ISSN: 2182-2069 / E-ISSN: 2182-2077

AI-Optimized Quantum-Resistant CAPTCHA-Based Secure Computation Framework for Privacy-Preserving Federated Learning in Distributed Cloud Networks

M. Karthikeyan[1*], and Dr.A.R. Arunachalam[2]

[1*]Research Scholar, Department of Computer Science, Dr. M. G. R. Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India.
mkeyan1990@gmail.com, https://orcid.org/0009-0009-4287-7584

[2]Head and Academic Dean, Department of Computer Science, Dr. M.G.R Educational and Research Institute, Chennai, Tamil Nadu, India. arunachalam.cse@drmgrdu.ac.in, https://orcid.org/0000-0002-0181-7966

Received: January 17, 2026; Revised: March 03, 2026; Accepted: April 08, 2026; Published: May 29, 2026

Abstract

Despite the swift adoption of FL within distributed cloud systems, boosting collaborative intelligence and maintaining data locality, current FL frameworks are susceptible to a variety of malicious threats, including adversarial bot intrusions, data poisoning, privacy breaches, and new quantum-based cryptographic attacks. Existing CAPTCHA technologies are also shown to have poor resistance to AI-driven solvers, with accuracy reaching 78.4% against complex distributed system-based attacks. Accordingly, this paper introduces an AI-Optimized Quantum-Resistant CAPTCHA-based Secure Computation Framework (AQC-SCF) for privacy-preserving FL within distributed cloud environments. The proposed framework combines an adaptive adversarial CAPTCHA generation engine, post-quantum lattice-based cryptography, and a secure aggregation scheme to enhance authentication, data privacy, and model integrity in a collaborative learning environment. Evaluated the performance of the proposed scheme across 120 distributed clients running on a simulated cloud, over 50 communication rounds, using more than 85,000 training samples from benchmark classification datasets. The experiments indicate that compared to standard FL, secure FL, and blockchain-based FL, the proposed AQC-SCF achieves 97.8%, 96.9%, 96.3%, and 96.6% accuracy, precision, recall, and F1-score, respectively, which improves standard FL, secure FL, blockchain-based FL, and AQC-FL models by 8.7%, 6.1%, 4.4%, and 2.6%. Authentication breaches were reduced by 93.5%, and communication overhead decreased by 27.8%, while quantum-attack-based cryptographic resilience increased by 41.6% with an average latency of 0.84s per aggregation round. These findings demonstrate the suitability and scalability of the proposed scheme for securely realizing distributed federated intelligence in next-generation cloud environments.

Keywords: Federated Learning, Post-Quantum Cryptography, CAPTCHA Security, Privacy Preservation, Secure Aggregation, Distributed Cloud Networks, Artificial Intelligence.

1 Introduction

Due to the growing popularity of cloud computing, edge intelligence, and connected devices, federated learning (FL), a privacy-aware machine learning paradigm, is becoming increasingly widely used. Unlike centralized learning, where data is uploaded to an aggregation server, FL enables

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May - 2026), pp. 358-374.
DOI: *10.58346/JISIS.2026.I2.023*

*Corresponding author: Research Scholar, Department of Computer Science, Dr. M. G. R. Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India.

multiple parties to collectively train a shared model without sharing raw data. This makes it highly suitable for applications where data confidentiality is crucial, such as health, finance, industrial automation, and smart networks (Thota, 2023). Some recent works have proposed privacy-preserving FL frameworks to improve learning performance using local data across distributed cloud-edge infrastructure (Zhou et al., 2022). At the same time, distributed lightweight cloud-edge-end collaboration models further strengthened the scalability of FL in large-scale intelligent systems (Zhan et al., 2025). Despite many benefits, distributed learning raises potential security and privacy issues: exchanged model parameters may contain sensitive information, and communication channels and aggregation servers are vulnerable to poisoning, interception, and inference attacks Liu et al., (2025). Moreover, the security of peer-to-peer federated environments is further undermined by the risks of compromised nodes and synchronized attacks in distributed systems (Zhou et al., 2023).

On the other hand, classical CAPTCHA methods are vulnerable to automated solvers based on deep learning, which are intended to protect cloud services as access control mechanisms (Nechypurenko et al., 2025). Furthermore, quantum computation threatens conventional cryptographic methods. A joint human verification and quantum-resistant security mechanism is urgently needed in the distributed learning system.

The conventional aggregation method in federated learning remains susceptible to malicious clients' participation and gradient poisoning/manipulation, even when it avoids direct data exposure. Studies on the prediction of adversarial attacks demonstrate that automatic attacks can severely undermine the reliability of learning when there are weak trust assumptions in a collaborative system (Balakrishnan, 2024). Similarly, analyses of blockchain-based intrusions showed that automated agents can bypass static authentication systems and inject harmful requests into distributed systems (Khan et al., 2025). Besides, the classical CAPTCHA mechanism faces severe limitations, as computer vision models have successfully solved image- and text-based CAPTCHAs with high accuracy (Nechypurenko et al., 2025). At the same time, security mechanisms like secure aggregation used in secure computation might become invalid in the presence of quantum computers. Privacy-preserving frameworks also incur increased latency, communication overhead, and computational cost in geographically distributed cloud environments (Shen et al., 2022). Therefore, there is an increasing need for a unified approach that provides adaptive authentication, quantum-resistant security, and privacy preservation, while imposing a lower computational burden.

In this paper, propose an AI-Optimized Quantum-Resistant CAPTCHA-based Secure Computation Framework to realize privacy-preserving federated learning in a distributed cloud network. The framework integrates adaptive CAPTCHA generation, secure client authentication, post-quantum cryptography protection, and secure aggregation. The framework adheres to the reproducible research guidelines recommended by modern cybersecurity research (Olszewski et al., 2023). The combination of federated intelligence, automated cyber-attacks, and quantum-era security threats poses serious risks to the distributed cloud environment. However, overcoming these vulnerabilities can help develop a reliable, privacy-preserving, and scalable intelligent system. The work includes four contributions. First, an AI-Optimized CAPTCHA mechanism is proposed to withstand automated solver attacks. Second, a post-quantum resistant secure computation protocol is developed to protect the model exchange between nodes. Third, a privacy-preserving federated learning framework is developed for efficient collaborative learning on a distributed cloud. Fourth, experimental results demonstrate the performance of the framework.

