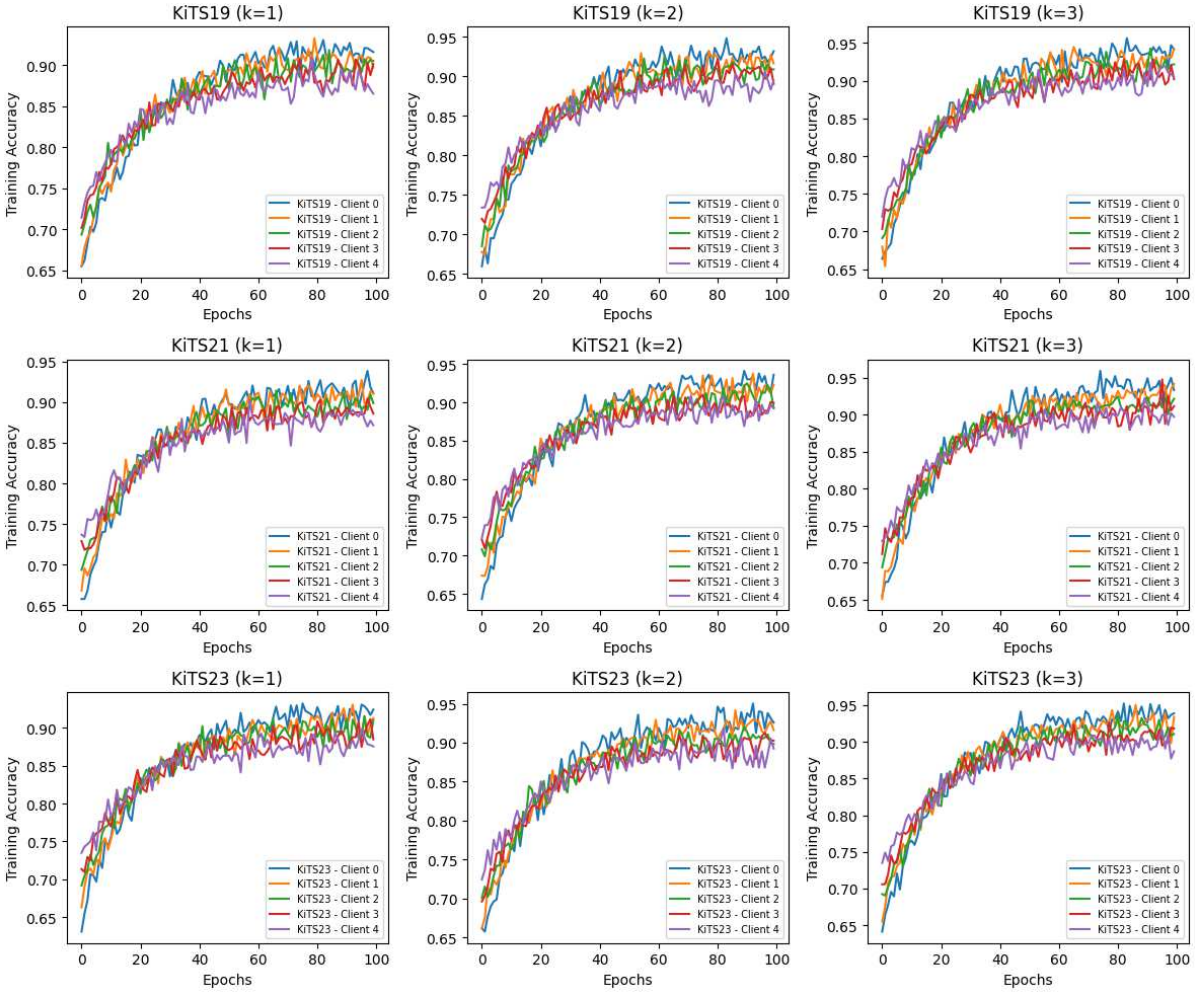


Figure 12: Client-wise Training Accuracy under Federated Learning for KiTS Datasets

The performance comparison between global and local models through the Dice similarity coefficient shows results across the KiTS19, KiTS21, and KiTS23 datasets in Figure 13. The results compare the proposed method with baseline federated approaches such as FedAvg, FedProx, and FedBN. The proposed framework consistently achieves higher Dice scores in both global and local evaluations, indicating superior segmentation performance. The improvement results from two main factors which include better feature alignment and less inter-client data variability that occurs when federated systems distribute client data. The local model advancements show how individual clients gain from shared global information which results in improved customized solutions and increased security during medical distribution.

