Chapter 19

# Quantum federated learning: architectural elements and future directions

**Siva Sai, Abhishek Sawaika, Prabhjot Singh, and Rajkumar Buyya**
*Quantum Cloud Computing and Distributed Systems (qCLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Melbourne, VIC, Australia*

## 19.1 Introduction

Federated Learning [1] trains machine learning models across several data silos without the need to move the raw data to a central server. In a typical FL iteration, the institutional nodes or clients download a shared global model, train the model using their private datasets, and share only the updates to a coordinating server. The server aggregates the updates from the clients and broadcasts them back for the next round. The federated learning setup allows learning from data that would be impossible due to privacy regulations, ownership constraints and bandwidth. It also lowers privacy risks and avoids the single point of failure problem. Despite the several benefits, FL meets a set of scientific and practical requirements at scale, which expose limitations in classical frameworks and consequently open a path towards quantum enhancements. A few of the relevant challenges in the FL setups are as follows:

1. High compute requirement: Classical FL faces several practical constraints in low-resource clients scenario, including high computational and memory demands of local model training, and the consequent latency and energy burdens.
2. Privacy and security issues: The core reason behind the privacy preservation in FL settings is that the clients only share the gradients without sharing the raw data. But that doesn't eliminate leakage completely. Membership inference, model inversion and poisoning by the adversaries still limit the privacy, thus raising the need for stronger protocols to resist adversaries and bound leakage.
3. High-dimensional and multi-modal data: Several application domains of FL, including healthcare, manufacturing and finance, produce data with several features and modalities like text, image, and temporal data. Hence, there is a clear need for models with the capability of powerful representation learning.
4. Communication efficiency: In the FL setting, frequent exchange of large model updates creates heavy downlink and uplink traffic. Although the techniques like sparsification and compression help, the tradeoff between bandwidth and accuracy remains a strong factor.
5. Heterogeneity and statistical robustness: Real-world data in an FL setting is almost always non-IID. The client's data may have different label distributions, sample sizes, and feature spaces. This heterogeneity leads to issues like instability during aggregation, model bias, and slow convergence.

The integration of Quantum Computing (QC) into FL addresses several of these concerns effectively.

### 19.1.1 Motivation for Quantum Federated Learning (QFL)

The integration of quantum computing and federated learning is based on the fact that each of these technologies supports the other. The integration of quantum computing into federated learning environments offers notable benefits, but that is not to minimize the use of the federated learning paradigm in quantum computing setups.

QC provides exceptional computational capabilities, superseding the classical systems. QC enables unique algorithms capable of solving complex problems which are intractable to solve with classical systems. Non-convex loss surfaces are typical in deep learning, which leads classical FL systems to struggle with complex optimization problems, especially when dealing with large-scale data. Quantum optimization algorithms enabled by QC explore large solution spaces very efficiently by leveraging quantum parallelism. A few notable optimization algorithms include Quantum Approximate Optimization (QAOA) and Variational Quantum Eigensolver (VQE). These quantum algorithms lead to improved accuracy and convergence as they can potentially find better minima in high-dimensional loss spaces. Classical FL fails to handle

**Federated Learning.** https://doi.org/10.1016/B978-0-44-344433-3.00024-1

quantum data or systems based on quantum mechanics, like quantum sensor networks and quantum chemistry. QC is a natural option to train QML models in these cases to represent and manipulate quantum states. Thus, by its integration into FL systems, QC enlarges the application space of FL into quantum-domain tasks. QC also assists FL in achieving reduced communication bottlenecks through quantum compression and encoding. A main limitation of classical FL is communication overhead due to recurrent transmission of large model updates. QC-enabled techniques like entanglement-assisted compression and quantum teleportation can significantly reduce the quantum information that needs to be shared across nodes [2].

Quantum Machine Learning (QML) models like Quantum Neural Networks (QNNs) and Variational Quantum Circuits (VQCs) can define highly non-linear entangled representations and feature maps with relatively few parameters. This would be very helpful for the clients with a limited computation budget in the QFL setting. Quantum generative models are very efficient in representing complex distributions. In the FL setting, the quantum generative models could be exploited for calibration or data augmentation of skewed local datasets while keeping raw data private. QC can help FL frameworks strengthen their privacy by incorporating quantum protocols like blind quantum computing, which enables computation on quantum-encrypted data.

FL becomes particularly important in privacy-sensitive quantum domains such as wireless networks and IoT. It also enables collaborative and scalable learning across distributed devices. Centralized quantum machine learning faces scalability challenges due to the need for transmission of large volumes of intermediate states and quantum data to a central processor. Current quantum communication infrastructure makes it almost impossible [3]. By incorporating FL, only the quantum model updates would be shared among the participants, thus making building intelligent quantum systems efficient. QFL would power a broad range of real-world quantum-driven applications while simultaneously improving data privacy.

### 19.1.2 Chapter organization

The rest of the chapter is organized as follows. Having covered the motivation of integration of quantum computing and federated learning in the introduction, the next section talks about the general QFL architecture. After that, we present a taxonomy of QFL systems—classified based on four important criteria. Then, we analyze the applications of QFL in a few highly relevant domains. After that, we explore current challenges and future directions in QFL. Finally, we conclude the chapter with key insights.