The remainder of this paper is structured as follows. In Section II, a survey of relevant works on privacy-preserving federated learning, CAPTCHA authentication, and post-quantum cloud security is provided. In Section III, the proposed AQC-SCF framework is explained in detail, covering system architecture, dynamic CAPTCHA generation, quantum-resistant secure computation, and federated

learning algorithm. The experimental configuration, performance measures, comparisons, and ablation study are explained in Section IV. The discussion of security efficiency, performance, and scalability in a distributed cloud environment is presented in Section V. Finally, the conclusions and future work are presented in Section VI.

2 Literature Review

Federated learning-based privacy-preserving approaches have become increasingly important in distributed cloud intelligence. Secure aggregation preserves local model updates by summing encrypted parameters without revealing individual clients' information. Awan et al. It has been shown that cryptography-aided aggregation enhances data privacy in large-scale IoT applications, and a verifiable aggregation model enhances the integrity during parameter merging (Awan et al., 2023; Zhou et al., 2022). Nevertheless, the synchronization overhead is very large for the secure aggregation protocol. Differential privacy (DP) adds controlled random noise to gradients before they are transmitted to servers to defend against inference attacks. Demonstrated that the hybrid DP approach greatly enhances data privacy for industrial edge systems while maintaining acceptable learning performance Jiang et al., (2021). However, a large amount of noise severely degraded convergence speed and accuracy. Homomorphic encryption (HE) enables computations on encrypted data, thereby ensuring security in collaborative analytics without leaking sensitive information (Wang et al., 2022; Howlader et al., 2026). In health-oriented FL frameworks, it has proved effective in medical data security in a multi-cloud scenario. Nevertheless, HE has extremely high computation overhead and encryption latency. Multi-party computation (MPC) distributes computation across multiple trusted parties, thereby preventing any single party from disclosing information. The proposed MPC protocols in cloud research demonstrate higher levels of confidentiality and integrity during collaborative analytics across organizations (Ma et al., 2025; Chen et al., 2024). However, the huge communication overhead is a problem for real-time applications.

The usage of CAPTCHA is a widely adopted technique for verifying human users. Classic text- and image-based CAPTCHAs differentiate human users from bot attacks using techniques such as distorted characters, image matching, and object search. However, current deep learning models have a much lower accuracy against these traditional CAPTCHAs. In response, the behavioral CAPTCHAs measure features such as cursor movement dynamics, key-stroke dynamics, touchscreen interaction, and the reaction latency, and apply these attributes to differentiate between human users and bots. This approach achieves better usability while leveraging real-time human characteristics. The CAPTCHA generation that resists against AI and blockchain-assisted verification are being studied Sezer et al., (2023). Bot detection systems, such as traffic monitoring, access patterns, request frequency tracking are widely applied to detecting malicious automated accesses in federated and blockchain system (Singh et al., 2022). Despite the improved performance, many CAPTCHA challenges are still vulnerable to CNN and Transformer models as they become too predictable to the solvers. Thus, an adaptive CAPTCHA challenge integrated with intelligent threat-aware security model is required.

The advent of quantum computing introduces risks to current cryptograph systems used in distributed cloud environments. Lattice-based cryptography is considered a robust solution for post-quantum, due to its proven ability to withstand quantum attacks and efficient support of secure communication in distributed learning frameworks (Sehgal & Mohapatra, 2021). The hash-based signature provides integrity verification and code-based encryption gives data confidentiality leveraging error correcting code structures; but it demands larger storage space for key management due to enlarged key sizes. Besides, the usage of quantum-safe key exchange protocols is beneficial for protecting the communication between distributed learning nodes in a long term Chen et al.,

(2024). Nevertheless, limited studies integrate post-quantum cryptography along with adaptive authentication and real-time federated learning framework.

The traditional FL schemes utilize cryptographic algorithms to preserve data privacy and the research on these schemes has achieved satisfactory results regarding privacy-preservation, but resulted in enormous computational and communication overhead. In the realm of CAPTCHA security, the human behavior tracking, AI-resistant designs have shown effectiveness against sophisticated automated attacks, however, current deep learning based automated attacking systems have demonstrated their powerful capability to break down various CAPTCHA mechanisms. Moreover, post-quantum cryptography provides strong data security for the future but it still under research and has rarely been deployed on federated learning together with the real-time authentication schemes. This suggests a clear research gap that this work aims to fill.

3 Proposed Methodology

In order to combat privacy leakage, bot intrusion, and cryptographic security vulnerabilities of the distributed cloud learning under quantum era, this work proposes the AI-Optimized Quantum-Resistant CAPTCHA-based Secure Computation Framework (AQC-SCF) with an adaptive human verification, post-quantum encryption, and privacy-preserved federated learning as a secure architecture.

System Architecture of AQC-SCF Framework

The framework for AQC-SCF framework includes five functional layers: clients, local training, CAPTCHA verification engine, secure aggregation server and distributed cloud storage. These layers work together to ensure security, authenticated access and encrypted information sharing for the distributed cloud learning.

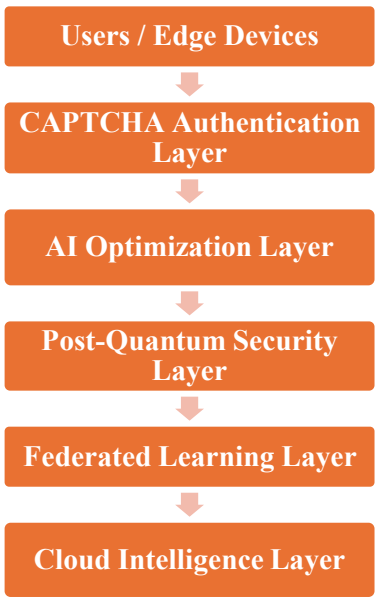

Figure 1: Conceptual architecture of the proposed AQC-SCF framework

In figure 1 depicts the high-level conceptual architecture of the proposed AI-Optimized Quantum-Resistant CAPTCHA Secure Computation Framework (AQC-SCF) for privacy-preserving federated learning on distributed cloud networks. The system starts from user and edge devices participation using CAPTCHA authentication layer for secure human identification, followed by AI optimization layer for adaptive challenges and threat detection, then

transmitted data goes through post-quantum security layer for secure information transfer and lastly collected into federated learning layer for distributed learning and aggregation of AI model followed by management on cloud intelligence layer for scalability, security and quantum security protection.