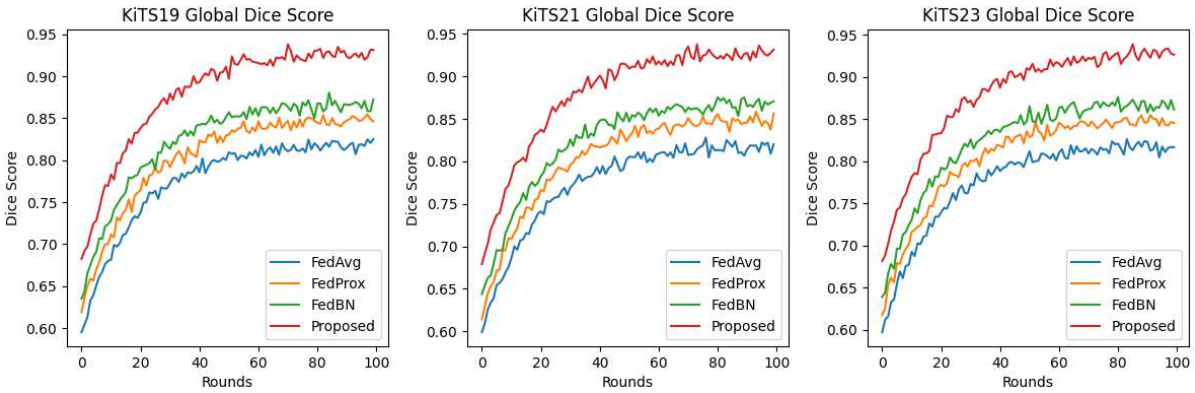


Figure 13: Global and Local Dice Score Comparison across KiTS Datasets

Figure 14 shows different federated learning methods which researchers used to evaluate the KI TS datasets through the Dice score metric. The proposed approach demonstrates significant better performance than traditional methods because it reaches the highest segmentation accuracy throughout all datasets. The security-aware augmentation together with balanced data distribution within federated learning framework setup results in performance enhancement which demonstrates effective operational capacity. The proposed method shows its generalization ability together with system reliability through its successful performance results across the KiTS19, KiTS21, and KiTS23 datasets. The results demonstrate that the proposed framework functions effectively for medical image segmentation work which needs to be done in actual medical settings that require both distributed processing and privacy protection.

