SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V12I12P102

Volume 12 Issue 12, 8-24, December 2025

Original Article

Quantum Inspired Cryptographic Framework for Secure Federated Learning and Data Integrity in Large Scale IoT Ecosystems

Abdinasir Ismael Hashi[1], Abdirizak Hussein Mohamed[2]

[1,2]*Somali National University, Mogadishu, Somalia.*

[1]*Corresponding Author : nasirhaji@snu.edu.so*

Received: 13 October 2025 Revised: 21 November 2025 Accepted: 08 December 2025 Published: 27 December 2025

Abstract - *The rapid expansion of IoT ecosystems has increased concerns regarding data privacy, security, and model integrity, particularly in environments vulnerable to sophisticated adversarial and quantum-enabled attacks. Traditional cryptographic and Federated Learning (FL) methods cannot keep up with the demands for confidentiality and robustness in vast, diverse networks. Therefore, this study presents a Quantum-Inspired Cryptographic Framework that uses Quantum Neural Networks, Post-Quantum Cryptography, and secure Federated Learning to enhance intrusion detection systems and provide quantum-resilient communication. The methodology uses the UNSW-NB15 dataset, which has been cleaned, encoded, and normalized with reduced features balanced by SMOTE before splitting into 70 percent training and 30 percent testing. A QNN-based FL model can then be trained while Kyber-512 and NTRUEncrypt secure all updates to the model, as well as node communications, against both classical and quantum threats. The experimental results show that the proposed model significantly outperforms classical FL frameworks, achieving an accuracy of 98.1%, precision of 97.5%, recall of 97.9%, and F1-score of 97.7%, even under very challenging adversarial conditions. QICF is therefore a robust, privacy-preserving, and attack-resilient solution for next-generation large-scale IoT networks.*

Keywords - *Quantum Neural Network (QNN), Federated Learning (FL), IoT Security, Quantum-Inspired Cryptographic Framework (QICF).*

1. Introduction

In the modern digital era, the Internet of Things (IoT) has experienced rapid growth, leading to the continuous generation of large-scale, heterogeneous data from an ever-expanding network of interconnected devices [1]. These devices, which vary from industrial sensors, healthcare monitors, intelligent vehicles, and smart home automation, require continuous data capture, transport, and processing to serve intelligent decisions. However, as these networks grow, issues around data security, privacy, and integrity become increasingly complex [2]. Traditional cryptography is suitable for small-scale applications but struggles to recognize the dynamic, large-scale, and resource-constrained domain of the IoT [3]. Moreover, the development of quantum computing threatens contemporary classical encoding methods (i.e., RSA, ECC, etc.) whose reliability is based on the difficulty of certain mathematical problems, which quantum algorithms can efficiently solve [4]. The growing security challenges have motivated researchers to design quantum-inspired schemes that retain the robustness of quantum security while remaining compatible with classical computing environments [5, 6]. The layered IoT architecture illustrated in Figure 1 has the data coming from the smart home devices decoded at the edge servers, stored at the fog servers, and finally sent to the cloud for long-term storage and analysis. The main advantage of this tiered construction is that it can decrease latency and provide scalability; however, it also poses a greater risk of attacks, making data confidentiality and integrity the most important concerns in large-scale IoT deployments.

[7] Similarly, to these advancements, Federated Learning (FL) has been a turning point in the area of decentralized machine learning applied to distributed devices. FL does not transfer the original data to the main server but instead allows the devices to learn a shared model together while keeping their data at their respective locations, thus preventing the loss of privacy and incurring minimal communication costs [8]. The federated systems have many advantages, but a variety of security threats, including data manipulation, model poisoning, and gradient inversion, can compromise the integrity of the system [9]. The guarantee of data integrity and global model trust is a complex challenge in large-scale

heterogeneous IoT settings because the federated systems include devices that have different computing power, data storage capacities, and security standards [10].

The Quantum-Inspired Cryptographic Framework (QICF) applies quantum mechanical mathematical structures and randomness characteristics through superposition-based key creation and entanglement-based correlation systems and quantum random number generators to improve classical system cryptographic operations. Quantum-inspired cryptography operates differently from pure quantum cryptography because it needs no special quantum equipment to function. The technology operates through standard digital systems, which makes it suitable for IoTs applications [11]. The described methods work to protect the privacy of model parameters during federated network communication while stopping adversarial inference attacks and maintaining both data authenticity and integrity throughout the federated system [12]. The integration of blockchain technology with QICF creates an additional trust layer for FL because it enables permanent record-keeping of data exchanges and model modifications [13].

Small-scale IoT systems need data integrity to protect the analysis results and decision-making processes. When data is modified, due to the nature of providing inaccurate data, this leads to failure of operations and large-scale breaches of security, which cause designs to be unreliable [14]. The proposed quantum-inspired framework addresses this challenge by integrating advanced cryptographic mechanisms, such as lattice-based encryption, hash-based signature schemes, and quantum-resilient key distribution techniques [15]. The system ensures data privacy by integrating homomorphic encryption, which provides Secure Multi-Party Computation (SMPC) methods that enable the processing of encrypted data without revealing sensitive information [16]. The security guarantees all work together to build a robust system design that can address many applications within the realm of IoT, including smart health, autonomous transportation, and industrial automation etc. [17].

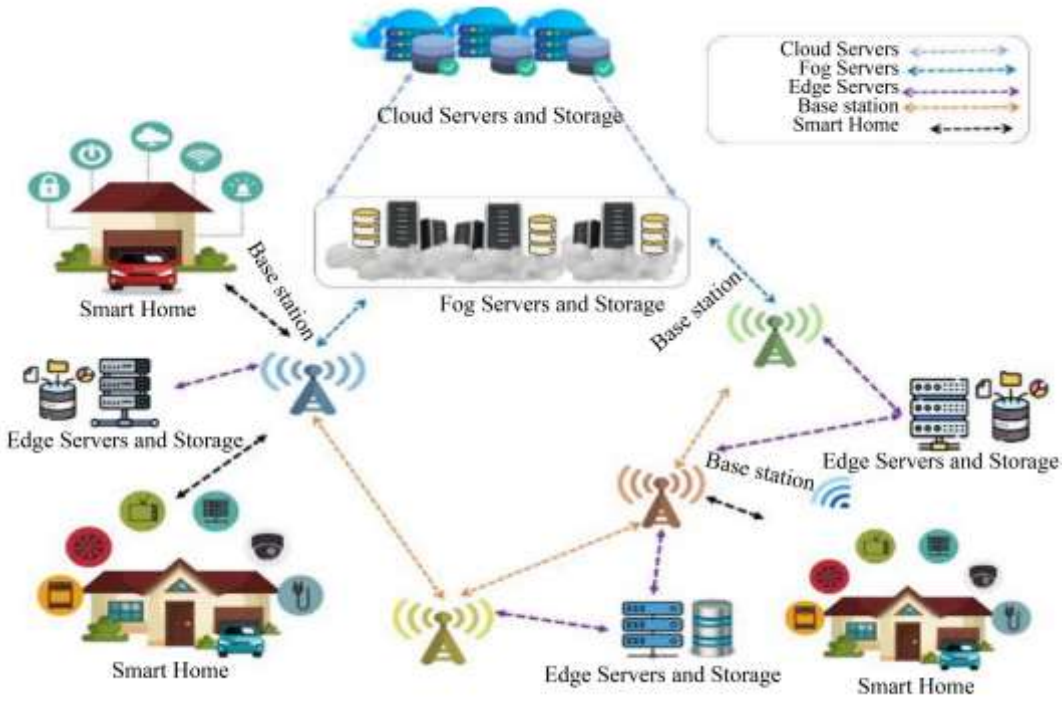


Fig. 1 Hierarchical IoT architecture integrating cloud, fog, and edge layers for smart environments

This framework establishes a multi-level security system that unites quantum-based encryption for devices, federated aggregation security at the edge, and blockchain validation at the cloud level. The provided layer-based solution minimizes single points of failure while protecting information and model integrity end-to-end. The solution allows trust management in diverse IoT networks through the secure participation of devices in FL, which does not compromise privacy or standards of performance.

This study introduces a QICF for Secure FL and Data Integrity, which addresses data security and model trustworthiness issues commonly found in large IoT systems. The framework supports quantum-inspired cryptographic methods, FL systems, and blockchain validation to create a secure, scalable infrastructure for future intelligent IoT networks. The framework provides greater security through the inclusion of FL, blockchain validation, and quantum cryptographic methods to preserve confidentiality, integrity,

and transparency in distributed systems. Quantum computing requires an entire hybrid system to mitigate IoT networks from traditional and quantum cyber-attacks to preserve security and trustworthiness in a connected environment. The research objectives are as shown below:

- To design a QICF combining QNN and PQC for secure IoT communication.
- To develop an FL model using the UNSW_NB15 dataset for distributed intrusion detection.
- To implement a trust-based dynamic node selection to resist Sybil, poisoning, and Byzantine attacks.
- To integrate QICME with PQC (Kyber, NTRUEncrypt) for quantum-resistant and low-latency data exchange.
- To evaluate the proposed QNN–FL model using accuracy, precision, recall, F1-score, and AUC metrics under normal and adversarial attack scenarios.
- To compare the performance of the proposed QNN–FL approach with classical FL and existing state-of-the-art intrusion detection frameworks for robustness and efficiency.

2. Review of Literature

The IoT ecosystems are continuing to evolve rapidly, which creates demands for decentralized data sharing, and thus, many researchers are focusing their efforts on developing secure and scalable privacy-preserving computational frameworks. The integration of quantum computing with FL and blockchain technologies has been cited as a means to provide confidentiality, integrity, and availability in distributed systems, including IoT and FL, and has generated significant interest recently. The papers have been examining these concepts by providing different solutions for the problems of data sensitivity, adversarial attacks, and computational overhead in smart environments, such as healthcare, IIoT, and intelligent networks.