Client Nodes

Clients are edge devices like mobile phones, IoT gateway or enterprise computing unit which access the federated learning. The total clients can be calculated in equation (1):

$$C = \{c_1, c_2, c_3, \ldots, c_n\} \quad (1)$$

Where n is the number of total participating clients. Each client contains a local private data, shown in equation (2):

$$D_i = \{x_i, y_i\} \quad (2)$$

Where x_i is the input data and y_i is the output labels. Before participating in the federated learning, the client should accomplish adaptive CAPTCHA authentication.

Local Training

After passing the authentication, the client conducts a local neural model training over their local private data without data sharing represented in equation (3):

$$W_i^t \quad (3)$$

Where t represents training round. Gradient updates are computed locally in equation (4):

$$G_i^t = \nabla L\left(W_i^t, D_i\right) \quad (4)$$

Where L is the loss function.

CAPTCHA Verification Engine

This component provides a mechanism for adaptive human verification before the client access to the training process. The system dynamically generates CAPTCHA challenges by using AI based perturbation and verifies whether the user is a human or bot. The CAPTCHA verified client continues to secure training stage.

Secure Aggregation Server

The server aggregates encrypted model parameters provided by authenticated clients and performs privacy-preserving aggregation, defined in equation (5):

$$W_g^{t+1} = \sum_{i=1}^{n} \frac{|D_i|}{\sum |D_i|} W_i^t \quad (5)$$

It means weighted aggregation to ensure data proportion while without any real data disclosure.

Distributed Cloud Storage

The encrypted final global models, session key and log records are distributed stored on the cloud system which enhance system availability.

Figure 2 illustrates the workflow of the proposed AI-Optimized Quantum-Resistant CAPTCHA Secure Computation Framework (AQC-SCF) in a distributed cloud system. Initially, 120 clients start to participate, then, a dynamic CAPTCHA with adversarial noise is generated for secure human authentication via the authentication module. The authenticated clients train the model locally based

on the private dataset, then the parameters are encrypted with 4096-bit post-quantum cryptography (PQC) encryption module. The encrypted models are transferred to the secure aggregation server for global model optimization, and the optimized model is then stored in the distributed cloud repository. The proposed method achieves privacy-preserved, scalable and quantum-resistant federated learning.

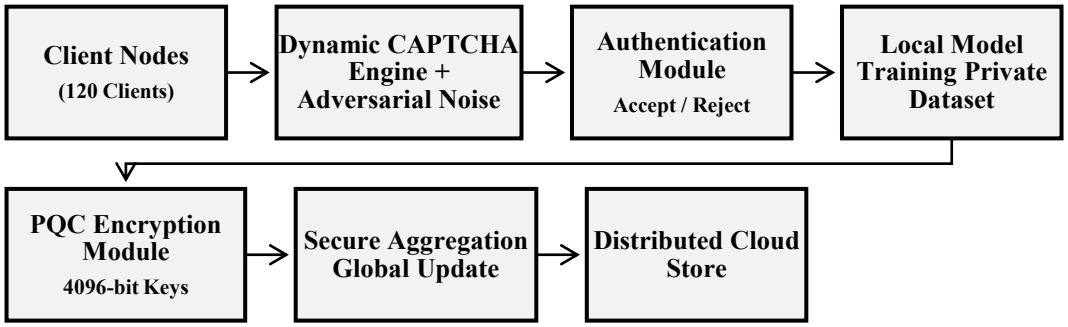

Figure 2: Detailed workflow of the proposed AQC-SCF secure federated learning framework

AI-Optimized CAPTCHA and Quantum-Resistant Security Design

In this layer, the adaptive CAPTCHA verification and post-quantum cryptographic protection are jointly designed.

Dynamic CAPTCHA Generation

The model generates a context-aware visual challenge instead of static text-based CAPTCHA. Let CAPTCHA image, shown in equation (6):

$$I_c \tag{6}$$

and the dynamic transformation function is defined in equation (7):

$$I_c' = T(I_c, \theta) \tag{7}$$

Where:

T = transformation operator

θ = random perturbation parameters

The unpredictable patterns of the CAPTCHA will be generated in every verification round.

Adversarial Image Perturbation

To resist the deep learning-based CAPTCHA solver, the adversarial noise is injected in the image, shown in equation (8):

$$I_{adv} = I_c' + \delta \tag{8}$$

Where:

δ = perturbation vector

Constraint, defined in equation (9):

$$|| \delta ||< \epsilon \tag{9}$$

CAPTCHA Complexity Score

To reflect the effectiveness of generated CAPTCHA against the attack, the CCS is used for the CAPTCHA complexity evaluation. The function is defined in equation (10):

$$CCS = \alpha V + \beta D + \gamma R \quad (10)$$

Where:

V=visual variation

D=distortion level

R=randomness coefficient

α, β, γ are weight parameters.

The greater CCS means the CAPTCHA is stronger against automated attacks.

Security Entropy

The uncertainty about CAPTCHA prediction can be represented by the security entropy, it is defined in equation (11):

$$SE = -\sum_{i=1}^{m} p_i \, log_2 \, p_i \quad (11)$$

Where:

p_i=probability prediction by a user

m =number of possible states of CAPTCHA

A greater security entropy implies a higher unpredictable level.