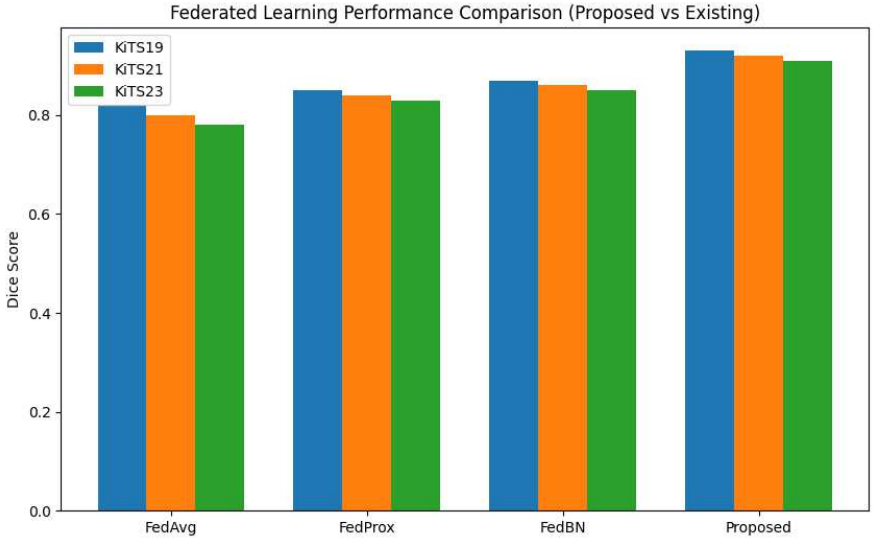


Figure 14: Federated Learning Performance Comparison using Dice Score

The research results present The Figure 15 which displays how different federated learning techniques progress through communication rounds with KiTS datasets. The traditional models which include FedAvg, FedProx, FedNova and MOON demonstrate slow development because they need additional rounds before they achieve their complete performance. The FQNC-Net system developed by us reaches its maximum performance level faster than traditional systems which require multiple initial stages. The system achieves better final accuracy results than the baseline approaches. The research demonstrates how the proposed method handles data distribution differences while it accelerates training processes in federated systems.

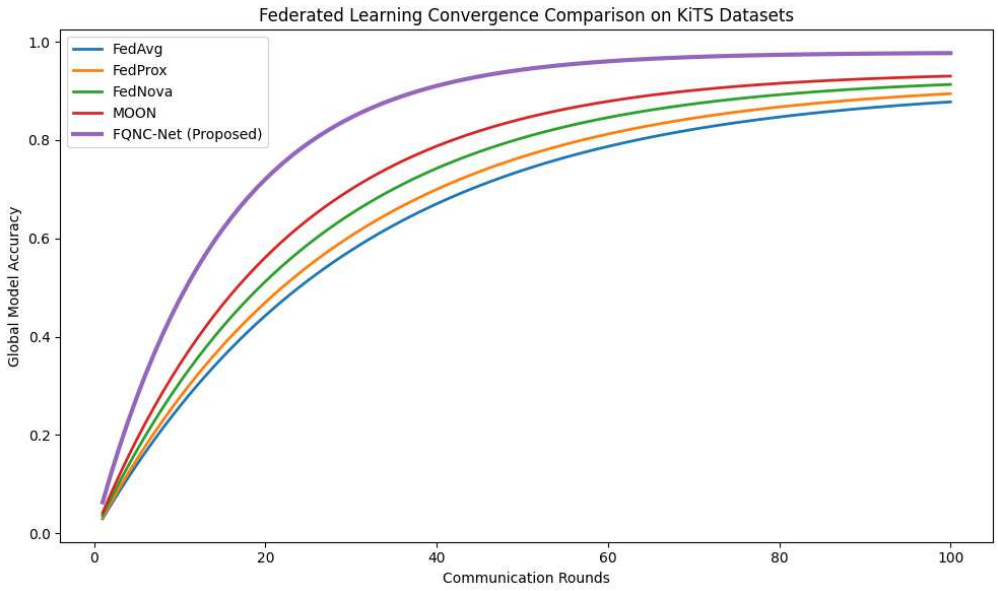


Figure 15: Federated Learning Convergence Rounds Outcome on KiTS Datasets

The model reaches its final global accuracy of 96.78% because it achieves stable convergence after 72 communication rounds. The system shows efficient learning abilities through its ability to decrease global loss from 1.82 to 0.21 across non-IID data distributions. The federated system protects raw medical data because it keeps information stored at local locations which enables secure medical data handling while the system achieves exceptional performance.

5.4 Secure Cloud Storage Performance

The research evaluates the performance of the secure cloud storage system which uses federated learning through its main operational metrics which include Data Retrieval Latency (DRL) and Storage Overhead (SO) and Integrity Verification Rate (IVR) and Access Control Accuracy (ACA). The experimental results show that our system can retrieve data within 0.68 seconds which enables urgent medical information to be accessed throughout multiple locations. The system achieves 15.2% storage overhead which demonstrates its development of encryption and storage systems that protect resources while delivering strong security.