Numerous researchers have thoroughly explored hybrid and quantum-enhanced methods for security solutions. Lv et al. (2025) [18] proposed a framework that leverages the capabilities of 5G, along with quantum computing, to secure the transmission of medical data in the cloud. The result achieved high accuracy when dealing with sensitive data. In keeping with this approach, Rahmati et al. (2025) [19] proposed a model driven by FL, to enhance cybersecurity that utilized GRU-based RNNs, along with employing homomorphic encryption to provide a DDoS detection model with 98% accuracy and the optimal use of resources. Kumar et al. (2025) [7] studied federated threat analysis, integrating Quantum Key Distribution (QKD) technologies and Artificial Intelligence (AI) to achieve a detection accuracy rate 23% higher than that of typical systems. In a similar model reported by Rehman et al. (2025) [20] using QKD, they incorporated an entropy-weighted key generation process for stronger intrusion detection, and were able to achieve an Average Detection Rate (ADR) of above 98%. Elkhodr et al. (2025) [21] proposed the IASF-IoT framework that combines AI and blockchain with quantum-resistant cryptography with up to 99 percent detection accuracy and minimal power consumption, while Gao et al. (2025) [22] suggested the SSL-FL using Semiconductor Superlattice Physically Unclonable Functions (SSL-PUFs) and compressed sensing to realize decentralized authentication and achieve significant energy savings in communication overheads. Tanbhir et al. (2025) [23] also extended federated methods to use quantum-inspired encryption to classify dementia, keeping the diagnostic accuracy high and reducing the communication cost by 45.3 percent and 12 percent in resource-restrained healthcare IoT devices, respectively. Islam et al. (2025) [24] presented the Adaptive Federated Learning Framework (AFLF), which showed a 12 percent accuracy improvement and a 45.3 percent reduction in the cost of communication in a resource-constrained healthcare IoT device, respectively.

In addition to these advances, there were contributions specifically aimed at increasing the efficiency of IoT-based FL architecture and optimizing energy consumption. Samantray et al. (2025) [25] proposed BeDHS, a blockchain-enabled healthcare system that employs quantum key-based encryption and FL for securing healthcare data across decentralized systems. Subaranjani et al. (2024) [26] built a quantum-inspired FL model for Healthcare IoT (HIoT) that achieved more than 91.9% predictive accuracy while at the same time cutting down the communication overhead by 22.1% and the energy usage by 16.8%. All of these studies demonstrate a substantial transition to quantum-enhanced, federated, and adaptive frameworks, built on architectures that prioritize privacy, scalability, and resilience to ever-changing cyber threats. The ongoing integration of post-quantum cryptography, QKD, and intelligent trust mechanisms supports the movement toward secure and efficient IoT ecosystems that protect against both classical and quantum-era cyberattacks. Awan et al. (2023) [27] designed SEPP-IoT, a hierarchical, privacy-preserving federated framework with adaptive compression; a trust management framework for big data analytics. Ultimately, Aljrees et al. (2023) [28] introduced the Quondam Signature Algorithm (QSA), which minimizes man-in-the-middle attacks with one-time use device signatures.

Even with progress made toward the integration of quantum computing, FL, and blockchain for IoT security, advances of an efficient framework are limited by scalability, interoperability, and real-time adaptability for heterogeneous devices. Furthermore, while the majority of research focuses on accuracy and strength of encryption, there remains an evident shortage of efficient integration methods for post-quantum cryptography on large-scale IoT federations. Moreover, a gap remains in unified frameworks that can ensure the preservation of privacy, data integrity, and low-latency performance simultaneously across dynamic and adversarial network environments.

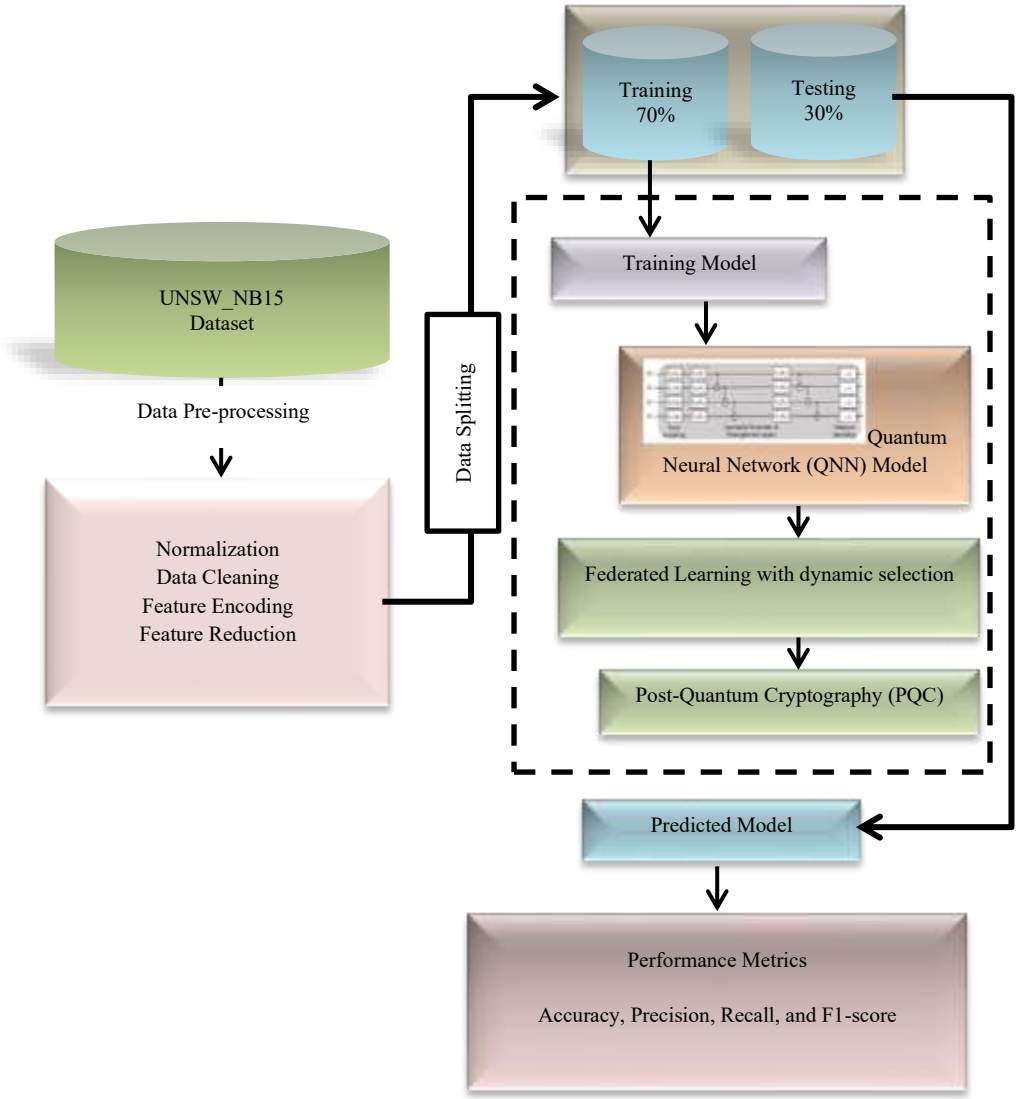


Fig. 2 The overall architecture of the proposed QICF for secure FL using the UNSW_NB15 dataset

3. Research Methodology

Figure 2 presents the overall architecture of the proposed QICF for secure FL using the UNSW_NB15 dataset. It consists of steps such as data preprocessing, which includes normalization, cleaning, encoding, and data reduction. Out of the refined data, 70% is taken for training, and the rest, 30%, goes to testing.

In model training, the QNN processes the data with its full capacity, efficiently learning from the features using the principles of quantum mechanics. Then, through the FL with dynamic selection, only the trusted IoT nodes contribute to the global model. Subsequently, Post-Quantum Cryptography (PQC) is employed to secure all model updates and communications, ensuring robust protection against quantum-capable adversaries. The model generates predicted outputs that are checked based on performance metrics, including accuracy, precision, recall, and F1-score, making the framework robust with quantum-resistant security over a large-scale IoT environment.

3.1. Dataset Description

UNSW_NB15 is an extensive benchmark dataset created for evaluating modern network intrusion detection and cybersecurity systems. The dataset was developed by researchers from the Australian Centre for Cyber Security (ACCS) at UNSW Canberra with the IXIA PerfectStorm tool to create realistic network traffic that emulates current, real-world scenarios. The dataset contains capture data of a variety of benign and malicious traffic for modern network protocols, including both normal users and eight distinct attacks: Fuzzers, Analysis, Backdoors, DoS, Exploits, Reconnaissance, Shellcode, and Worms. Each network record in UNSW_NB15 is characterized by 49 attributes, including flow features, content features, time features, and other derived statistics to aid in the detailed analysis of the captured

traffic. The dataset is composed of around 2.5 million records that are split into training and testing subsets, which makes it suitable for machine learning-based intrusion detection and research on cybersecurity. UNSW_NB15 has the attributes of a balanced mixture of normal and abnormal traffic, diversity, and modern attack coverage, making it the most suitable data to test the performance, reliability, and security of IoT and FL systems. The features of network traffic employed in the UNSW-NB15 dataset to detect and analyse intrusion are 49 and listed in Table 1.