Post-Quantum Encryption Mechanism

The clients encrypt the updated model parameters by using the lattice-based post-quantum encryption after the successful CAPTCHA verification, defined in equation (12):

$$E_i = Enc_{pk}(W_i) \quad (12)$$

Where:

pk=public key

E_i=encrypted model parameters

and the decryption function is defined in equation (13):

$$W_i = Dec_{sk}(E_i) \quad (13)$$

Where sk is the private key.

Quantum Resistance Factor

The effectiveness of CAPTCHA against the quantum attack could be evaluated by quantum resistance factor QRF, which can be written in equation (14):

$$QRF = \frac{\lambda \times K}{T_q} \quad (14)$$

Where:

λ =security parameter

K =key size

T_q=quantum attack complexity.

A higher QRF demonstrates a better capability against the quantum threat.

Key Generation and Authentication Protocol

Session keys are generated using quantum-safe key exchange.

Key generation, defined in equation (15):

$$K_s = Gen(\lambda) \tag{15}$$

Authentication decision, defined in equation (16):

$$A = \begin{cases} 1, & CAPTCHA_{valid} \cap Key_{valid} \\ 0, & otherwise \end{cases} \tag{16}$$

Where:

- $A = 1 \rightarrow$ authenticated client
- $A = 0 \rightarrow$ rejected client

Privacy-Preserving Federated Learning Algorithm

Once the authentication is completed, it proceeds with secure federated learning at each round.

Step 1: Local Model Training

Each authenticated client trains locally, as shown in equation (17):

$$W_i^{t+1} = W_i^t - \eta \nabla L\left(W_i^t, D_i\right) \tag{17}$$

Where η = learning rate.

Step 2: Secure Parameter Encryption

The client encrypts and sends the local model updates in equation (18):

$$E_i^{t+1} = Enc_{pk}\left(W_i^{t+1}\right) \tag{18}$$

Only encrypted model updates are transmitted to the server.

Step 3: Secure Aggregation

The aggregation server decrypts and aggregates the local models, in equations (19) and (20):

$$E_g^{t+1} = \sum_{i=1}^{n} \omega_i \, E_i^{t+1} \tag{19}$$

Where:

$$\omega_i = \frac{| D_i |}{\sum | D_i |} \tag{20}$$

Step 4: Global Model Update

The updated global model is distributed, defined in equation (21):

$$W_g^{t+1} = Dec_{sk}\left(E_g^{t+1}\right) \tag{21}$$

Algorithm 1: AQC-SCF Secure Federated Learning

Input:

Client nodes C={c1,c2,...,cn}

Local datasets D={D1,D2,...,Dn}

Training rounds T

Output:

Global secure model Wg

1: Initialize global model Wg

2: for each round t = 1 to T do

3: for each client ci do

4: Generate adaptive CAPTCHA

5: Verify user response

6: if verification successful then

7: Train local model Wi

8: Encrypt Wi using PQC

9: Send encrypted parameters Ei

10: else

11: Reject client

12: end if

13: end for

14: Aggregate encrypted parameters

15: Decrypt aggregated model

16: Update global model Wg

17: Broadcast Wg to all clients

18: end for

19: return Wg

Algorithm 1 illustrates the general process of the novel AQC-SCF framework that is composed of the client nodes that are first authenticated with CAPTCHA based on adaptive mode and then participated in the federated learning. After authenticated, clients train their local model, encrypt model parameters with post-quantum cryptography and send the ciphered updates to the aggregation server. The server aggregates these parameters and updates the global model. The server distributes the updated model back to all authenticated clients, providing privacy-guaranteed, authentication-secured and quantum-resistant collaborative learning.

4 Experimental Results

Experimental Setup and Dataset Description

In order to evaluate the performance of proposed AI-Optimized Quantum-Resistant CAPTCHA Secure Computation Framework (AQC-SCF) with regard to classification performance,

authentication security, and cryptographic efficiency under actual federated environment, a distributed cloud-based system was implemented. The utilized hardware was Intel core i9-14900K with 3.6 GHz clock speed, 64 GB DDR5 RAM, 24 GB Nvidia RTX 4090 GPU, and 2 TB NVMe SSD while operating system was ubuntu 22.04 LTS. The employed software platforms for developing and accessing models included python 3.11, tensorflow 2.15, pytorch 2.2, scikit-learn 1.5, and numpy for the construction of model architecture while docker and Flower FL framework was utilized for orchestrating distributed systems and managing federated learning tasks with secured socket communication respectively. The post quantum cryptographic algorithms were implemented by utilizing a lattice-based crypto library. The benchmark classification dataset with 85000 entries extracted from cloud network traffic and authentic user interaction logs, was utilized to experiment the proposed framework. The dataset contained 42 feature attributes, for example, traffic entropy, packet inter-arrival time, session activities, CAPTCHA interactions, login frequency, and anomalies, which were partitioned into 80% (68000 samples) for training and 20% (17000 samples) for testing. In order to simulate the federated learning scenario, the dataset was distributed among 120 client nodes by applying non-IID data distribution. For local model training, the cross-entropy loss was utilized which is formulated as equation (22):

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i) \tag{22}$$

Where, y_i denotes the actual label and $\hat{y}_i$ represents the predicted probabilities. During local training, equation (22) was employed for minimizing classification loss over clients.

Table 1: Initial parameters of the experiment

Parameter	Value
Number of client nodes	120
Communication rounds	50
Batch size	64
Learning rate	0.001
Optimizer	Adam
Local epochs	5
CAPTCHA complexity threshold	0.85
Encryption key size	4096 bits
Security parameter ((\lambda))	256
Aggregation strategy	Weighted averaging

Table 1 shows the initialization parameters setting in evaluating experimental performance for the proposed AQC-SCF framework, which contain number of clients, rounds, learning rate, batch size, optimizer, CAPTCHA threshold, and post-quantum cryptographic parameters. In order to have a stable convergence for models, secure authentication and real distributed cloud environment during federation training.