## 19.2 Background

### 19.2.1 Power of quantum computing

The fundamental unit of classical information is the bit, which can exist in only two states: 0 or 1. Conversely, the qubit, the basic unit of quantum information, can exist in a superposition of orthogonal states $|0\rangle$ and $|1\rangle$. A superposition is a state in between $|0\rangle$ and $|1\rangle$, represented as $\alpha|0\rangle + \beta|1\rangle$, where $\alpha$ and $\beta$ are complex numbers and are called amplitudes, making this different from a probabilistic state as it has real numbers as amplitudes. One other property of a qubit is that upon measurement, it collapses to one of its orthogonal states. The probability that the state collapses to either orthogonal state is determined by the norm square of the amplitude of the respective state. In a quantum circuit, the Hadamard gate facilitates the introduction of superposition. Superposition enables us to perform operations on multiple states simultaneously; on the other hand, when we measure, the state collapses and we get a single value. This makes it very hard to create quantum algorithms, so interference effects are used to ensure the correct answer is reached. Another crucial aspect introduced by qubits is entanglement, a phenomenon where two systems, despite their physical separation, exhibit correlated behaviors that defy classical randomness. In a quantum circuit, the CNOT gate enables the introduction of superposition.

The power of superposition and entanglement allows the development of algorithms that deliver exponential speedups in specific scenarios. One notable example of this is the Deutsch-Jozsa Algorithm. The primary objective of this algorithm is to ascertain whether a function exhibits constant behavior or exhibits balance. Consider a hypothetical black box (or an Oracle) that accepts input as a n-bit string and outputs either 0 or 1. Classically, it would require at most $N/2 + 1$ queries to determine if the function is constant or balanced, where $N = 2^n$. However, one can achieve this determination in a single query using the power of quantum computing. Initially, an equal superposition of all possible $N$ states is constructed by applying Hadamard gates to each of n qubits. Subsequently, this information is passed through a phase oracle (an oracle analogous to the classical oracle, ensuring its reversibility, as quantum gates must be reversible). Finally, Hadamard gates

are applied to each qubit once more, resulting in the final state. Eq. (19.1) illustrates the process:

$$\sum_{z\in\{0,1\}^n}\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot z}\right)|z\rangle \tag{19.1}$$

Upon performing measurement, the probability of obtaining all zeros is $\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right)^2$. If the function is constant, $(-1)^{f(x)}$ remains constant, resulting in a probability of 1. Conversely, if the function exhibits balance, $(-1)^{f(x)}$ alternates between $+1$ and $-1$, yielding a probability of 0. Therefore, by measuring the n qubits, one can determine whether the function is constant or balanced. If all zeros are obtained, the function is constant; otherwise, it is balanced. Apart from the Deutsch-Jozsa algorithm, other algorithms such as Bernstein-Vazirani, Simon, and Grover algorithms provide significant speedup compared to their classical counterparts, demonstrating the immense power of quantum computing.

### 19.2.2 Common tools used in quantum computing

- **Qiskit**—IBM's open-source SDK for building, simulating, and running quantum circuits on real IBM Quantum hardware.
- **PennyLane**—A Python library for differentiable quantum programming and hybrid quantum-classical machine learning.
- **Cirq**—Google's framework for designing, simulating, and executing quantum circuits on Google Quantum processors.
- **Braket SDK**—Amazon's Python interface to build, test, and run quantum algorithms on cloud-hosted hardware backends.
- **QuTiP**—Quantum Toolbox in Python for simulating open quantum systems and dynamics using density matrices.
- **t|ket⟩**—Cambridge Quantum's compiler optimizing quantum circuits for different hardware architectures.
- **Ocean SDK**—D-Wave's developer suite for formulating and solving problems on quantum annealers.
- **Q# / QDK**—Microsoft's domain-specific language and development kit for quantum algorithm design and simulation.
- **Strawberry Fields**—Xanadu's platform focused on photonic quantum computing and continuous-variable circuits.
- **ProjectQ**—A Python framework for high-performance quantum simulation and flexible backend compilation.

### 19.2.3 Quantum hardware

Quantum hardware is diverse, with each architecture offering unique advantages. Superconducting transmons, used by IBM and Google, provide fast gates and well-developed tools, though they have shorter coherence times [4]. Trapped ions, from IonQ and Quantinuum, are known for their excellent coherence and comprehensive connectivity, albeit with slower gate speeds [5]. Neutral-atom Rydberg systems, developed by QuEra and Atom, allow for rapid qubit scaling with adaptable layouts, but they are still refining their error rates [6]. Photonic platforms, like those from Xanadu, are notable for their room-temperature operation and integration with optics, though achieving universal high-fidelity gates is still a work in progress [7]. Spin qubits in silicon or diamond offer the potential for CMOS-style scalability but are still in the early stages for large-scale algorithms [8]. Lastly, topological approaches focus on intrinsic error protection, with practical devices still being developed [9].

## 19.3 Architecture

In this section, we present the working concept of QFL, which is illustrated in Fig. 19.1. The QFL paradigm enables collaborative training of a shared model by multiple quantum-enabled devices. This decentralized training approach enhances data privacy and leverages the computational advantages of quantum-enabled devices. In vanilla QFL, a central server coordinates the overall QFL process. The coordination includes management of aggregation, communication, and synchronization between quantum devices. The QFL (centralized QFL in particular) follows a multi-step and cyclical process with the following key stages:

1. Data Encoding: Each client encodes its private classical data into quantum states. A quantum state encoder is used to map classical features into quantum Hilbert space representations. State preparation is the starting step in the encoding process, where each qubit is initialized in its ground state. There are several encoding techniques that can be employed depending on the desired learning tasks and the nature of the data. Amplitude encoding, basis encoding, and angle encoding are popular choices. The data encoding steps make sure that the data is transformed into a form that is compatible with parametrized quantum circuits.