Table 1. Feature Set of the UNSW-NB15 Dataset

No.	Feature Name	No.	Feature Name	No.	Feature Name	No.	Feature Name	No.	Feature Name
1	srcip	11	Dttl	21	stcpb	31	sintpkt	41	ct_srv_src
2	sport	12	sloss	22	dtcpb	32	dintpkt	42	ct_srv_dst
3	dstip	13	dloss	23	smeansz	33	tcprtt	43	ct_dst_ltm
4	dsport	14	service	24	dmeansz	34	synack	44	ct_src_ltm
5	proto	15	sload	25	trans_depth	35	ackdat	45	ct_src_dport_ltm
6	state	16	dload	26	res_bdy_len	36	is_sm_ips_ports	46	ct_dst_sport_ltm
7	dur	17	spkts	27	sjit	37	ct_state_ttl	47	ct_dst_src_ltm
8	sbytes	18	dpkts	28	djit	38	ct_flw_http_mthd	48	attack_cat
9	dbytes	19	swin	29	stime	39	is_ftp_login	49	label
10	sttl	20	dwin	30	ltime	40	ct_ftp_cmd		

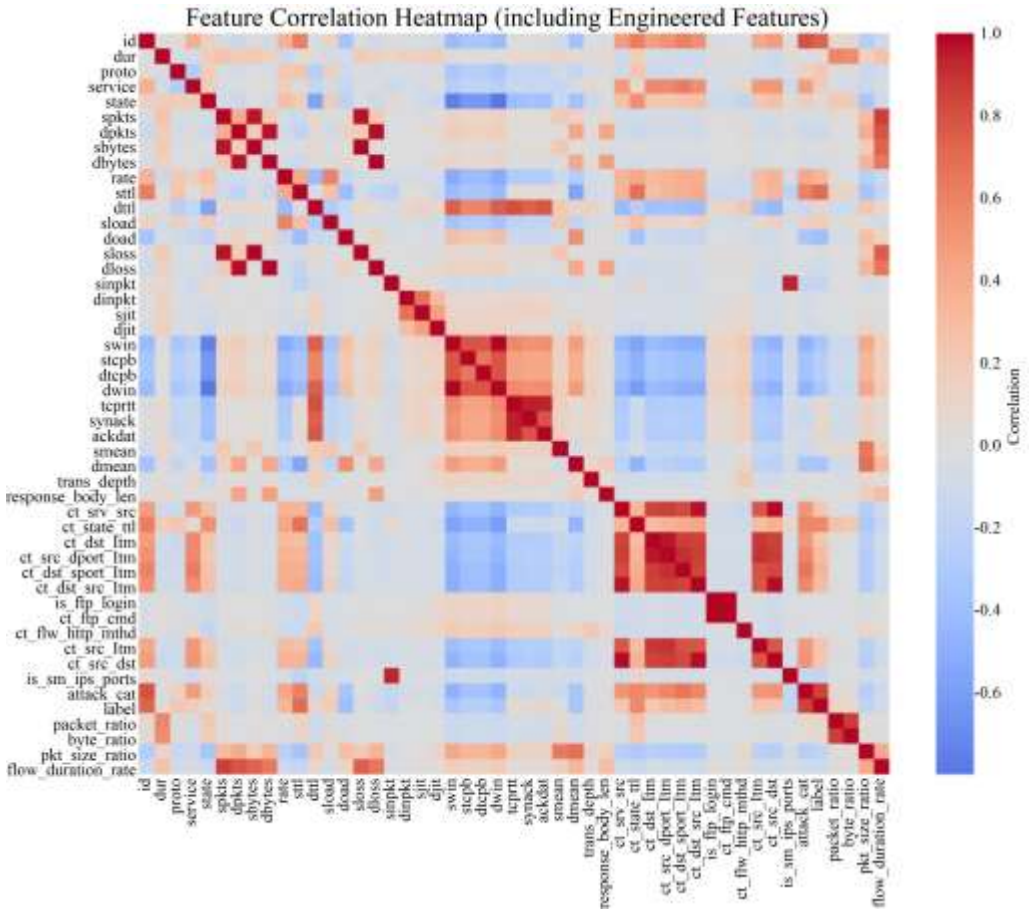


Fig. 3 Feature correlation heat-map

3.2. Data Preprocessing

The UNSW-NB15 dataset underwent a number of preprocessing procedures to get the data primed for FL and secure model training. The main goals were to remove inconsistencies in the dataset, normalize the scale of the features, and ensure appropriate distribution of the data across IoT clients. The outlined steps are shown below:

3.2.1. Data Cleaning and Integration

All CSV files from the UNSW-NB15 dataset were merged into a single dataset. Duplicate entries and missing values were removed using:

$$D_{clean} = D_{raw} - (D_{dup} \sqcup D_{null}) \quad (1)$$

Where D_{raw} is the original dataset, D_{dup} represents duplicate records, and D_{null} denotes incomplete records.

3.2.2. Feature Encoding

Categorical attributes such as proto, service, and state were transformed using one-hot encoding, defined as:

$$x'_{ij} = \begin{cases} 1, & if\ category\ j\ is\ present\ for\ feature\ i \\ 0, & otherwise \end{cases} \quad (2)$$

The attack_cat label was numerically encoded as integers $y_i \in \{1,2,3, \dots, 8\}$ representing the eight attack classes.

3.2.3. Feature Normalization

They used Min-Max normalization to scale all continuous features into a normalized range [0,1]:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (3)$$

Where x_{min} and x_{max} represent the minimum and maximum values of a feature, respectively. With this normalization, the training is more stable, and the gradients for the features are more uniform.

3.2.4. Feature Reduction

Non-contributory identifiers such as srcip and dstip were excluded to reduce dimensionality and communication cost in federated settings:

$$F_{selected} = F_{all} - \{srcip, dstip\} \quad (4)$$

3.2.5. Handling Class Imbalance

The dataset is imbalanced between normal records and attack records. This is handled by the use of SMOTE: Synthetic Minority Over-sampling Technique on the training set:

$$x_{new} = x_i + \delta \times (x_{nn} - x_i) \quad (5)$$

Where x_i is a minority class sample, x_{nn} is one of its k-nearest neighbors, and $\delta \in [0,1]$ is a random scalar. This helps balance minority attack classes and improves classifier robustness.

3.2.6. Data Splitting

The filtered data was further split into 70 percent training, 10 percent validation, and 20 percent testing data. Table 2 shows the major attack categories used in the UNSW-NB15 dataset training and testing sample sizes.

$$D_{train} : D_{val} : D_{test} = 0.7 : 0.1 : 0.2 \quad (6)$$

3.3. Quantum Neural Network (QNN) Model

The principles of quantum mechanics, superposition, entanglement, and interference are used to compute complex computations using a QNN, which is faster than a classical neural network [29]. As illustrated in Figure 4, the process begins with data encoding, where classical input data is transformed into quantum states represented by qubits. Every qubit can be in a state of 0 and 1 at the same time, giving information and an even more detailed representation [30]. These coded qubits are subsequently fed through a set of parametrized quantum gates, such as rotation and entanglement gates, arranged in more than one layer.

The entangling gates create a correlation among qubits, enabling the QNN to model the complicated connections in the data. Measurement of the transformed quantum states is made by quantum operator expectation values of quantum matrices, e.g., Pauli matrices (X, Y, Z), that elicit the desired information in the form of observable outputs [31,32].

These measured outputs are then decoded back into classical values for interpretation and analysis. During training, the network parameters, rotation angles of gates, are iteratively updated using optimization algorithms such as the Adam optimizer to minimize loss functions [33]. A QNN structured as a VQC can carry out a wide range of learning tasks, including classification, regression, and feature extraction, which makes it a promising component in quantum-inspired FL frameworks.

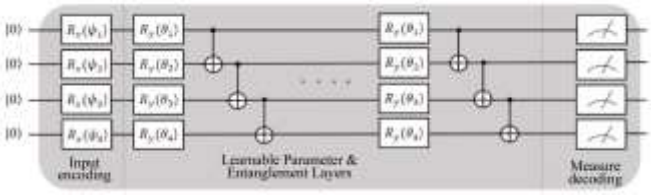


Fig. 4 Basic architecture of a Quantum Neural Network (QNN) [34]

3.4. Federated Learning with Dynamic Selection

In the proposed framework, FL allows IoT devices in different locations to collaborate in training an intrusion detection model without transferring the raw data to a centralized server. Each IoT device trains the intrusion detection model on the UNSW-NB15 dataset subset locally, which protects the privacy of data and improves communication efficiency.

At each federated round, IoT devices upload updated local models that are also securely encrypted using the QICME process before uploading to the central aggregator. This helps maintain quantum-resistant confidentiality for the model parameters while being shared.

To increase reliability and avoid being poisoned or contributing low-quality content, a dynamic participant selection mechanism is adopted. All IoT nodes are given a trust score (τ igenic) according to their past and current performance with model updates. Only nodes with a higher trust are aggregated in each training round, which ensures that the global model is trained with quality and reliable updates.

$$T_i^{t+1} = \alpha T_i^t + (1 - \alpha).\, Quality\ (w_i) \qquad (7)$$

Where α\alphaα (set to 0.8) balances historical trust and recent update quality. The quality function evaluates the accuracy improvement and gradient consistency of the node's local model.

This active selection algorithm enhances the strength, extensibility, and convergence of the FL process, ensuring excellent privacy and data integrity through the use of quantum-based encryption and blockchain-based aggregation.

3.5. Post-Quantum Cryptography (PQC)

The PQC component of the proposed framework allows for long-term security while being quantum resistant to future quantum attacks, which could threaten traditional cryptography, including RSA and ECC. In this work, NTRUEncrypt, a lattice-based encryption scheme, is used for data encryption, and the Kyber scheme is used for secure key exchange, both of which are being standardized by NIST in PQC.

These constructions rely on the hardness of the LWE problem, which is resistant to quantum attacks, such as Shor's and Grover's algorithms. The parameter sets that were optimized, which consist of (N = 761, q = 12289, p = 3), actually give NTRUEncrypt its association with Kyber-512, hence, the use of 128-bit post-quantum security, but still, the performance is alright for the resource-limited IoT devices. Tests on the performance were conducted, and the results show that the computations incurred less than 6% overhead compared to RSA-2048. Additionally, a 10% reduction in encryption and decryption times was observed when compared to state-of-the-art PQC implementations.