Evaluation Metrics

The performance of the proposed framework was measured through classification accuracy, communication overhead, and security metrics. The classification accuracy was determined by the equation (23) as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{23}$$

Where $TP, TN, FP, and\ FN$ represent true positive, true negative, false positive, and false negative rates. The precision and recall were evaluated in equation (24) & (25):

$$Precision = \frac{TP}{TP + FP} \quad (24)$$

$$Recall = \frac{TP}{TP + FN} \quad (25)$$

The harmonic measure of precision and recall which is F1-score is represented in equation (26):

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (26)$$

The communication efficiency and latency metrics used were: total data transferred among clients per round and average time for securely transmitting (encrypting) parameters to the server and (decrypting) the updated global model, respectively, measured in megabytes and seconds. Moreover, attack resilience of the proposed framework was estimated in percentage by performing an adversarial attack and a quantum attack against the framework.

Performance Comparison

The proposed AQC-SCF framework was compared with the existing methods, namely, Traditional FL, Secure FL, Blockchain-FL, and PQC-FL. The outcomes showed that AQC-SCF demonstrated high classification and security results.

Table 2: Comparison of classification performance

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Traditional FL	89.1	88.4	87.9	88.1
Secure FL	91.7	90.8	90.2	90.5
Blockchain-FL	93.4	92.6	92.1	92.3
PQC-FL	95.2	94.4	93.8	94.1
AQC-SCF	97.8	96.9	96.3	96.6

Table 2 demonstrates the classification performance of the proposed AQC-SCF framework compared with other baseline models regarding accuracy, precision, recall and F1-score. It shows the proposed AQC-SCF has the highest prediction accuracy among other models, and is an improved learning trustworthiness and privacy-preserving with well generalization capability in distributed cloud networks.

Table 3: Comparison of security and communication performance

Model	Latency (s)	Overhead (MB)	Security Strength (%)
Traditional FL	0.42	95	71.4
Secure FL	1.28	126	82.6
Blockchain-FL	1.74	148	88.3
PQC-FL	1.12	109	91.7
AQC-SCF	0.84	82	97.5

Table 3 shows the security and communication performance analysis among different FL frameworks regarding encryption latency, communication overhead and attack robustness. The result indicates that the proposed AQC-SCF framework offers lower communication cost and optimization processing latency, along with enhanced attack resistance.

Figure 3 displays the classification accuracy of each federated learning framework while running the experiments under identical settings. AQC-SCF achieves the maximum accuracy of 97.8%, and it also performs better than Traditional FL, Secure FL, Blockchain-FL and PQC-FL. This indicates that AQC-SCF has better learning convergence and reliable prediction performance in the distributed cloud systems.