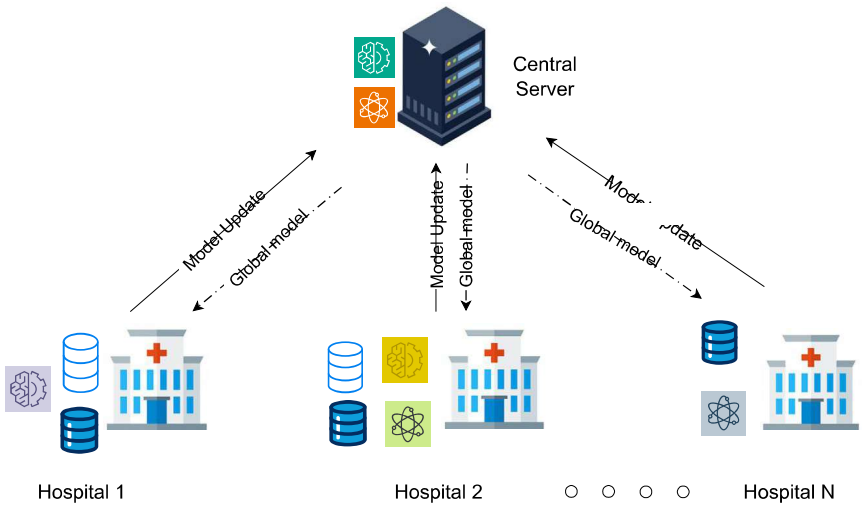


**FIGURE 19.1** Centralized QFL architecture.

2. Local Training: After the data is encoded, it is passed through a parametrized quantum circuit at each client. Generally, this circuit is finalized by the server and passed down to all the clients. A Parametrized Quantum Circuit (PQC) consists of a set of quantum gates, the behavior of which is controlled by trainable parameters. The quantum gates explore complex quantum correlations in the data by manipulating and entangling the qubits. Post the application of PQC, the qubits are measured, and the expectation values or measurement probabilities (resulting classical outputs) are used to compute loss functions. The client updates its local parameters using gradient-based optimization techniques like Stochastic Gradient Descent (SGD). Quantum version of SGD called Quantum Natural Gradient Descent (QGND) can also be used based on the type of circuit at the client.
3. Aggregation and model sharing: After the local training, each client shares its updated PQC parameters or gradients to the central server. The server generates an updated global model by applying techniques like FedAvg. The server tries to ensure that the aggregation is privacy-preserving and safe. After the aggregation, the server sends back the model to every client, which is then used by the clients to update their local models. Thus, an iteration of QFL training is completed, and the same process is continued for several rounds until the models achieve an acceptable performance or converge.

The QFL training process looks similar to that of classical FL; however, QFL has multiple special features, including quantum-specific noise management, circuit depth restrictions, and quantum encoding. All these features make QFL an appropriate choice for privacy-sensitive use cases in quantum-enabled environments. Schuld et al. [10] classify the intersection of machine learning and quantum computing into four categories—quantum for classical (processing classical data on quantum computers), quantum for quantum (processing quantum data on quantum computers), classical for quantum (processing quantum data on classical computers), and classical for classical (processing classical data on classical computers, but with quantum-inspired algorithms). While the QFL paradigm applies to all the categories, it is more relevant to quantum for classical and quantum for quantum. QFL includes the possibility of a hybrid nature of clients and servers (with the capabilities to run either or both of the classical and quantum neural network models), thus aligning with the current real-world scenarios where complete training on quantum devices only is infeasible.

### 19.3.1 An approach for realization of QFL

To establish a quantum federated learning (QFL) system, one must first implement a hybrid federated-learning pipeline. In this configuration, each client trains a local variational quantum model or a hybrid quantum-classical model and transmits model updates to a central aggregator, such as Federated Averaging (FedAvg) or Federated Proximal (FedProx), while complying with privacy and communication constraints. Tools like PennyLane offer differentiable programming with seamless integration into PyTorch, TensorFlow, and JAX, supporting gradient methods such as parameter-shift and adjoint differentiation. Qiskit provides robust transpilation, advanced noise modeling, and direct access to IBM Quantum hardware

through Aer and Runtime. The pure or hybrid QML models required in QFL can be built using tools like Pennylane and Qiskit. PennyLane can also connect to various providers via plugins, including AWS Braket, IonQ, and IBM.

A staged simulation strategy should be implemented: one should begin with small-qubit analytic or statevector simulations, progress to shot-based noisy simulations (such as Qiskit Aer noise models from "Fake" backends like FakeManila), and finally conduct targeted hardware runs. In practice, large circuits with more than approximately 100 qubits are typically impractical for end-to-end QFL due to circuit depth, device noise, and queuing constraints. For orchestration, frameworks like Flower, along with FedML or TensorFlow Federated, enable the creation of custom clients that call quantum backends and return gradients or expectation values. Throughout the process, it is crucial to plan for device heterogeneity, error-mitigation techniques, secure aggregation, and bandwidth limitations.

## 19.4 Taxonomy

As shown in Fig. 19.2, we classify the existing QFL systems based on four aspects—quantum architecture [11], data processing method, network topology, and involved security mechanism.

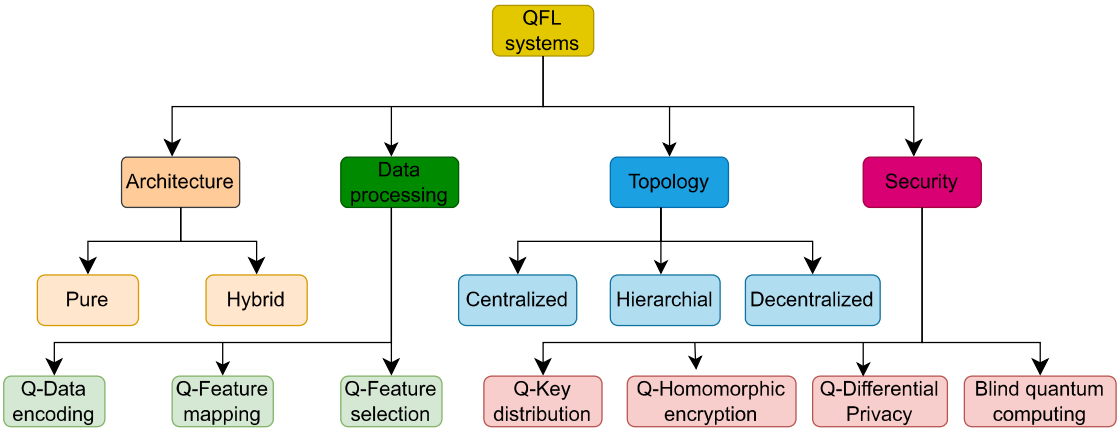


**FIGURE 19.2** Classification framework for QFL systems based on architecture, data processing, topology, and security mechanism dimensions.