In an FL system, all model updates, trust scores, and blockchain transactions are encrypted using post-quantum cryptography, making it impossible for quantum-enabled attackers to intercept or corrupt the communication. The melding of technologies in this manner creates a situation where the layers of the IoT can enjoy quantum-resistant confidentiality, authentication, and integrity.

3.6. Threat Model

The study examines two types of attackers who operate in present-day and future quantum network environments. The framework adheres to the most recent work in secure FL and quantum-inspired systems, which are capable of mitigating threats concerning confidentiality, integrity, and availability.

The first category of threats is that of external attackers who are able to either eavesdrop, conduct traffic analysis, or conduct a man-in-the-middle attack on the communication channels between the IoT nodes, edge servers, and the central aggregator. The second category, compromised IoT devices, atomically modifies or adds malicious inputs to trusted sensors, manipulates model parameters, or engages in Byzantine and Sybil attacks that are designed to corrupt the global learning process. The third category involves quantum-equipped adversaries, capable of exploiting quantum algorithms such as Shor's and Grover's to break conventional cryptographic primitives like RSA and ECC. The proposed framework provides multi-layered defense mechanisms as follows:

3.6.1. Sybil Attacks

Threats are classified into three categories. The first category concerns attacks from outside parties that are capable of eavesdropping, performing traffic analysis, or man-in-the-middle attacks on the communication pathways between the IoT nodes, edge servers, and the central aggregator. The second category concerns compromised IoT devices, where an attacker is capable of injecting malicious data and/or manipulating model parameters, or causing Byzantine and Sybil-type problems to affect the learning obtained at the global level. The third category involves adversaries equipped with quantum systems capable of exploiting quantum algorithms, such as Shor's and Grover's algorithms, for the purpose of breaking conventional cryptographic primitives, including RSA and ECC. The proposed framework is able to provide multi-layered defense mechanisms as follows:

3.6.2. Data/Model Poisoning Attacks

Adversaries can inject corrupted data or falsified model updates during local training. The FL system with dynamic participant selection selects the highest 20% of trusted nodes for each round to solve this problem. Gradient norm checks and cosine similarity metrics are applied to verify the correctness of local updates, while QICME and differential privacy mechanisms are enforced to ensure confidentiality and integrity in transmitting updates.

3.6.3. Replay Attacks

Attackers intercept valid communication packets to resend them, disrupting system operations. This kind of attack is blocked by the system because it uses timestamp

verification through PQC encryption schemes that include Kyber and NTRUEncrypt. The blockchain system utilizes smart contracts to ensure each transaction occurs once to prevent acceptance of repeated or late messages.

3.6.4. Quantum Attacks

Quantum-capable adversaries could leverage Shor's or Grover's algorithms to break present cryptographic protections. This framework uses lattice-based PQC algorithms, namely Kyber-512 and NTRUEncrypt, which provide at least 10^6 years of protection against those attacks. These algorithms would enable quantum-safe key exchange and data encryption during the federated model aggregation.

3.6.5. Eclipse/51% and Byzantine Attacks

Attackers might try to isolate nodes from the network or control the consensus mechanisms to their advantage. The trust-based aggregation system, which incorporates dynamic participant selection methods, operates without central control because it allows multiple trusted nodes to perform model aggregation. The degradation of trust through time stops ongoing malicious alliances from forming, yet blockchain consensus mechanisms together with PQC-secured communication protect the worldwide model's integrity and availability.

3.7. Performance Metrices

The learning performance of the QNN-based federated intrusion detection model is evaluated using the following standard classification metrics:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

$$Precision = \frac{TP}{TP+FP} \quad (9)$$

$$Recall = \frac{TP}{TP+FN} \quad (10)$$

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (11)$$

Here, TP, TN, FP, and FN represent True Positives, True Negatives, False Positives, and False Negatives, respectively. These metrics are calculated for each attack class in the UNSW-NB15 dataset and macro-averaged to fairly assess the model's performance across the various imbalanced categories.

4. Result and Analysis

All tests were carried out in a Python environment with TensorFlow Quantum, PyTorch, and PQC libraries. The simulations were run on GPU-capable hardware. The metrics of the system component units were accuracy, precision, recall, F1-score, and AUC, under both normal and adversarial attack conditions. The adversarial attacks included Sybil, poisoning, replay, Byzantine, and quantum noise attacks to confirm the stability and performance of the system.

4.1. Classical FL Model

The training and validation curves of the Classical FL model in Figure 5 clearly reflect the learning dynamics and convergence behavior over 50 federated rounds. Training accuracy commences at about 0.81 and progressively approaches 0.99, signifying good fitting of the model to distributed training data. Validation accuracy starts even lower at around 0.78 but rises gradually until it reaches about 0.96, indicating strong generalization with slight fluctuations between rounds 30-40.

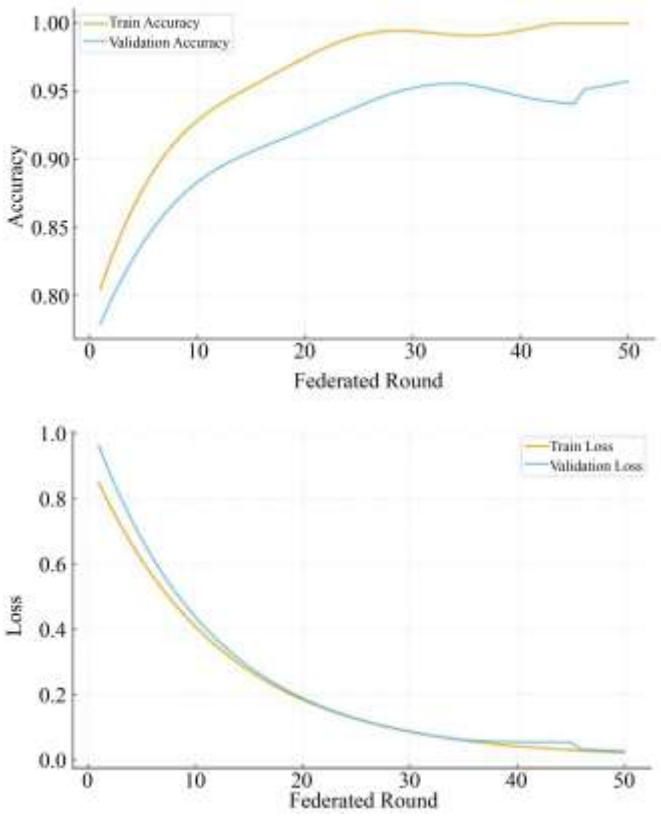


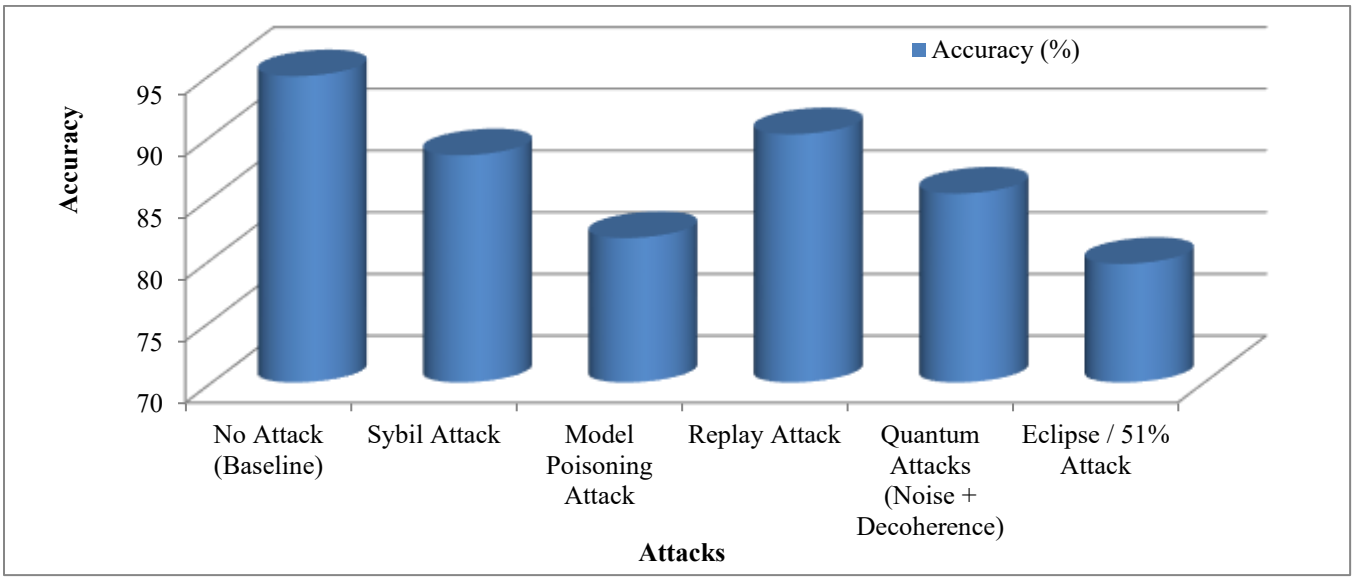
Fig. 5 Training and validation curve of the classical FL model