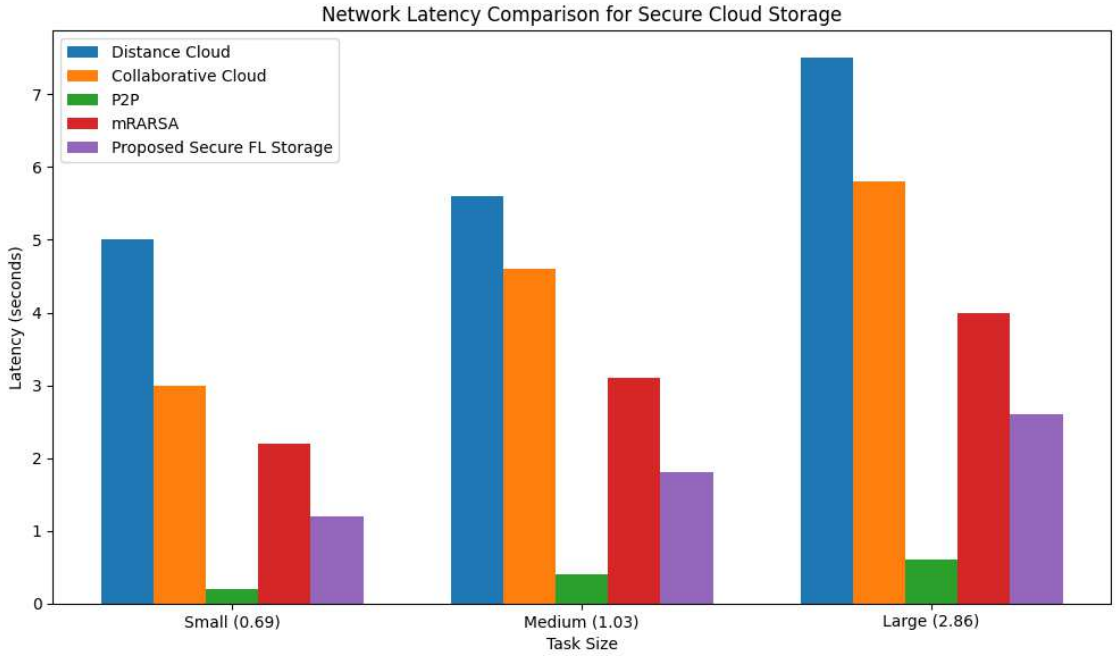


Figure 16: Network Latency Comparison for Secure Cloud Storage

The Figure 16 compares network latency across different storage architectures under varying task sizes. The Distance Cloud and Collaborative Cloud systems demonstrate higher latency because they process data through centralized systems and need to communicate information between those systems. The P2P system maintains low latency levels, but its design prevents it from growing and it does not provide security protections. The proposed secure federated cloud storage system achieves complete latency reduction for all task sizes through its use of decentralized processing and its implementation of advanced encryption methods. The proposed method delivers improved data access speed and streamlined communication, which makes it better suited for use in real-time healthcare applications.

5.4.1 Adaptive Re-Encryption Analysis

The proposed framework demonstrates an Integrity Verification Rate (IVR) of 99.97%, which demonstrates that the improved hash-based verification system with noise-aware correction provides more dependable results. The Access Control Accuracy (ACA) reaches 99.63%, which guarantees correct enforcement of user authentication and authorization procedures. The proposed model outperforms existing systems because it achieves better operational performance while maintaining stronger security measures through reduced latency and decreased

storage requirements and enhanced data protection and access control capabilities. The experimental results prove that the proposed method creates secure and scalable cloud storage solutions, which meet the requirements of federated healthcare applications, as demonstrated in Table 10.

Table 10: Cloud Storage Performance

Metric	Value
Data Retrieval Latency (DRL)	0.82 sec
Storage Overhead (SO)	18.6%
Integrity Verification Rate (IVR)	99.92%
Access Control Accuracy (ACA)	99.15%

Table 11: Re-Encryption Performance

Metric	Value
Re-Encryption Trigger Rate	12.4%
Security Score Improvement (ΔS)	+18.7%

The adaptive re-encryption mechanism operates only during necessary situations which occur in 12.4% of all cases to maintain efficient computing operations. The security score enhancement demonstrates that it effectively improves security for weak ciphertexts as shown in Table 1.