### 19.4.1 Quantum architecture

Based on the type of machine learning model used in the federated setup, we divide the QFL models into two categories—those that incorporate pure quantum machine learning models (Pure QFL) and those that incorporate hybrid quantum models (Hybrid QFL), i.e., combining classical neural network layers with quantum layers.

Pure QFL enables training of a global quantum model, maintaining the data privacy of sensitive local classical or quantum data. A common configuration in Pure QFL setup is training of PQCs with the VQE optimization technique [12]. PQCs, with modifiable classical parameters, enable quantum devices to learn and incorporate intricate patterns in complex systems. When the clients securely upload measurement results or quantum model updates, the server uses a suitable quantum aggregation technique to create a global quantum model, which is later sent to the clients. Pure QFL models make use of quantum techniques like superposition, inference, and quantum entanglement to learn from data more efficiently. As quantum features limit inferences of device data, pure QFL models tend to be more secure against unauthorized data breaches, FL system faults, and adversarial attacks. Recent research developed Pure QFL models for multiple application areas. Park et al. [13] introduced entangable slimmable quantum neural networks (esQNNs) to adapt QFL to work well under changing channel conditions in IoT environments. Based on esQNNs, the authors propose an entangable slimmable QFL (esQFL) framework wherein the superposition-coded parameters of esQNNs are shared. Huong et al. [12] proposed a communication-efficient Variational Quantum Algorithm (VQA) and showcased the superiority of the proposed model on near-term processors. Abou et al. [14] proposed a QFL-enabled intrusion detection system to detect network intrusions in consumer electronics networks.

Hybrid QFL models combine quantum layers with classical neural network layers. Generally, these models consist of initial convolutional or fully connected layers to lower the computational overhead by effectively handling large-dimensional data. These initial layers take care of data processing and feature extraction. After that, the extracted features

are encoded into quantum states and passed on to PQCs. The quantum circuits of further quantum layers are parametrized by classical parameters, which are trainable. Classical optimization algorithms are used to enable quantum circuits to learn optimal parameters in an iterative fashion. After the training of the hybrid QML models at the clients, they are passed on to the server for aggregation. Ren et al. [15] proposed a hybrid QFL system for smart cyber-physical dynamic security assessment. Hisamori et al. [16] proposed a hybrid QFL framework, which consists of a two-qubit quantum circuit embedded with a convolutional neural network that further uses variational quantum circuits.

### 19.4.2 Data processing method

When classical data is fed for training in QFL systems, it needs to be transformed in such a way that QML models can process it. Based on the data processing methods, we classify the QFL systems into three categories: quantum data encoding-based, quantum feature mapping-based, and quantum feature selection and dimensionality reduction-based [17].

QFL systems employing quantum data encoding and processing methods investigate different encoding schemes with the aim of efficiently transforming the classical data into quantum states. The broader goal of these systems is the minimization of the resources required for processing and encoding the varied data (discrete, continuous, and categorical) in quantum states. Recent research developed multiple QFL systems employing quantum encoding methods. Yang et al. [18] proposed a vertical quantum federated learning architecture based on a quantum-BERT model for text classifications. The authors made use of variational quantum circuits for quantum encoding of the textual data. In another study, Yang et al. [19] proposed a privacy-preserving decentralized feature extraction method for speech recognition. The authors upstreamed the input speech to a quantum computing server for extracting Mel-spectrogram features in a decentralized setup. They used VQC to encode the convolutional features. Huang et al. [12] also utilize a quantum encoding method to create quantum data.

The QFL systems based on the quantum feature mapping technique exploit quantum properties to create nonlinear and high-dimensional representations of classical data. Quantum versions of the classical feature transformation methods, like kernel methods, are developed by QFL systems in this category. Apart from developing resource-efficient quantum mapping methods, the systems also aim at building optimal quantum feature maps that balance the robustness with the expressiveness of quantum feature mapping. Yun et al. [20] developed a quantum split neural network framework which also employs cross-channel pooling to efficiently leverage the unique quantum state tomography built by QCNN. The proposed framework achieved better performance than a traditional QFL system in terms of communication cost, faster convergence, and privacy.

The QFL systems employing quantum feature selection aim at identifying the most informative and relevant features by strategic selection of a subset of important features, while the quantum dimensionality reduction techniques focus on reducing the dimensionality of a dataset while preserving its important characteristics in a quantum computing environment. An important way of quantum feature selection is by analyzing the weights of the trained QNN to find the parameters that contribute better to the network's predictions. Li et al. [21] proposed a quantum variational feature selection, which is based on graph theory and the quantum approximate optimization algorithm. He et al. [22] proposed a quantum locally near embedding for nonlinear dimensionality reduction, which can be employed in QFL systems for dimensionality reduction.

### 19.4.3 Network topology

Network topology refers to the way the different quantum systems are connected in the QFL setup. Based on network topology, we divide the QFL systems into three categories: centralized QFL, hierarchical QFL, and decentralized QFL.