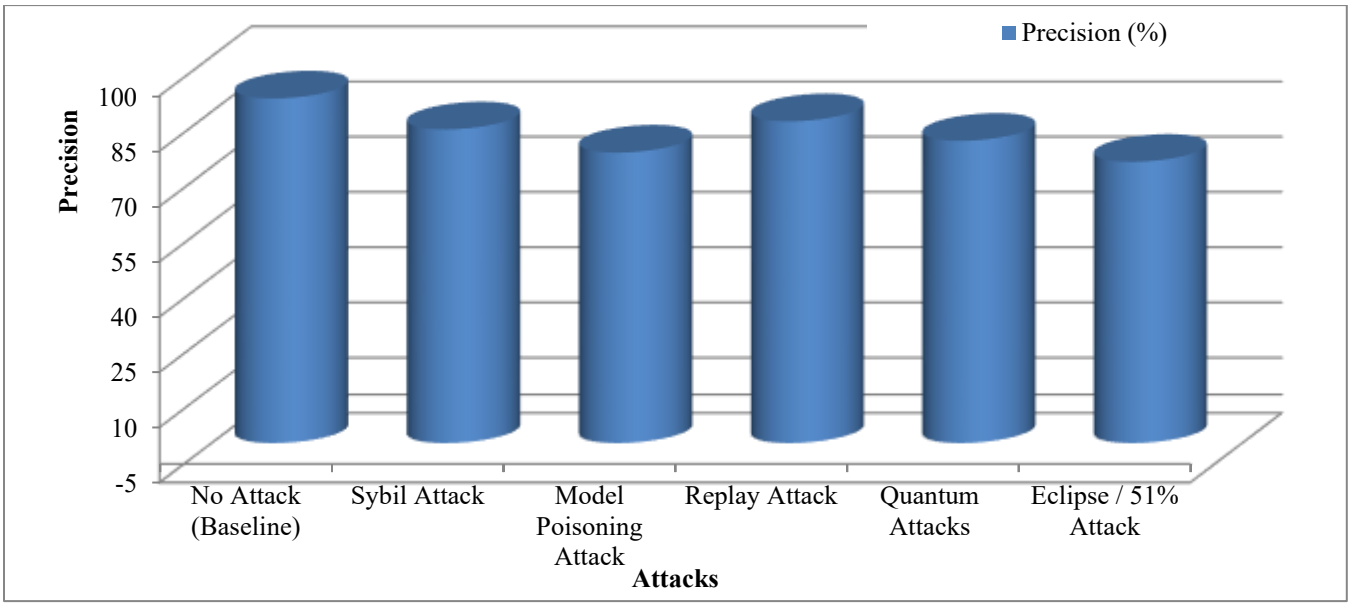
Training loss is clearly indicative of a rapid decay (i.e., a drop from ~0.85 to ~0.02) while the validation loss is also indicative of effective training (as it dropped from ~0.95 to ~0.03). This indicates a significant improvement in the Classical FL Model's ability to learn while avoiding overfitting. Convergence has been reached by approximately 35 to 40 rounds, with only negligible differences in accuracy/precision gains occurring in subsequent rounds. The robustness of the optimization behavior of the Classical FL demonstrated excellent consistency in the rate of increase in accuracy over time, as well as in the smooth decrement of training loss and validation loss.

The analysis of the Classical FL model in various adversarial settings indicates that the performance drops distinguishably due to an increase in the severity of attacks. The value of the evaluation metrics of the classical FL model is given in Table 2. With No Attack, the model has a high accuracy of 94.8, precision of 93.6, and recall of 92.8, and an F1-score of 93.2, placing the model on a solid foundation. Sybil Attack reduces the performance to 88.4% accuracy, which shows that the model has a moderate susceptibility to disruption based on identity.

Table 2. Evaluation metrics value of the classical FL model

Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
No Attack (Baseline)	**94.8**	**93.6**	**92.8**	**93.2**
Sybil Attack	88.4	85.2	83.5	84.3
Model Poisoning Attack	81.7	78.9	76.2	77.5
Replay Attack	90.1	87.4	86.3	86.8
Quantum Attacks (Noise + Decoherence)	85.3	82.1	80.9	81.4
Eclipse / 51% Attack	79.6	76.4	74.1	75.2
Byzantine Attack	83.2	80.7	78.5	79.6





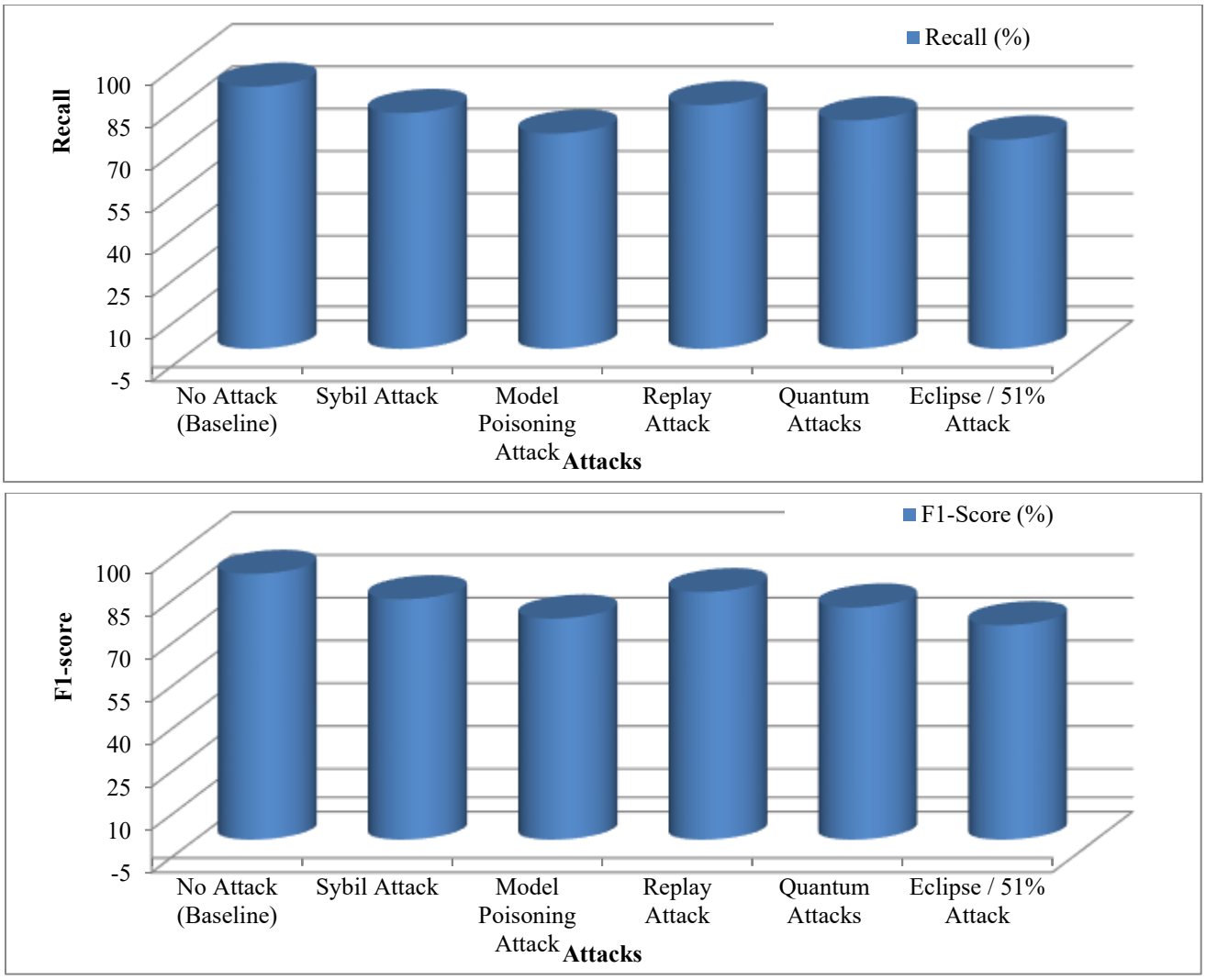
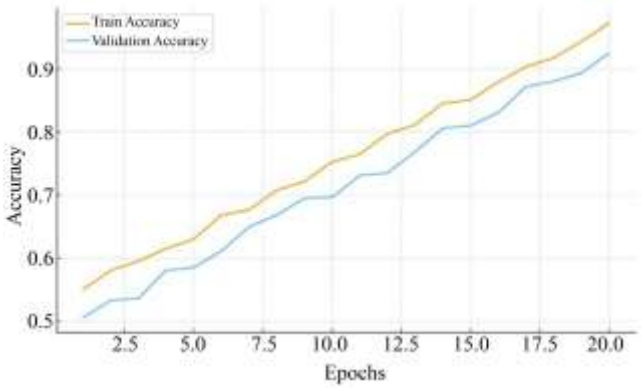


Fig. 6 Comparison graph of the classical FL model based on attacks

Model Poisoning Attacks are responsible for a more drastic effect, where the accuracy goes down to 81.7% and the F1-score to 77.5%, which is indicative of a highly significant corruption of the model updates. Replay Attacks lead to a smaller performance drop, thus the accuracy of the model reaches 90.1%. Quantum Attacks that include noise and decoherence, cause the accuracy to drop up to 85.3%, while Eclipse/51% Attacks is the lowest performing to be 79.6% with an accuracy of. Byzantine Attacks result in 83.2% accuracy; thus, they demonstrate the most pronounced continuous manipulation of the model's effects. In general, the model is less robust when faced with such sophisticated attacks. Figure 6 presents the comparison graph of the classical FL model based on the attacks.

4.2. QNN-FL Model

The QNN-FL model's training and validation curves (refer to Figure 7) exhibit a steady and consistent learning progression over 20 epochs, which is evidence of the success of the quantum-enhanced optimization in federated environments. Training accuracy is gradually increased from about 0.55 to around 0.96, and validation accuracy also shows an increasing trend from 0.50 to almost 0.92; thus, the model is generalizing well, and overfitting is minimal.