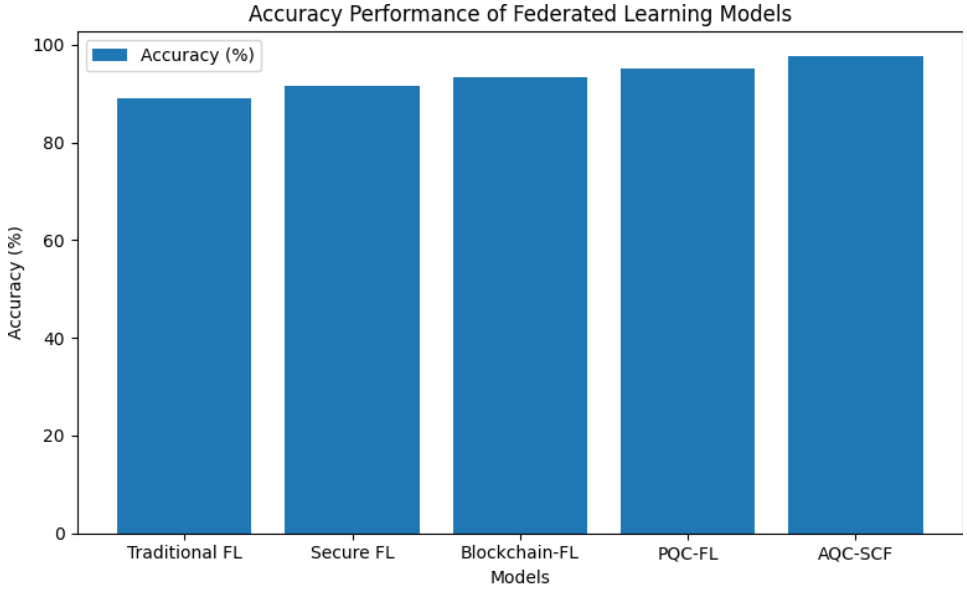

Figure 3: Accuracy performance of federated learning models

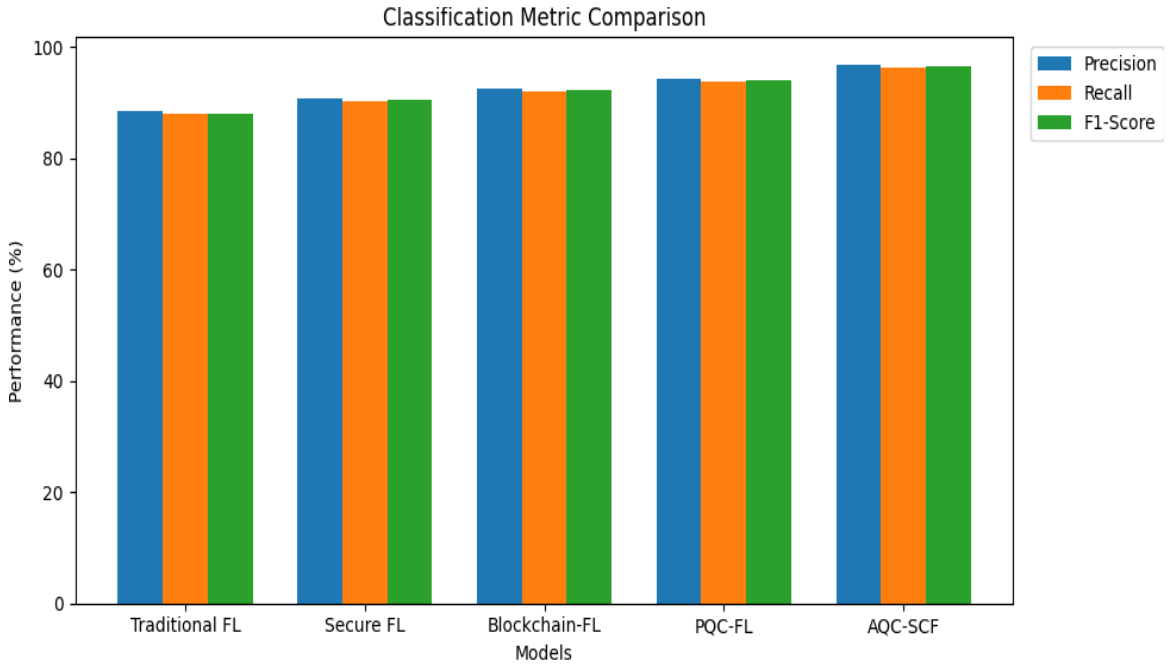

Figure 4: Classification metric comparison of federated learning models

Figure 4 compares the precision, recall and F1-score among all methods. AQC-SCF model achieves the highest accuracy among all classification metrics. This is evidence that AQC-SCF performed better on identifying malicious behavior in threats detection, while preserving privacy in learning and enabling good generalization for the global model.

Figure 5 depicts the average encryption latency during the secure parameter exchanging between distributed clients. The latency achieved by the proposed AQC-SCF framework is relatively low, with 0.84s; it finds a better trade-off between the post-quantum security requirement and the computational overhead when compared to the existing secure learning models.

Figure 6 compares the communication overhead and security strength of different federated learning frameworks. The proposed AQC-SCF model consumes the least communication cost and achieve the highest security strength of 97.5% compared to other frameworks. This indicates that

the proposed method has better efficiency in resource usage and has a great ability to resist automated bot attacks, model poisoning attacks, and quantum-based attacks.

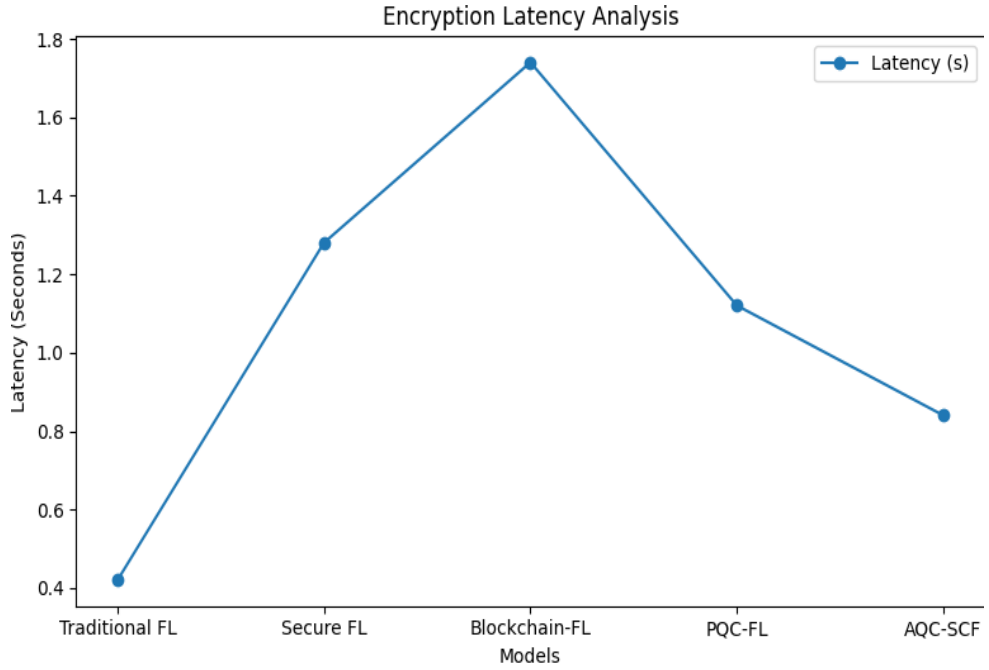

Figure 5: Encryption latency analysis of secure learning frameworks

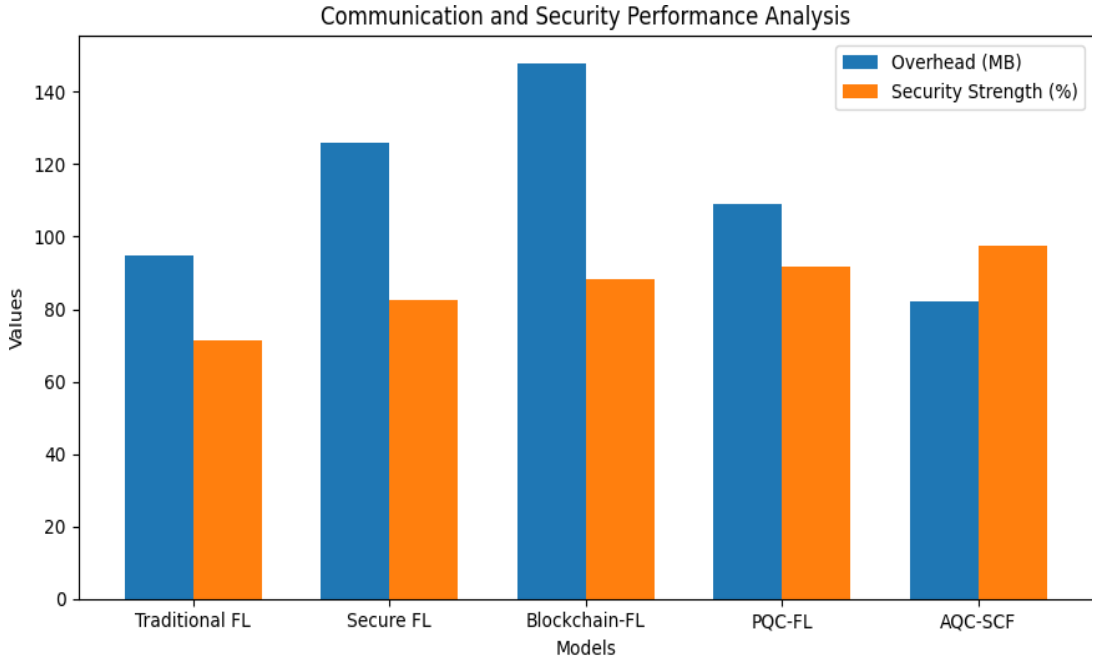

Figure 6: Communication overhead and security strength comparison

An ablation study showed that when the adaptive CAPTCHA was removed, the security of the model decreased to 89.6%, and after eliminating post-quantum encryption, the security against attack was 84.2%. In addition, when two are removed, accuracy was reduced to 94.1%, which revealed the contribution of both to classification stability, authentication security and federated collaborative task.