In this most popular topology of centralized QFL systems, the central server organizes the model aggregation and coordinates the communications across the client devices based on a hub-and-spoke network model topology. Each client will have either pure quantum models or hybrid quantum models, which they train and send the updates to the server, and receive the updated global model in every iteration. Reduced system complexity, better control over training and synchronizing convergence, and simplified communication protocols are the primary benefits of the centralized QFL setup. The server may employ sophisticated quantum techniques like blind quantum computing and quantum key distribution to guard against hostile and eavesdropping interference nd to guarantee safe communication. A key disadvantage of the centralized QFL topology is that the system is susceptible to the single point of failure problem. Zhang et al. [23] proposed a centralized QFL system based on quantum secure aggregation, which guarantees that all attempts to eavesdrop local model parameters would be immediately detected and stopped. Liu et al. [23] proposed a practical QFL system that enables secure aggregation with information-theoretic security and utilizes distributed quantum secret keys in order to protect local model updates. The authors validated their framework experimentally based on a 4-client quantum neural network.

Hierarchical QFL systems follow a multi-tiered networking design to lower latency, improve scalability, and control quantum resource allocation over large-scale distributed systems. Under this design, the upper layer consists of the central quantum cloud server, while quantum edge servers and quantum clients constitute the lower layer. Through this tiered communication hierarchy, system scalability and training efficiency are enhanced to a great degree. The quantum clients train a local pure or hybrid QML model and send its local updates to quantum edge servers. These intermediate edge servers perform intra-cluster aggregation and then transfer the intermediate global model to the central quantum cloud server, which receives many such intermediate global models and aggregates them to get a final global model. Naorottama et al. [24] proposed a two-tier hierarchical QFL framework for power allocation optimization in wireless networks. Gurung et al. [25] also proposed a hierarchical QFL framework for secure low orbital satellite networks.

In the decentralized QFL setups, several quantum clients collaboratively train a global model based on peer-to-peer networking, thus eliminating the need for a central server. Both the pure and hybrid QFL models can be trained with this setup. After the quantum models are locally trained on the clients, the clients directly exchange the quantum measurement results or model parameters with their neighboring devices over safe communication links based on quantum key distribution and entanglement-assisted quantum networks. Decentralized QFL systems enhance resistance against adversarial attacks, scalability, and fault tolerance, and also remove the single point of failure problem. The quantum systems make use of distributed protocols like blockchained-inspired synchronizing techniques, quantum gossip protocols, and quantum consensus algorithms to achieve collective model convergence. Gurung et al. [26] designed and implemented a trustworthy and decentralized QFL framework for Metaverse services. The proposed systems create transparent and secure systems that are robust to fraud and cyberattacks by leveraging blockchain technology. In another study, Gurung et al. [27] proposed a chained continuous QFL framework which avoids the need for a server and aggregation. In the proposed model, the clients participate in a sequential continuous QFL process. They collaboratively exchange the models among themselves.

### 19.4.4 Quantum security mechanism

QFL frameworks often employ one or more quantum security mechanisms to defend against several possible attacks in the federated learning setup. Based on the employed quantum security mechanism, we divide the QFL systems into four categories: quantum key distribution-based systems, quantum homomorphic encryption-based systems, quantum differential privacy-based systems, and blind quantum computing-based systems.

Quantum Key Distribution (QKD) protocols allow two distributed participants to generate shared cryptographic keys, which ensures secrecy is securely granted. These protocols are inspired by the laws of quantum physics. The quantum principles like quantum superposition, entanglement, and the Heisenberg uncertainty principle are exploited to grant security to QKD protocols. QKD protocols ensure detectable disruptions to the quantum systems in the case of any attempt to eavesdrop. They also rely on the fact that the quantum-generated keys are immune to both quantum and classical attacks [28]. BB84, BB92, and E91 are a few popular QKD protocols [29]. Based on the channel noise or key refresh rate in QKD protocols, QFL systems can dynamically change communication intervals and model update rates. Thus, the use of QKD protocols in QFL systems enhances both the system performance and the security aspects. Liu et al. [30] developed a practical QFL framework that ensures secure aggregation with information-theoretic security and protects local model updates by exploiting QKD protocols. The authors validated their framework on a 4-client framework with a scalable structure. Gurung et al. [25] proposed an access-aware and hierarchical QFL framework that partitions satellites into primary and secondary systems and schedules simultaneous, asynchronous, and sequential edge training. The authors used QKD protocols to grant quantum-resilient integrity and confidentiality, enabling authenticated encryption for model exchange. The authors also make use of quantum teleportation for quantum state transfer.

Quantum Homomorphic Encryption (QHE) provides a quantum analog to classical homomorphic encryption, which preserves confidentiality and privacy by allowing the calculations to be performed on encrypted content without the need for decryption. Thus, QHE allows computation on encrypted quantum states and thus even guards against quantum-powered attackers. A representative diagram of a QHE-enabled QFL system is shown in Fig. 19.3. In QHE-enabled QFL systems, the clients securely provide encrypted updates after training on classical or quantum data to the central server, which trains a global QML model. All the computations at the server happen on encrypted quantum states. Chu et al. [31] proposed CryptoQFL system that enables distributed QML training on encrypted data. CryptoQFL exploits the QHE mechanism to encrypt the local model updates before sending them to the central server. The authors also present a quantum aggregation circuit that significantly reduces the latency. Li et al. [32] also employ QHE for securing their QFL framework. A limitation of QHE in QFL systems is its deployability due to the existing quantum computing constraints, like controlling quantum noise and maintaining coherence.