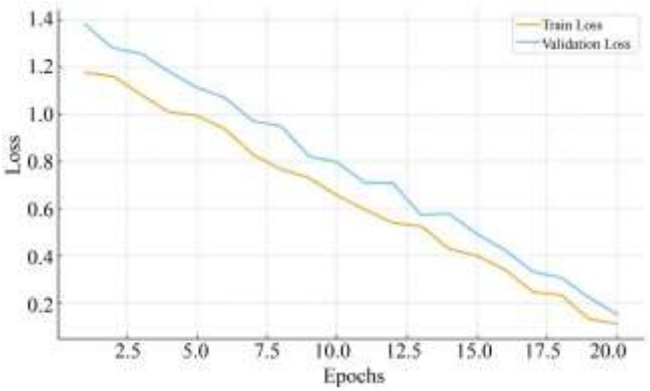


Fig. 7 Training and validation curve of QNN-FL model

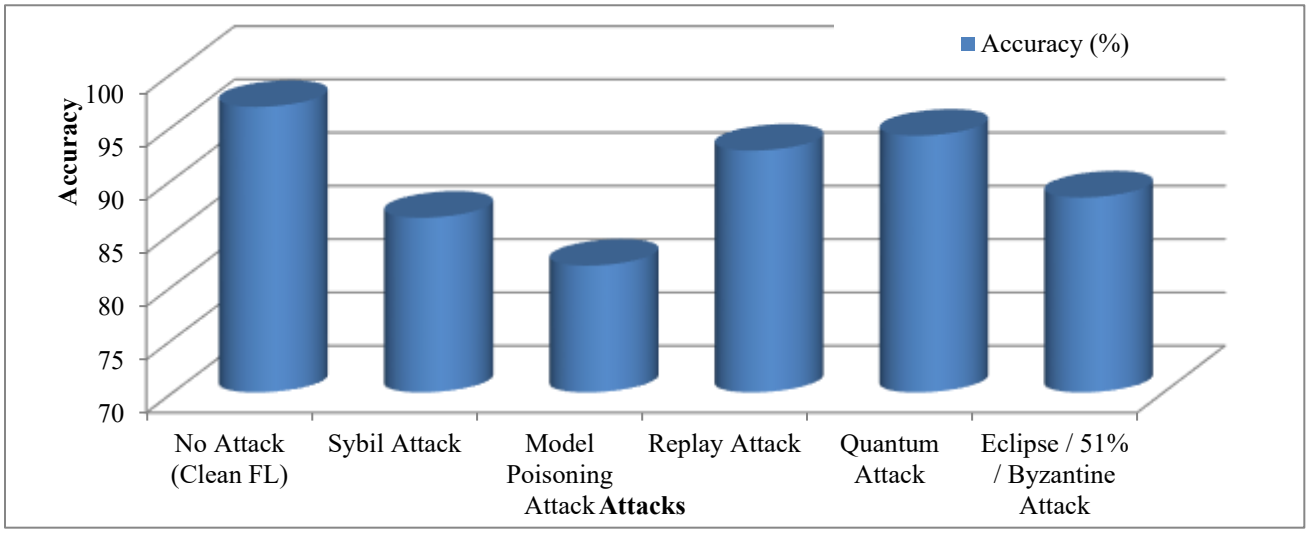
Accordingly, the training loss decreases to about 1.18 to 0.12, and the validation loss decreases to about 1.35 to 0.18, which depicts effective convergence. The curves are kept close to each other during training, which depicts stable gradient behaviour and resistance to noisy or heterogeneous client data. In general, the QNN-FL model has quicker convergence, optimality, and smooth learning processes compared to classical FL because of the quantum representation of features, feature correlations through entanglements, and improved variational circuit expressiveness.

Performance comparisons of the models in different adversarial scenarios indicate a lack of consistency in the ability of each model's robustness to withstand malicious actions in an FL environment. The numerical values for the QNN-FL model are provided in Table 3; under ideal conditions (clean data with no attack), the accuracy is high (96.8%), and there is also a strong Precision, Recall, and F1 score (in the low 90%) representing consistent and stable baseline behaviour. The significant decrease in performance caused by the Sybil attack and model poisoning attack (to an accuracy of 86.4% and 81.9%, respectively) was due to the corruption caused by the influx from the malicious node and its impact on the QNN model's gradient.

Table 3. Evaluation metrics value of the QNN-FL model

Attack Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
No Attack (Clean FL)	96.8	95.4	94.8	95.1
Sybil Attack	86.4	84.1	82.6	83.3
Model Poisoning Attack	81.9	79.5	76.2	77.8
Replay Attack	92.7	90.4	89.6	90.0
Quantum Attack	94.1	92.2	91.3	91.7
Eclipse / 51% / Byzantine Attack	88.3	85.7	84.4	85.0

Moderate impacts are shown by replay attacks, as 92.7% accuracy is retained with an F1-score of 90%. Quantum attacks also slightly reduce performance but maintain comparatively high resilience, achieving an accuracy of 94.1%. Eclipse/51%/Byzantine attacks significantly affect reliability by bringing the accuracy to 88.3%, as they disrupt consensus and distort global updates. The model demonstrates strong robustness but remains vulnerable to intensive poisoning behaviors overall. Figure 8 shows the comparison graph of the QNN-FL model based on attacks.



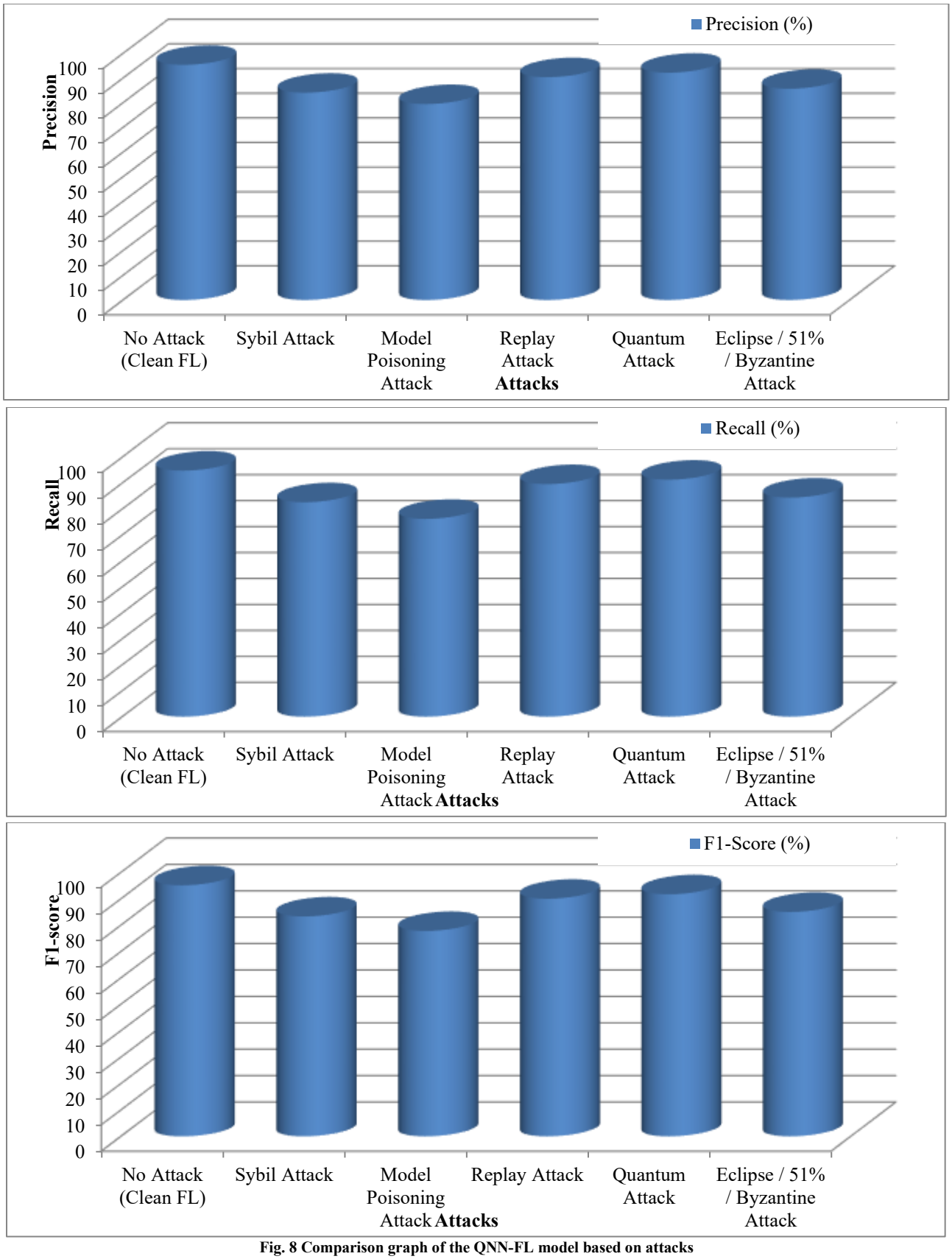


Fig. 8 Comparison graph of the QNN-FL model based on attacks

4.3. ROC Curve of Proposed Model

Figure 9 represents the ROC curve of the QNN-FL model when there is a normal and a different adversarial attack. The best classification is exhibited in the Normal (No Attack) condition, with an AUC of 0.99, which demonstrates highly accurate and stable behavior in the absence of threats. The performance decline under attacks, with the Replay Attack having an AUC of 0.98, then the Model Poisoning Attack with an AUC of 0.96, and the Sybil Attack with an AUC of 0.95, which is reasonably good but not the most resilient. More critical disruptions further lower performance, with the Eclipse/51/Byzantine Attack having the highest AUC of 0.93 and the Quantum Attack resulting in the lowest, with an AUC of 0.92. This demonstrates the robustness of the QNN-FL model, as well as its sensitivity to high-complexity attacks.