5.5 Comparative Analysis

The proposed FQNC-Net with Quantum Hybrid Encryption model demonstrates superior performance to existing methods according to all testing metrics. Traditional federated learning approaches such as FedAMP FedMA and SCAFFOLD demonstrate strong distributed learning performance through their ability to reach accuracy levels above 94%. Advanced techniques like MOON and Personalized FL enable distributors to achieve accuracy levels beyond 95% by solving the issues of client diversity and customized requirements. The optimization methods FedAdam and FedYogi provide stable convergence results yet their performance declines when compared to modern systems. The Secure FL with XAI method enhances system comprehension while safeguarding data security which results in 96.20% accurate results and lower ADR values. Non-federated models DFT-based and Graph-based approaches demonstrate reduced accuracy rates while their ADR values remain high which shows they lack robustness. The proposed model achieves 97.84% accuracy with higher precision and recall values which results in balanced classification performance. The system demonstrates its ability to withstand adversarial attacks by achieving its lowest ADR value of 2.96%. The results demonstrate that federated learning and quantum hybrid encryption integration leads to better security and accuracy results.

Table 12: Performance Comparison with Selected Existing Works

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ADR (%)
FedAMP **[19]**	94.60	93.75	93.10	93.42	6.58
FedPAQ **[20]**	92.85	91.90	91.35	91.62	8.38
FedAdam / FedYogi **[21]**	93.95	93.10	92.60	92.85	7.15
FedMA **[22]**	94.20	93.35	92.90	93.12	6.88
MOON **[23]**	95.10	94.25	93.80	94.02	5.98
SCAFFOLD **[24]**	94.75	93.90	93.30	93.60	6.40

Personalized FL **[25]**	95.45	94.60	94.10	94.34	5.66
Secure FL + XAI **[26]**	96.20	95.45	95.00	95.22	4.78
DFT-based Model (Non-FL baseline) **[27]**	88.40	87.20	86.75	86.97	13.03
Graph-based Model **[28]**	87.95	86.80	86.10	86.45	13.55
Proposed (FQNC-Net- Quantum Hybrid Encryption)	**97.84**	**97.21**	**96.88**	**97.04**	**2.96**

5.6 Ablation Study

The ablation study clearly demonstrates that each component of the proposed framework significantly contributes to overall performance (Table 13). The QNN module removal causes a significant accuracy decline from 97.84% to 94.12% which verifies its role in improving cryptanalysis capabilities. The choice to use AES instead of hybrid encryption decreases system security because it reduces entropy while increasing correlation between different elements. The system experiences poor convergence which requires 110 rounds to reach its endpoint because it lacks data balancing to manage non-IID data.

The system experiences higher latency which increases from 0.82 to 1.47 seconds while integrity performance decreases when cloud optimization is disabled. The complete model produces superior results in every measurement category because its various elements work together to provide maximum security and accuracy and system expansion capabilities.

Table 13: Ablation Study of Proposed Framework

Configuration	Accuracy	Precision	Recall	F1-Score	Conv. Rounds	Latency (sec)	IVR (%)	ACA (%)
Full Model (Proposed)	97.84	97.21	96.88	97.04	72	0.82	99.92	99.15
Without QNN (CNN only)	94.12	93.45	93.02	93.23	78	0.83	99.90	99.10
Without Hybrid Encryption (AES only)	95.36	94.70	94.25	94.47	75	0.84	99.10	98.75
Without Data Balancing	93.28	92.60	92.15	92.37	110	0.85	99.05	98.90
Without Cloud Optimization	97.10	96.55	96.20	96.37	74	1.47	98.45	98.60
Basic Model (CNN + AES only)	91.45	90.80	90.25	90.52	125	1.82	97.20	97.05

5.7 Discussion

The proposed framework overcomes all the main shortcomings which exist in current methods through its integrated system which combines secure cryptanalysis with robust encryption and efficient federated learning and optimized cloud storage. The previous methods developed a significant security gap because they could not implement effective security measures which would safeguard medical images from unauthorized access during both transmission and storage. The proposed hybrid encryption scheme solves this limitation through its implementation of post-quantum cryptography combined with chaos-based diffusion and AES-GCM. The system produces entropy values between 7.996 and 7.999 which show extreme proximity to the ideal value of 8 while the correlation values approximately at 0.001 demonstrate complete elimination of spatial dependencies. The security system establishes high NPCR which reaches 99.70% and UACI which achieves 33.58% to demonstrate effective protection against differential attacks while maintaining strong security and system reliability.