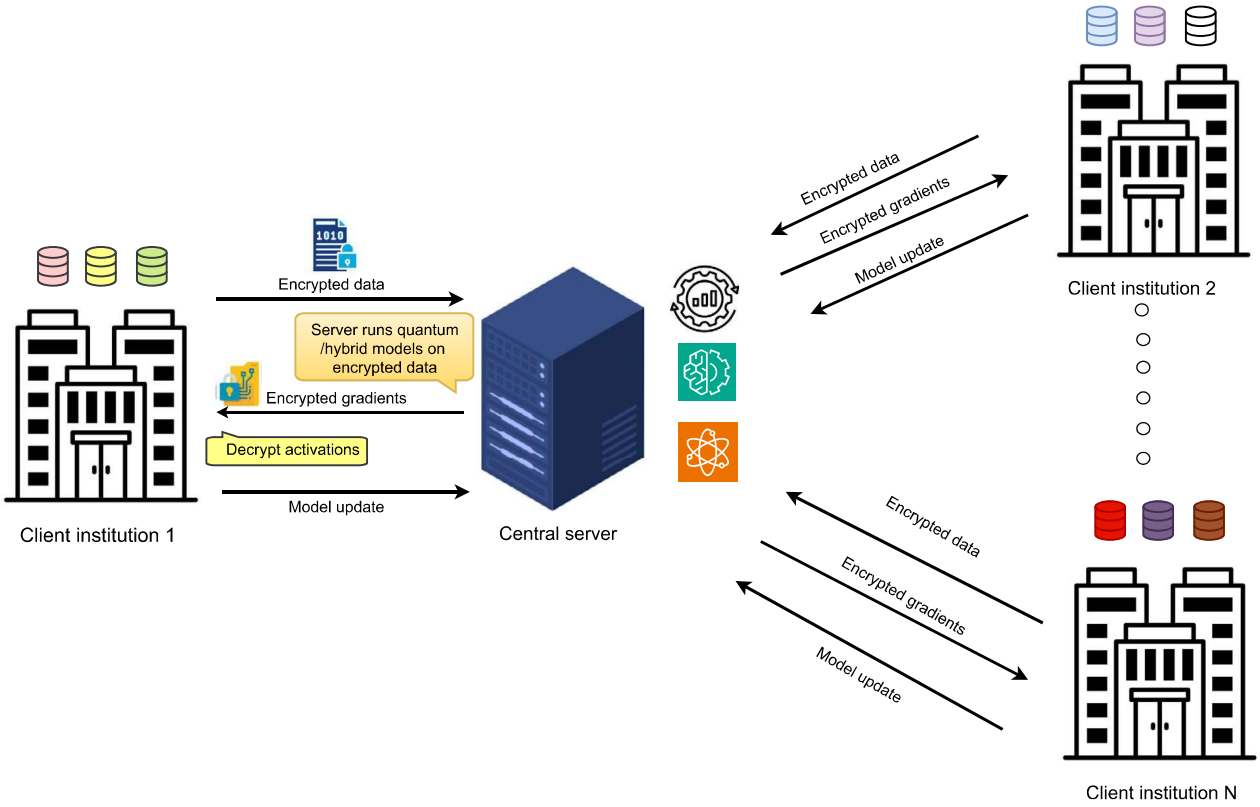


**FIGURE 19.3** Quantum Homomorphic Encryption security mechanism in a QFL framework.

Quantum Differential Privacy (QDP)-based QFL systems extend the classical differential privacy technique into quantum computing by making use of quantum information theory and quantum mechanics to enable security. The classical differential privacy adds calibrated randomness to computations or data to make sure that the output does not reveal whether any single individual's data was included. QDP carefully perturbs quantum measurements or quantum states to avoid the risk of disclosure of information about individual quantum states. Techniques like quantum noise, probabilistic quantum measurement, and quantum uncertainty are utilized to create the perturbations. By integration of QDP in QFL, the clients collaboratively train QML models with the guarantee that the individual contributions remain secure from adversaries and also indistinguishable. Recent research reveals that the QDP can ensure stronger privacy guarantees than classical differential privacy. Rofougaran et al. [44] combined QFL and QDP for the first time to achieve a framework which is resilient to both model inversion attacks (due to QDP) and data leakage (due to QFL). The authors also show federated differentially private training as a viable privacy-preserving method. Pokharel et al. [45] tuned noise variance of QDP through depolarizing channel strength and measurement shots in their QFL system. The authors demonstrated the effectiveness of their framework by considering the relationship between noise parameters and differential privacy budget, and between training accuracy and security.

Blind quantum computing (BQC) allows the clients to delegate quantum computations to computationally stronger quantum servers without disclosing computational tasks or sensitive quantum data. BQC ensures that the server running the computations remains completely unaware of the inputs, intermediate quantum states, and the final output. Quantum techniques like cryptographic obfuscation, unpredictability, and intrinsic uncertainty are employed to achieve blind quantum computing. In QFL systems employing BQC, the client encrypts the (classical) instructions to manipulating the quantum states along with the input quantum states and communicates them to the server for execution. After the server executes the computations, the client decodes the results. An enhancement of BQC, called verifiable blind quantum computing [46], allows the QFL clients to verify that the server had actually performed the computations as per the provided instructions. Li et al. [47] exploited BQC for their QFL system. The authors first proposed a protocol for private single-party training of QML models based on BQC and then extend the same to private multiparty distributed learning with differential

privacy. The simulations by the authors showed that the proposed protocol is secure against gradient inversion attack and also robust to experimental imperfections.

## 19.5 Applications

In this section, we list the applications of QFL across four domains—healthcare, vehicular networks, wireless networks, and network security. A summary of the applications covered is presented in Table 19.1.