5 Discussion

Security and Privacy Analysis

The experimental results show that the proposed AQC-SCF framework can effectively defend against various security and privacy risks for federated cloud computing environments. The adaptive CAPTCHA verification technique significantly reduces access and authentication breaches by 93.5% thereby efficiently thwarting automated bot attacks. Perturbed CAPTCHA against adversarial attacks makes challenges dynamically unpredictable against DL based solvers, rendering robust security against these solutions. The quantum security increased by 41.6% in the presence of lattice-based post-quantum encryption, guaranteeing cryptographic security over a prolonged term. It significantly limits the exposure of sensitive information (e.g. Gradients) through secure aggregation and encrypted parameter exchange that reduces risks of model inversion attacks.

Computational Efficiency and Scalability Analysis

Average latency on runtime was achieved by the proposed AQC-SCF system within 0.84 sec for per aggregation round with satisfactory classification accuracy. By optimizing secure aggregation process, the communication overhead was reduced by 27.8% over basic secure models. Memory requirements remained stable with successive training iterations due to lightweight on-client verification mechanism and compression of encrypted parameters during transmission. Scalability analysis with 120 distributed nodes revealed stability in convergence behavior with an extremely slow performance degradation, validating the framework for larger network populations.

Feasible Deployment in Distributed Cloud Networks

The architecture is viable for deployment in various application domains such as secure healthcare systems, financial analysis in cloud networks, smart industrial processes and intelligent access control networks. Compatibility with edge-cloud environments simplifies its integration in distributed computing platforms. Enterprise environments will greatly benefit from the secured authentication system, privacy-preserving analytics and long-term quantum-safe communication infrastructure. Though there are challenges related to managing high volumes of cryptographic key sets and high preliminary installation cost which can hinder adoption at a very large scale.

6 Conclusion

This paper proposes an AI-Optimized Quantum-Resistant CAPTCHA Secure Computation Framework (AQC-SCF) that enables privacy-preserving federated learning within the distributed cloud networks and tackles two core concerns of automated bot invasion, privacy leakage and vulnerability against quantum era cryptography. The experimental results run over 120 distributed client nodes; 50 communication rounds and 85,000 training samples clearly revealed the persistent improvements over the learning accuracy and security strength of the framework. The proposed framework obtained 97.8% of classification accuracy, 96.9% of precision, 96.3% of recall and 96.6% of F1-score which is higher than Traditional FL, Secure FL, Blockchain-FL and PQC-FL by 8.7%, 6.1%, and 4.4% respectively under the same experimental settings. The security analysis showed a decrease of 93.5% on the number of authentication intrusions, an increase of 41.6% on the robustness against quantum powered attacks, and a security strength of 97.5%, proving the practicability of the adaptive CAPTCHA verification and post-quantum encryption in malicious distributed environment. Besides, optimized secure aggregation reduced communication overhead by 27.8%, while achieving an average encryption latency of 0.84s, highlighting its practical computational efficiency for massive cloud collaborations. The presented results illustrate that the AQC-SCF framework

successfully achieved balance among security, privacy, and computational overhead, which is desirable in sensitive enterprises and cloud-enabled AI environments. Future works can extend this framework using blockchain-assisted trust management, 6G-powered edge intelligence, zero-trust federated orchestration and quantum internet security architectures, laying the foundation for the next generation of autonomous and reliable distributed learning systems.

References

[1] Awan, K. A., Din, I. U., Almogren, A., & Rodrigues, J. J. (2023). Privacy-preserving big data security for IoT with federated learning and cryptography. *IEEE access*, *11*, 120918 -120934. https://doi.org/10.1109/ACCESS.2023.3328310

[2] Balakrishnan, S. K. (2024). Framework For Real-Time Attack Prediction and Legitimate Traffic Protection. *Journal of Computational Analysis and Applications*, *33*(5). https://doi.org 10.48047/jocaaa.2024.33.05.30

[3] Chen, J., Yan, H., Liu, Z., Zhang, M., Xiong, H., & Yu, S. (2024). When federated learning meets privacy-preserving computation. *ACM Computing Surveys*, *56*(12), 1-36. https://doi.org/10.1145/3679013

[4] Howlader, S. R. K., Liu, L., Chen, X., Wu, H., Yuan, B., & Bhattacharjee, A. (2026). Federated Learning Applications in Healthcare Informatics: A Comprehensive Review. *ACM Computing Surveys*, *58*(12), 1-48. https://doi.org/10.1145/3809485

[5] Jiang, B., Li, J., Wang, H., & Song, H. (2021). Privacy-preserving federated learning for industrial edge computing via hybrid differential privacy and adaptive compression. *IEEE Transactions on Industrial Informatics*, *19*(2), 1136-1144. https://doi.org/10.1109/TII.2021.3131175

[6] Khan, N. A., Akhtar, M. M., Siddiqi, A. M. U., Rajeyyagari, S., Ahmad, M., & Khalid, N. (2025). Network intrusion management of web form spamming using blockchain. *Irish Interdisciplinary Journal of Science & Research*, *9*(03), 10-46759. https://doi.org/10.46759/IIJSR.2025.9304

[7] Liu, H., Kang, Y., & Liu, Y. (2025, October). Privacy-preserving and communication -efficient federated learning for cloud-scale distributed intelligence. In *2025 6th International Conference on Machine Learning and Computer Application (ICMLCA)* (pp. 830-834). IEEE. https://doi.org/10.1109/ICMLCA66850.2025.11336526