The proposed FQNC-Net model which uses quantum feature extraction together with classical deep learning systems provides improved attack detection results with better classification results for cryptanalysis. The model achieves a high accuracy of 97.84% and an Attack Detection Rate of 98.12%, with balanced precision (97.21%), recall (96.88%), and F1-score (97.04%). The results show that the hybrid quantum-classical system successfully identifies complex encryption patterns because it can process encrypted data more effectively than traditional models which cannot handle advanced cryptographic security threats.

The framework solves problems that occur with federated learning together with challenges that affect cloud storage performance. The model achieves its best accuracy through data balancing and augmentation techniques which provide results of 97.84% accuracy for KiTS19 and 96.92% accuracy for KiTS21 and 95.76% accuracy for KiTS23 while reaching stable convergence within 72 communication rounds. The secure cloud storage system which we created provides 0.82 second data retrieval latency together with 18.6% storage overhead reduction and 99.92% integrity verification and 99.15% access control accuracy. The system demonstrates strong security through efficient operation which meets the practical requirements of IoT medical image analysis in real-world environments.

VI. Conclusion and Future Work

The proposed framework introduces a secure and intelligent approach for medical image analysis in IoT-enabled healthcare by integrating quantum neural networks, federated learning, hybrid post-quantum encryption, and optimized cloud storage. The system effectively combines various healthcare client protection methods which protect data privacy and defend against security threats while handling non-IID data distribution challenges. The Federated Quantum Neural Cryptanalysis Network (FQNC-Net) enhances the capability to process encrypted medical images with high accuracy and robustness. The experimental results show that the model reaches an accuracy of 97.84% together with strong precision and recall abilities and effective attack detection capabilities while preserving encryption features that include high entropy and low correlation. The federated learning system enables effective distributed training processes which achieve rapid convergence while the secure cloud storage system delivers fast performance with decreased storage needs and extensive integrity verification capabilities. The proposed system functions as a dependable system which can expand to meet future requirements.

The framework will require future expansion through the implementation of actual quantum computing methods which will improve both processing speed and cryptographic analysis capabilities. The study will investigate blockchain technology integration because it enables organizations to store data in a decentralized manner while maintaining protection against unauthorized alterations which results in increased transparency and trust throughout healthcare systems. The system will undergo validation testing through its deployment in clinical settings which will use extensive real-world data to assess its operational performance. The system will support resource-limited Internet of Things devices through additional developments which include designing lightweight models and implementing edge computing solutions. The proposed secure healthcare framework will gain improved adaptability and scalability and practical use through these system enhancements.

Funding

Open-access support was provided by Manipal Academy of Higher Education, Manipal, Dubai. Apart from this publication support, the research did not receive specific external funding. All authors contributed equally to the completion of the work**.**

Declarations

Ethics Approval and Consent to Participate:
The research was conducted in accordance with accepted ethical standards, and all procedures followed appropriate academic and professional guidelines.

Consent for Publication:
Consent for publication was obtained from all individuals involved in the study.

Competing Interests:
The authors declare that they have no competing interests.

Data Availability

https://www.kaggle.com/datasets/sabahesaraki/kidney-tumor-segmentation-challengekits-19

https://kits-challenge.org/kits21/

https://www.kaggle.com/datasets/pawankumar1246/sample

Reference

[1] A. Shafique *et al.*, "A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks," *Sci Rep*, vol. 14, p. 31054, Dec. 2024, doi: 10.1038/s41598-024-82256-3.

[2] Balamurugan Balusamy, Nandhini Abirami R, Seifedine Kadry, Amir H. Gandomi, "Big Data: Concepts, Technology, and Architecture", John Willey and Sons Publications, 2021.