**TABLE 19.1** Summary of the covered applications of QFL.

| Work | Contribution | Quantum Architecture | Topology |
|---|---|---|---|
| [33] | Dynamic aggregation quantum federated learning algorithm for intelligent diagnosis in Internet of Medical Things | Pure | Centralized |
| [34] | Framework for quantum-enhanced federated learning with edge computing for advanced pain assessment | Hybrid | Centralized |
| [35] | Federated quanvolutional neural network in a healthcare scenario | Hybrid | Centralized |
| [36] | Federated hierarchical tensor networks for healthcare | Hybrid | Centralized |
| [37] | Quantum-enhanced federated learning for metaverse-empowered vehicular networks | Pure | Decentralized |
| [38] | Quantum-based federated learning framework for defending against adversarial attacks in intelligent transportation systems | Hybrid | Centralized |
| [39] | Quantum federated learning algorithm for speech emotion recognition in 5G IoV | Hybrid | Centralized |
| [40] | Quantum federated learning for space-air-ground integrated networks | Pure | Centralized |
| [41] | Quantum federated reinforcement-learning-based joint mode selection and resource allocation for STAR-RIS-aided VRCS | Pure | Centralized |
| [42] | Hybrid quantum enhanced federated learning for cyber attack detection | Hybrid | Hierarchical |
| [43] | Quantum federated adversarial learning | Pure | Centralized |

### 19.5.1 Healthcare

QFL for healthcare brings QC's capacity for optimization and compact representations to the privacy-preserving workflow of federated learning. Healthcare is a strong testbed for QFL, given several issues of FL in healthcare like heterogeneous data, limited labels, class imbalance, and the need for robust generalization across hospitals.

Zhiguo et al. [33] proposed a Dynamic Aggregation Quantum Federated Learning (DAQFL) framework to improve the performance of QFL models on IoMT-based heterogeneous healthcare data. The framework employs both VQCs and QNNS for local model training. The authors proposed a dynamic aggregation technique where the central server weighs the clients' updates based on the reported accuracy of the client in that round. The higher the accuracy of the local model, the more weight the local model's weights are given in aggregation. The authors conducted experiments on IID, non-IID, and long-tail data distributions, which show the superior performance of the proposed framework in terms of training speed, accuracy, and even with high heterogeneity.

Balasubramani et al. [34] introduced a framework that combined QFL with quantum transfer learning to create a privacy-preserving and robust system for classifying pain levels based on electrocardiogram (ECG) signals. At the EHE computing layer, the raw one-dimensional ECG signals are preprocessed and then transformed into Continuous Wavelet Transform (CWT) images that capture both frequency and time characteristics of cardiac variation. A quantum convolutional hybrid neural network is used to encode the classical features into a 9-qubit PQC for further processing. The authors also used homomorphic encryption to ensure privacy during aggregation of local models. The experimental results show that the proposed QFL model achieved a better performance than the classical model with a tan accuracy of 94.8%.

Bhatia et al. [35] proposed a hybrid quanvolutional neural network-based QFL framework for privacy-preserving training on real-world and non-IID medical image data. The authors use a quanvolutional layer (as a part of QCNN) to encode small subsections of an input image into quantum states using parametrized gates. A learnable quantum circuit is used to process the quantum states, and the resultant outputs' measurements are used for subsequent classical poling and dense layers. The authors also experimented with a combination of a classical CNN with a 16-qubit variational quantum

circuit for classification. The experimental results showed that the proposed model achieved a communication speedup of 14 and 40 times over the baseline and also achieved good accuracy.

In another study, Bhatia et al. [36] FedQTN—a QFL framework based on Quantum Tensor Networks (QTNs) and differential privacy. The proposed framework utilizes three different hierarchical QTN architectures as local models—multiscale entanglement renormalization ansatz, tree tensor network, and matrix product state. The authors followed a patch-based encoding scheme to encode the input images, where each image is divided into smaller patches that are individually flattened and encoded into quantum states through single-qubit rotations. After encoding, the quantum states are then fed to QTN circuits, which are built using two-qubit unitary gates arranged in a strong or simple entangling block structure. The authors used the FedAvg aggregation algorithm, and the results show that the proposed FedTTN consistently achieved the fastest training convergence. Their experimentation on MRI and CT-scan datasets significantly improved the performance of low-data clients.

### 19.5.2 Vehicular networks

QFL for vehicular networks integrates the quantum subroutines with privacy-preserving collaborative training to deal with the heterogeneous and high-velocity roadside data. The vehicular networks setting imposes strict bandwidth and latency limits, intermittent connectivity, and frequent topology changes; hence, integrating light-weight client-side quantum modules with communication-efficient aggregation would be helpful. The importance of security in vehicular networks also motivates quantum-safe keying with quantum protocols.

Hazarika et al. [37] introduced QV-FedCom, a decentralized and heterogeneity-aware QFL framework for the vehicular metaverse that aims to address challenges of data heterogeneity, memory efficiency, and communication cost. The proposed framework has three components—Quantum-inspired PCA (QPCA), Quantum Sequential Training Program (QSTP), and Quantum Vehicle Context Grouping (QVCG). QPCA is applied as a data processing method to compress quantum data and reduce the memory footprint. QVCG manages heterogeneity by employing simulated annealing and hierarchical clustering to group vehicles based on contextual data similarity. QSTP employs reinforcement learning to dynamically switch vehicles between local calibration mode and active streaming mode in order to minimize communication costs. The framework also utilizes quantum trajectory loss (QTL), which is a combination of angular deviation penalty and Huber loss to robustly handle errors in trajectory prediction tasks. The proposed framework consistently outperformed baseline models, achieving a test accuracy of 85%. The ablation studies also showed the effectiveness of the framework's individual components—QSTP maintained the lowest communication cost, and the integration of QPCA reduced memory consumption from 16 GB to 13 GB.

Yamany et al. [38] proposed a novel Optimized Quantum-based Federated Learning (OQFL) framework, which is designed to defend against data poisoning attacks in intelligent transportation systems. Quantum-behaved Particle Swarm Optimization (QPSO) is employed by the authors to automatically tune the hyperparameters of the FL process. QPSO optimizes the number of local and global epochs, the learning rate, with an aim of enhancing the model's resilience against adversarial attacks. Analogous to a classical PSO, each particle in QPSO represents a combination of the above-mentioned hyperparameters, and the technique evolves the population to find the combination that yields the highest accuracy. The authors simulated an adversarial environment with four data poisoning attacks while training using QPSO. Tested on the Fashion-MNIST dataset and MNIST dataset, the proposed framework achieved around 98% accuracy while maintaining a high accuracy of 91% even when subjected to data poisoning attacks.