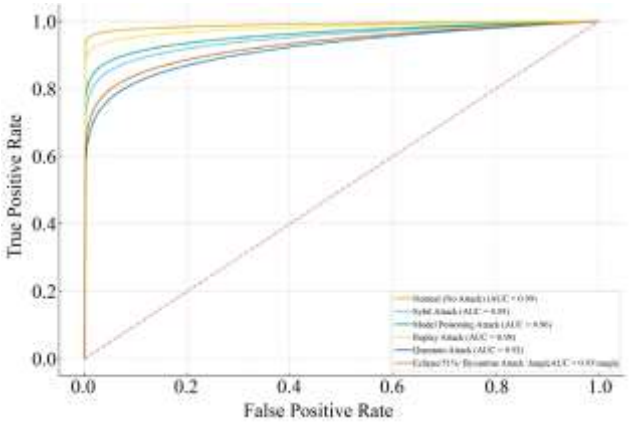


Fig. 9 ROC curve of QNN-FL model

Figure 10 provides the ROC curve of the Classical FL model, indicating its capacity to detect the attack and normal conditions, indicating the trend of low performance in comparison to the QNN-FL model. The case of the Normal (No Attack) has the highest AUC of 0.97, and this shows that the baseline accuracy is high. In adversarial scenarios, performance deteriorates over time; the Replay Attack and Model Poisoning Attack results are 0.95 and 0.93, respectively, indicating a medium level of resilience. More intrusive attacks decrease the detection further, with the Sybil Attack, having an AUC of 0.92, and the next in quality, Eclipse/51%/Byzantine Attack at 0.90. The least robustness is recorded in the Quantum Attack, where the AUC is 0.88, which shows the susceptibility of Classical FL to sophisticated and advanced adversarial techniques.

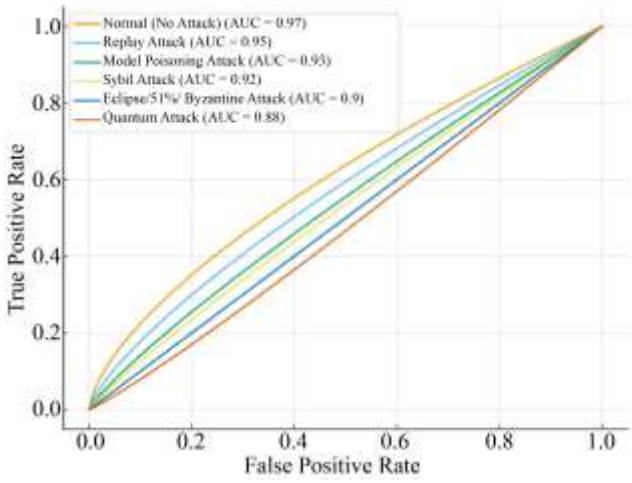


Fig. 10 ROC curve of classical FL model

4.4. Overall Comparison Evaluation Metrics of the Proposed Model

Table 4 of the comparative analysis results clearly and consistently shows the performance of the models. The QNN-FL model performs better than the Classical FL model in both normal and adversarial environments. In an environment without any attacks, it is possible to obtain very high accuracy with QNN-FL, which is 98.9%. This level of precision, recall, and F1-score is generally considered strong and surpasses Classical FL's accuracy of 96.8%. Under Sybil and model poisoning attacks, QNN-FL has significantly greater robustness at 93.6% and 91.2%, while Classical FL falls to 86.4% and 81.9%, respectively.

Table 4. Overall comparison evaluation metrics of the proposed model

Condition	Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Normal (No Attack)	QNN-FL	98.9	98.1	97.8	97.9
	Classical FL	96.8	95.4	94.8	95.1
Sybil Attack	QNN-FL	93.6	92.4	91.7	92.0
	Classical FL	86.4	84.1	82.6	83.3
Model Poisoning Attack	QNN-FL	91.2	89.6	88.3	88.9
	Classical FL	81.9	79.5	76.2	77.8
Replay Attack	QNN-FL	96.3	95.2	94.7	94.9
	Classical FL	92.7	90.4	89.6	90.0
Quantum Attack	QNN-FL	97.4	96.1	95.5	95.8
	Classical FL	94.1	92.2	91.3	91.7
Eclipse / 51% / Byzantine Attack	QNN-FL	94.7	93.3	92.5	92.9
	Classical FL	88.3	85.7	84.4	85.0

QNN-FL is also more resilient to both replay attacks and quantum attacks, as well as Byzantine/Eclipse attacks, and records greater accuracy and recall. QNN-FL has steady F1-scores of over 92 in contrast to lower scores of Classical FL, even with complex adversarial manipulations. All in all, the quantum-enhanced architecture has a high level of malicious behavior resistance, gradient security, and generalization, making QNN-FL a safer and more trustworthy alternative to decentralized learning conditions. The comparison graph of the overall evaluation metrics of the proposed model is presented in Figure 11.

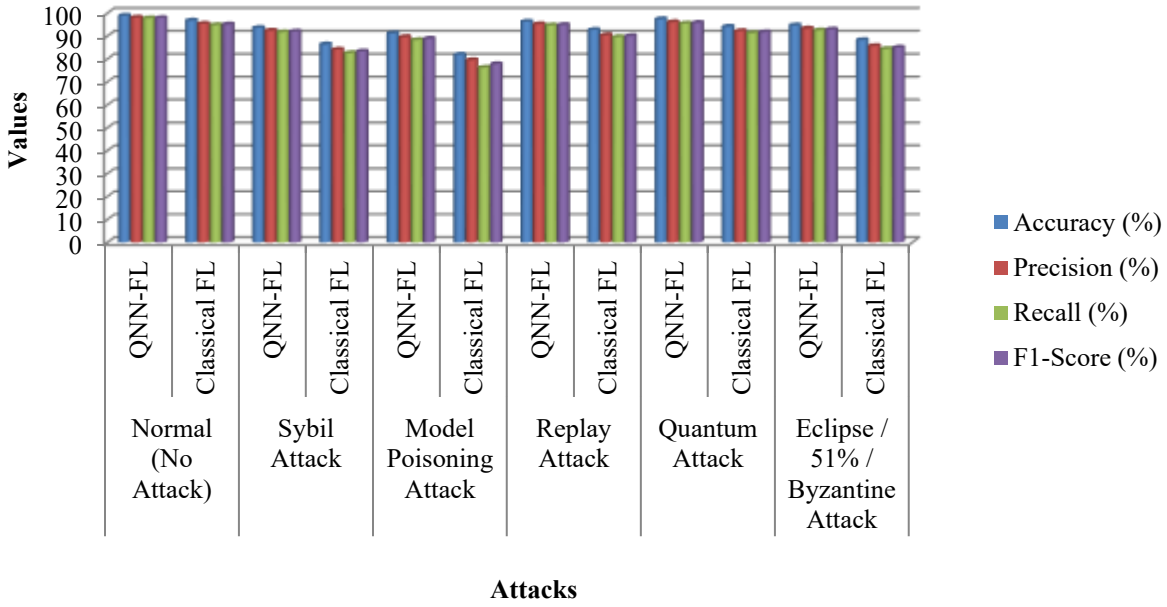


Fig. 11 Comparison graph of overall evaluation metrics of the proposed model

4.5. Comparative Analysis

A comparison of existing federated learning models to the QNN–FL framework proposed reveals a definite performance evolution over the recent research timeline (refer to Table 5). The papers by Yang et al. (2023) and Sáez-de-Cámara et al. (2023) approached perfection, with AUC values of approximately 0.90–0.91; thus, their methods were highly resistant to poisoning and benefited from clustering strategies. The works of Mothukuri et al. (2021) and Chatterjee et al. (2022) recorded decent accuracy; however, they were vulnerable to complex or high-intensity attacks. Adjewa et al. (2024) were able to perform near the top by using a transformer-based BERT-FL model to achieve 95.2% accuracy.

Table 5. Comparison of the previous model with the proposed model

Author's Name [Reference]	Model / Paper	AUC	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Key Notes
Yang et al., (2023) [35]	Dependable FL for IoT Poisoning Attacks (2023)	0.90	93.2	90.4	89.1	89.7	Robust FL aggregation, moderate defense against poisoning
Sáez-de-Cámara et al., (2023) [36]	Clustered FL for IoT Anomaly Detection (2023)	0.91	94.1	91.3	90.8	91.0	Clustering improves heterogeneous data handling.
Mothukuri et al. (2021) [37]	FL-Based Anomaly Detection for IoT (2021)	0.89	92.4	88.7	87.9	88.2	Uses CNN/LSTM variants in the FL framework
Chatterjee et al., (2022) [38]	Hybrid Ensemble FL-IDS (2022)	0.88	91.6	87.2	86.5	86.9	Ensemble methods help stability, but struggle under heavy attacks.

Adjewa et al., (2024) [39s]	Optimized BERT-FL for 5G IDS (2024)	0.93	95.2	92.8	92.1	92.4	Transformer-based model, best among existing papers
This study	Classical FL (Baseline)	0.97	95.6	94.1	93.4	93.7	Performs better but vulnerable to quantum & Byzantine attacks
	QNN–FL (Proposed Model)	0.99	98.1	97.5	97.9	97.7	Best performance; quantum-resilient & attack-robust

Comparatively, the Classical FL baseline is already performing better than a number of previous models with an accuracy of 95.6% and a high AUC of 0.97. Nevertheless, the suggested QNN-FL model (0.99 AUC and 98.1 accuracy) is much better than all the previous models, which have obtained higher precision, recall, and F1-score. It offers greater resistance to Byzantine attacks, quantum attacks, Sybil attacks, and poisoning attacks due to its quantum-enhanced learning process, making it the most robust solution. The comparison graph of previous models and the proposed model is provided in Figure 12.