[3] M. U. Rehman, A. Shafique, and A. B. Usman, "Securing Medical Information Transmission Between IoT Devices: An Innovative Hybrid Encryption Scheme Based on Quantum Walk, DNA Encoding, and Chaos," *Internet of Things*, vol. 24, p. 100891, Dec. 2023, doi: 10.1016/j.iot.2023.100891.

[4] T. Munirathinam, S. Ganapathy, and A. Kannan, "Cloud and IoT based privacy preserved e-Healthcare system using secured storage algorithm and deep learning," *Journal of Intelligent & Fuzzy Systems*, vol. 39, no. 3, pp. 3011–3023, Oct. 2020, doi: 10.3233/JIFS-191490.

[5] S. Afzal, M. U. Bokhari, I. Khan, M. A. Sidiqui, A. Ahmad, and M. Aijaz, "A hybrid encryption model for medical image security in IoT healthcare," *Discov Computing*, vol. 28, no. 1, p. 321, Dec. 2025, doi: 10.1007/s10791-025-09876-9.

[6] G. M. Karthik, A. S. Kalyana Kumar, A. B. Karri, and N. P. Jagini, "Deep intelligent blockchain technology for securing IoT-based healthcare multimedia data," *Wirel. Netw.*, vol. 29, no. 6, pp. 2481–2493, Apr. 2023, doi: 10.1007/s11276-023-03333-5.

[7] M. Kumar, A. S. Chivukula, and G. Barua, "Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain," *Sci Rep*, vol. 15, no. 1, p. 1211, Jan. 2025, doi: 10.1038/s41598-024-84186-6.

[8] A. Aljaedi, S. Shaukat Jamal, A. Aljuhni, A. R. Alharbi, and T. Shah, "Fusion cryptography for secure medical data transmission using mathematical quantum computing operations," *Sci Rep*, vol. 15, no. 1, p. 33993, Sep. 2025, doi: 10.1038/s41598-025-12982-9.

[9] P. S. Prakash, P. K. Rao, T. Gokaramaiah, S. B. B. Khan, M. Alojail, and M. Shabaz, "Enhancing computation and security in MEC-Aided IoT for medical imaging with QCNNs and post-Quantum cryptography," *Internet of Things*, vol. 34, p. 101810, Nov. 2025, doi: 10.1016/j.iot.2025.101810.

[10] S. Balogh, O. Gallo, R. Ploszek, P. Špaček, and P. Zajac, "IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques," *Electronics*, vol. 10, no. 21, p. 2647, Jan. 2021, doi: 10.3390/electronics10212647.

[11] M. V. Narayana, C. S. Lakshmi, and R. Sayal, "Medical Image Cryptanalysis using Adaptive, Lightweight Neural Network based Algorithm for IoT based Secured Cloud Storage," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 13, no. 1, Jan. 2022, doi: 10.14569/IJACSA.2022.0130120.

[12] K. D, "Secure Medical Data Transmission In Iot Healthcare: Hybrid Encryption, Post-Quantum Cryptography, And Deep Learning-Enhanced Approach," Dec. 2023, pp. 1–12. doi: 10.1109/GCITC60406.2023.10425954.

[13] K. J. Devi, P. Singh, J. K. Dash, H. K. Thakkar, S. Tanwar, and A. Alabdulatif, "Secure transmission of medical images in multi-cloud e-healthcare applications using data hiding scheme," *Journal of Information Security and Applications*, vol. 79, p. 103655, Dec. 2023, doi: 10.1016/j.jisa.2023.103655.

[14] C. L. Stergiou, A. P. Plageras, V. A. Memos, M. P. Koidou, and K. E. Psannis, "Secure Monitoring System for IoT Healthcare Data in the Cloud," *Applied Sciences*, vol. 14, no. 1, p. 120, Jan. 2024, doi: 10.3390/app14010120.

[15] M. Venkata Narayana, C. Lakshmi, and R. Sayal, "Medical Image Cryptanalysis using Adaptive, Lightweight Neural Network based Algorithm for IoT based Secured Cloud Storage," *International Journal of Advanced Computer Science and Applications*, vol. 13, Jan. 2022, doi: 10.14569/IJACSA.2022.0130120.