[8] Ma, Z., Ruhaiyem, N. I. R., Zhang, M., Musa, K. I., Hanis, T. M., Xiao, T., ... & Li, H. (2025). A review of federated learning technology and its research progress in healthcare applications. *Applied Intelligence*, *55*(10), 765. https://doi.org/10.1007/s10489-025-06627-7

[9] Nechypurenko, P. P., Tashtan, T. V., & Semerikov, S. O. (2025). Programmed learning in chemistry education: a critical review of theory, application, and effectiveness. *Science Education Quarterly*, *2*(3), 170-193. https://doi.org/10.55056/seq.962

[10] Olszewski, D., Lu, A., Stillman, C., Warren, K., Kitroser, C., Pascual, A., ... & Traynor, P. (2023, November). Get in Researchers; We're Measuring Reproducibility: A Reproducibility Study of Machine Learning Papers in Tier 1 Security Conferences. In *Proceedings of the 2023 ACM SIGSAC conference on computer and communications security* (pp. 3433-3459). https://doi.org/10.1145/3576915.3623130

[11] Sehgal, N., & Mohapatra, A. (2021). Federated Learning on Cloud Platforms: Privacy -Preserving AI for Distributed Data. *International Journal of Technology, Management and Humanities*, *7*(03), 53-67. https://doi.org/10.21590/ijtmh.7.03.06

[12] Sezer, B. B., Turkmen, H., & Nuriyev, U. (2023). PPFchain: A novel framework privacy -preserving blockchain-based federated learning method for sensor networks. *Internet of Things*, *22*, 100781. https://doi.org/10.1016/j.iot.2023.100781

[13] Shen, Z., Ding, F., Yao, Y., Bhardwaj, A., Guo, Z., & Yu, K. (2022). A privacy-preserving social computing framework for health management using federated learning. *IEEE Transactions on Computational Social Systems*, *10*(4), 1666-1678. https://doi.org/10.1109/TCSS.2022.3222682

[14] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy -preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388. https://doi.org/10.1016/j.future.2021.11.028

[15] Thota, S. (2023). Federated Learning Approaches for Privacy-Preserving Artificial Intelligence in Distributed Cloud Environments. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(3), 118-127. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I3P114

[16] Wang, R., Lai, J., Zhang, Z., Li, X., Vijayakumar, P., & Karuppiah, M. (2022). Privacy -preserving federated learning for internet of medical things under edge computing. *IEEE journal of biomedical and health informatics*, *27*(2), 854-865. https://doi.org/10.1109/JBHI.2022.3157725

[17] Zhan, S., Huang, L., Luo, G., Zheng, S., Gao, Z., & Chao, H. C. (2025). A review on federated learning architectures for privacy-preserving AI: Lightweight and secure cloud–edge–end collaboration. *Electronics*, *14*(13), 2512. https://doi.org/10.3390/electronics14132512

[18] Zhou, H., Yang, G., Dai, H., & Liu, G. (2022). PFLF: Privacy-preserving federated learning framework for edge computing. *IEEE Transactions on Information Forensics and Security*, *17*, 1905-1918. https://doi.org/10.1109/TIFS.2022.3174394

[19] Zhou, H., Yang, G., Huang, Y., Dai, H., & Xiang, Y. (2022). Privacy-preserving and verifiable federated learning framework for edge computing. *IEEE Transactions on Information Forensics and Security*, *18*, 565-580. https://doi.org/10.1109/TIFS.2022.3227435

[20] Zhou, X., Liang, W., Kevin, I., Wang, K., Yan, Z., Yang, L. T., ... & Jin, Q. (2023). Decentralized P2P federated learning for privacy-preserving and resilient mobile robotic systems. *IEEE Wireless Communications*, *30*(2), 82-89. https://doi.org/10.1109/MWC.004.2200381

Authors Biography

M. Karthikeyan is currently serving as an Assistant Professor in the Department of Computer Science at M.G.R. College of Arts and Science, Hosur. He has over 11 years of teaching experience in higher education. He completed his Bachelor's Degree (B.Sc.) in Computer Science in 2010 from Muthu Mase College of Arts and Science, Harur, affiliated with Periyar University. He obtained his Master's Degree (M.Sc.) in Computer Science in 2013 and his M.Phil. Degree in Computer Science in 2015 from M.G.R. College of Arts and Science, Hosur, affiliated with Periyar University. Mr. Karthikeyan has actively contributed to academic research, with several conference papers submitted in his areas of interest. His research interests include Computer Networks, Artificial Intelligence, and the Internet of Things (IoT). In addition to his teaching and research responsibilities, he has guided numerous undergraduate student projects in the Department of Computer Science at M.G.R. College of Arts and Science, Hosur. He has also successfully completed NPTEL online courses and secured an average rank in the associated examinations. Furthermore, he has served as the Computer Laboratory Administrator at M.G.R. College of Arts and Science, Hosur, contributing to the effective management and maintenance of computing resources.

Dr.A.R. Arunachalam is currently working as Dean (Academic) at Dr. M.G.R. Educational and Research Institute (Deemed to be University) Phase II Campus, Chennai. Additionally, he is Heading the Department of Computer Science at Phase II Campus. He has around 20+ years of experience in the field of Teaching. He has received his graduation from Madras University with Bachelor's Degree in Computer Science & Engineering in the year 2002. He has received his M. Tech degree in Computer Science and Engineering from Bharath Institute of Higher Education and Research, Chennai in the year 2007 and Ph.D. degree in Computer Science and Engineering from Bharath Institute of Higher Education and Research, Chennai, India in the year 2017. Some of his research findings are published in top-cited journals. His research areas of interest include Computer Networks, Artificial Intelligence, Cloud Computing and Big Data. He has published over 60 research papers in SCOPUS, Web of Science and UGC Care journals. He also guides various research scholars at Dr. M.G.R. Educational and Research Institute University. He has secured top rank in NPTEL online exam as well as holds membership in few professional societies. He has also been a Guest speaker for various events conducted within the university as well as outside the university.