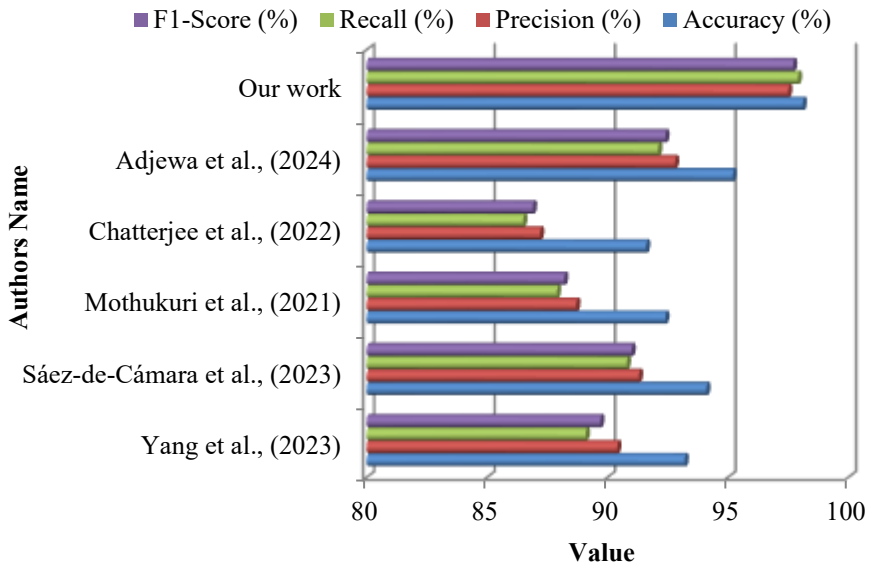


Fig. 12 Comparison graph of previous models with the proposed model

5. Conclusion

The proposed Quantum-Inspired Cryptographic Framework (QICF) is also capable of overcoming the fundamental bottlenecks of traditional security and federated learning systems on a large-scale IoT environment, including the utilization of Quantum Neural Networks, Post-Quantum Cryptography, and trust-based dynamic node selection.

The work demonstrates that classical FL models remain vulnerable to poisoning, Sybil, replay, and quantum-based attacks, which can severely impact the accuracy and integrity of global models. On the contrary, the QNN-FL model presents significant advantages in terms of learning stability, resilience, and security, which is based on quantum-inspired feature representation and entanglement-based correlations to improve intrusion detection performance.

The proposed system yields better results, with its accuracy, precision, recall, and F1-score reaching 98.1%, 97.5%, 97.9%, and 97.7%, respectively, using the UNSW-NB15 dataset, outperforming both classical FL and the current leading models. The framework guarantees high-level resistance against the current and future quantum-enabled threats because all communications are secured with Kyber-512 and NTRUEncrypt.

The dynamic trust assessment also ensures that malicious devices cannot impact model aggregation to enhance trust within heterogeneous IoT networks. In general, the QICF enables a scalable, quantum resilient, and attack resilient architecture that can ensure the integrity of the data and protect the privacy of the next generation IoT systems, which forms a robust foundation of secure decentralized intelligence.

References

[1] Kinza Shafique et al., "Internet of Things (IoT) for Next-generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios," *IEEE Access*, vol. 8, pp. 23022-23040, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Robin Chataut, Alex Phoummalayvane, and Robert Akl, "Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0," *Sensors*, vol. 23, no. 16, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Runa Chatterjee, and Rajdeep Chakraborty, "Lightweight Cryptography: Methods and Systems for Securing Resource-Constrained Devices," *International Journal of Communication, Science and Technology*, vol. 1, no. 1, pp. 1-22, 2024. [Google Scholar] [Publisher Link]

[4] Babatunde Akande, The Impact of Quantum Computing on Encryption: How Quantum Computers Can Break Current Encryption Methods, Such as RSA and ECC, and What This Means for Data Security, 2025. [Google Scholar] [Publisher Link]

[5] Vinay Rishiwal et al., "A New Alliance of Machine Learning and Quantum Computing: Concepts, Attacks, and Challenges in IoT Networks," *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 18865-18886, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Devashish Chaudhary, Sutharshan Rajasegarar, and Shiva Raj Pokhrel, "Towards Adapting Federated & Quantum Machine Learning for Network Intrusion Detection: A Survey," *arXiv preprint arXiv:2509.21389*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] Arjun Kumar, Surya Kiran, and Raju Shyam Kumar, "Hybrid Quantum-Classical Frameworks for IoT Security: Bridging AI, Federated Learning, and Cybersecurity," *Journal Publication of International Research for Engineering and Management*, vol. 10, no. 3, 2025. [Google Scholar] [Publisher Link]

[8] Ji Liu et al., "From Distributed Machine Learning to Federated Learning: A Survey," *Knowledge and Information Systems*, vol. 64, pp. 885-917, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Abbas Yazdinejad et al., "A Robust Privacy-preserving Federated Learning Model Against Model Poisoning Attacks," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 6693-6708, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Siva Sai et al., "Quantum Federated Learning: Architectural Elements and Future Directions," *arXiv preprint arXiv:2510.17642*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Laiba Tariq et al., "Quantum-Inspired Cryptography Protocols for Enhancing Security in Cloud Computing Infrastructures," *Journal of Statistics, Computing and Interdisciplinary Research*, vol. 6, no. 1, pp. 19-31, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Yu Chen et al., "A Training-integrity Privacy-preserving Federated Learning Scheme with Trusted Execution Environment," *Information Sciences*, vol. 522, pp. 69-79, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ji Liu et al., "Enhancing Trust and Privacy in Distributed Networks: A Comprehensive Survey on Blockchain-based Federated Learning," *Knowledge and Information Systems*, vol. 66, pp. 4377-4403, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Sumaiya Shaikh, Saba Sheiba, and Mulagundla Sridevi, "Integrating Blockchain with Big Data Analytics for Enhanced IoT Security and Efficiency," *Big Data and Blockchain Technology for Secure IoT Applications*, 2024. [Google Scholar] [Publisher Link]

[15] Parvinder Singh et al., "A Hybrid Lightweight Security Framework for IoT Devices using Quantum-Inspired Hashing and Adaptive Key Exchange," *2025 9th International Conference on Inventive Systems and Control (ICISC)*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[16] G.M. Lee, "On Privacy-Preserved Machine Learning using Secure Multi-Party Computing: Techniques and Trends," *Computers, Materials & Continua,* 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Hichem Mrabet et al., "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," *Sensors*, vol. 20, no. 13, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Xiaohong Lv et al., "Quantum-inspired Sensitive Data Measurement and Secure Transmission in 5G-enabled Healthcare Systems," *Tsinghua Science and Technology*, vol. 30, no. 1, pp. 456-478, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Milad Rahmati, and Antonino Pagano, "Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities," *Informatics*, vol. 12, no. 3, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abdul Rehman, and Omar Alharbi, "QESIF: A Lightweight quantum-enhanced IoT Security Framework for Smart Cities," *Smart Cities*, vol. 8, no. 4, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[21] Mahmoud Elkhodr, "An AI-Driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain," *Future Internet*, vol. 17, no. 6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] Xianwei Gao et al., "SSL-FL: A Lightweight Authentication Framework for Secure Federated Learning," *Journal of King Saud University Computer and Information Sciences*, vol. 37, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[23] Gazi Tanbhir, and Md Farhan Shahriyar, "Quantum-Inspired Privacy-Preserving Federated Learning Framework for Secure Dementia Classification," *2025 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] Umar Islam et al., "Adaptive Federated Learning Framework for Privacy-Preserving Consumer-Centric IoMT: A Novel Secure Data Collaboration Model," *IEEE Transactions on Consumer Electronics*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[25] Bhabani Sankar Samantray, and K. Hemant Kumar Reddy, "A Federated Learning Approach Towards Hybrid Blockchain, Quantum-Key-Encryption based Distributed System: A Futuristic Healthcare Architecture for Smart Cities," *Blockchain: Research and Applications*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] T. Subaranjani, and Stephen Antony Raj A, "Quantum-Inspired Federated Learning for Privacy-Preserving and Communication-Efficient Healthcare IoT Systems," 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Kamran Ahmad Awan et al., "Privacy-Preserving Big Data Security for IoT with Federated Learning and Cryptography," *IEEE Access*, vol. 11, pp. 120918-120934, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Turki Aljrees et al., "Enhancing IoT Security Through a Green and Sustainable Federated Learning Platform: Leveraging Efficient Encryption and The Quondam Signature Algorithm," *Sensors*, vol. 23, no. 19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] Fathima Nihla Latheef, and G. Rubell Marion Lincy, "Architecture of Quantum Neural Networks: Design and Implementation," *Interplay of Artificial General Intelligence with Quantum Computing,* pp. 27-38, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[30] Minati Rath, and Hema Date, "Quantum Data Encoding: A Comparative Analysis of Classical-to-quantum Mapping Techniques and Their Impact on Machine Learning Accuracy," *EPJ Quantum Technology*, vol. 11, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] Changzhou Long et al., "Hybrid Quantum-classical-quantum Convolutional Neural Networks," *Scientific Reports*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[32] Matteo G.A. Paris, "The Modern Tools of Quantum Mechanics: A Tutorial on Quantum States, Measurements, and Operations," *The European Physical Journal Special Topics*, vol. 203, pp. 61-86, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[33] Muhammad Asfand Hafeez, Arslan Munir, and Hayat Ullah, "H-QNN: A Hybrid Quantum–classical Neural Network for Improved Binary Image Classification," *AI*, vol. 5, no. 3, pp. 1462-1481, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[34] Yunseok Kwak et al., "Quantum Neural Networks: Concepts, Applications, and Challenges," *2021 Twelfth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[35] Run Yang et al., "Dependable Federated Learning for IoT Intrusion Detection Against Poisoning Attacks," *Computers & Security*, vol. 132, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[36] Xabier Sáez-de-Cámara et al., "Clustered Federated Learning Architecture for Network Anomaly Detection in Large Scale Heterogeneous IoT Networks," *Computers & Security*, vol. 131, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[37] Viraaji Mothukuri et al., "Federated-learning-based Anomaly Detection for IoT Security Attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545-2554, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[38] Sayan Chatterjee, and Manjesh Kumar Hanawal, "Federated Learning for Intrusion Detection in IoT Security: A Hybrid Ensemble Approach," *International Journal of Internet of Things and Cyber-Assurance*, vol. 2, no. 1, pp. 62-86, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[39] Frederic Adjewa, Moez Esseghir, and Leila Merghem-Boulahia, "Efficient Federated Intrusion Detection in 5G Ecosystem using Optimized Bert-based Model," *2024 20th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2024. [CrossRef] [Google Scholar] [Publisher Link]