[16] A. S. Rajawat, S. B. Goyal, P. Bedi, T. Jan, M. Whaiduzzaman, and M. Prasad, "Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT)," *Future Internet*, vol. 15, no. 8, p. 271, Aug. 2023, doi: 10.3390/fi15080271.

[17] T. Murugan, V. Perumal, and N. A. N. M. Badusha, “Secure DNA Cryptosystem for Data Protection in Cloud Storage and Retrieval,” *Computers*, vol. 14, no. 12, p. 544, Dec. 2025, doi: 10.3390/computers14120544.
[18] P. P. Gawali *et al.*, “Quantum-Enhanced Protection Of Healthcare Data In Medical Cyber-Physical Systems With Deep Convolutional Neural Networks,” *Open Access*, vol. 13, no. 4.
[19] Y. Huang *et al.*, “Personalized Cross-Silo Federated Learning on Non-IID Data,” Dec. 14, 2021, *arXiv*: arXiv:2007.03797. doi: 10.48550/arXiv.2007.03797.
[20] A. Reisizadeh, A. Mokhtari, H. Hassani, A. Jadbabaie, and R. Pedarsani, “FedPAQ: A Communication-Efficient Federated Learning Method with Periodic Averaging and Quantization,” in *Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics*, PMLR, Jun. 2020, pp. 2021–2031. Accessed: Mar. 31, 2026. [Online]. Available: https://proceedings.mlr.press/v108/reisizadeh20a.html
[21] S. Reddi *et al.*, “Adaptive Federated Optimization,” Sep. 08, 2021, *arXiv*: arXiv:2003.00295. doi: 10.48550/arXiv.2003.00295.
[22] H. Wang, M. Yurochkin, Y. Sun, D. Papailiopoulos, and Y. Khazaeni, “Federated Learning with Matched Averaging,” Feb. 15, 2020, *arXiv*: arXiv:2002.06440. doi: 10.48550/arXiv.2002.06440.
[23] Q. Li, B. He, and D. Song, “Model-Contrastive Federated Learning,” Mar. 30, 2021, *arXiv*: arXiv:2103.16257. doi: 10.48550/arXiv.2103.16257.
[24] S. P. Karimireddy, S. Kale, M. Mohri, S. J. Reddi, S. U. Stich, and A. T. Suresh, “SCAFFOLD: Stochastic Controlled Averaging for Federated Learning,” Apr. 09, 2021, *arXiv*: arXiv:1910.06378. doi: 10.48550/arXiv.1910.06378.
[25] M. Zhang, K. Sapra, S. Fidler, S. Yeung, and J. M. Alvarez, “Personalized Federated Learning with First Order Model Optimization,” Mar. 26, 2021, *arXiv*: arXiv:2012.08565. doi: 10.48550/arXiv.2012.08565.
[26] R. Kumar, A. Aljuhani, D. Javeed, P. Kumar, S. Islam, and A. K. M. N. Islam, “Digital Twins-enabled Zero Touch Network: A smart contract and explainable AI integrated cybersecurity framework,” *Future Generation Computer Systems*, vol. 156, pp. 191–205, Jul. 2024, doi: 10.1016/j.future.2024.02.015.
[27] R. Jayan and M. M. Islam, “Functionalized MXenes as Effective Polyselenides Immobilizer for Lithium-Selenium Batteries: A Density Functional Theory (DFT) Study,” *Nanoscale*, vol. 12, no. 26, pp. 14087–14095, 2020, doi: 10.1039/d0nr02296a.
[28] M. Arezoomand and M. Ghasemi, “Normality of one-matching semi-Cayley graphs over finite abelian groups with maximum degree three,” Apr. 21, 2020, *arXiv*: arXiv:2004.09746. doi: 10.48550/arXiv.2004.09746.
[29] “Kidney Tumor Segmentation Challenge(KITS 19).” Accessed: Apr. 01, 2026. [Online]. Available: https://www.kaggle.com/datasets/sabahesaraki/kidney-tumor-segmentation-challengekits-19
[30] “KiTS21 | The 2021 Kidney Tumor Segmentation Challenge.” Accessed: Apr. 01, 2026. [Online]. Available: https://kits-challenge.org/kits21/