Qu et al. [39] proposed a novel framework for addressing the challenges of computational efficiency and privacy in speech emotion recognition in 5G Internet of Vehicles (IoV). In the 5G IoV setup, the vehicles collect speech data and send it to edge servers that act as clients in the QFL system. The authors use Quantum Minimal Gated Units (QMGUs) to perform local model training at edge servers. QMGU improves the classical MGU by replacing its non-linear functions with VQCs, which enables faster convergence. The VQCs are implemented using a 4-qubit architecture, which consists of a variational part with RX and CNOT gates and an encoding part with an RX gate. All the edge servers coordinate with a central cloud server for the FL process. The authors show that the proposed QMGU model achieved a superior F1-score compared to QLSTM and QGRU while only using a few resources in terms of qubits and parameters.

### 19.5.3 Wireless networks

QFL for wireless networks integrates quantum subroutines into FL to handle tight resource budgets and fast-changing radio environments. The core concerns, like reliability and security, motivate quantum-safe key exchange and robust aggregation against adversarial updates in FL.

Quy et al. [40] explored the application of QFL to Space-Air-Ground Integrated Networks (SAGINs) to enable computationally efficient and privacy-enhanced AI model training for 6G applications. In the proposed framework, a base station serves as a central aggregator with a network of Unmanned Aerial Vehicles (UAVs) being the clients. The proposed quantum machine learning model operates on four qubits, making use of a controlled-rotation (CRX) gate and single-qubit rotation gates (RX, RY, RZ). In the experimentation, the authors compared the performance of their framework with classical FL, showing that the proposed framework has a faster convergence with a convergence of up to 90% accuracy in 10 epochs, which took classical FL 40 epochs.

Chaudhary et al. [41] proposed a QFL framework for joint optimization of resource allocation and mode selection in a Simultaneous Transmission and Reflection-Reconfigurable Intelligent Surface (STAR-RIS) assisted Vehicle-Road Cooperation System (VRCS). The authors formulated the joint optimization problem as a Markov Decision Process (MDP), where every V2V pair acts as an agent making decisions. Local observations like queue length and channel gains include the state space for the agent while the action space consists of sub-channel allocation, transmission mode selection, and power control. A novel Quantum Federated Reinforcement Learning (QFRL) algorithm is employed to solve MDP problems where vehicles collaboratively train a global model. A QNN is used as a local model, and each client employs a fidelity-based cost function. The authors demonstrate the superior performance of the proposed QFRL compared to the traditional QFL framework with a 20% improvement in network sum-rate. QFRL also showed improvements in terms of latency, recording a latency of 2.2 ms compared to 3.2 ms for standard FL.

### 19.5.4 Network security

QFL helps in network security by merging with FL with quantum techniques to detect threats across organizations without exposing the edge devices' data and logs to cloud providers. Variational circuits and quantum kernels enrich feature spaces for obfuscated signals, improving sampling efficiency in wireless networks.

Subramanian et al. [42] integrated Quantum-inspired Federated Averaging (QIFA) and Spatio-Temporal Attention Network (STAN) to propose a hybrid federated learning framework for cyber-attack detection. The framework employs hierarchical model aggregation, where the nodes in the network are dynamically grouped into regions based on k-means clustering using a combined score of network conditions and data similarity. After each local node trains its STAN model, the model updates of each region are aggregated by a regional server to create an intermediate regional model. These regional models are then sent to a central server, which uses QIFA for global model aggregation. Notably, the QIFA algorithm introduces periodic quantum-inspired perturbations and a quantum superposition-based adjustment term to avoid local minima and improve convergence. The authors evaluated the proposed framework on the UNSW-NB15 dataset, where it achieved a high accuracy of 98.3%, which is superior compared to the standard FL models.

Maouaki et al. [43] integrated adversarial training into QFL to defend against adversaries or vulnerabilities in a distributed environment. Each client trains a local 6-qubit QNN using amplitude encoding to prepare the initial quantum state. A strongly entangling parametrized circuit with two layers is used to process the encoded quantum states, after which the final measurements are taken for classification. The methodology also involves local adversarial training where a particular fraction of clients generate adversarial examples by using the Projected Gradient Descent (PGD) technique. The clients generating adversarial data update their local models using mini-batches composed of 50% perturbed data and 50% clean data. The experimental results showed a clear tradeoff between robustness and accuracy in a 5-client system—an introduction of 20% adversarial training data improved resistance to attacks by 12.48%, but at the cost of a 4.83% drop in clean-data accuracy. The authors noted that larger QFL rounds are more effective in balancing accuracy and robustness.

## 19.6 Case study 1: quantum enhanced federated framework for financial fraud detection

In this section, we present a case for the use of QFL techniques in financial applications in fraud detection, which is derived from the work of Sawaika et al. [48].

### 19.6.1 Motivation

With an unprecedented increase in the use of digital modes for financial transactions, vulnerabilities to various threats have also increased simultaneously [49]. These include, but are not limited to, insurance fraud, identity theft, phishing, investment fraud, online transaction fraud, etc [50]. Some of the recent works using classical ML techniques to solve such problems in financial systems include those by Hashedi et al. [51], Cheng et al. [52], and Ali et al. [53]. Quantum

approaches were also recently studied by Innan et al. [54], Paquet et al. [55], Innan et al. [56], with Innan et al. proposing a federated framework for fraud detection in [56]. With around a trillion dollars in terms of market impact, McKinsey [57] predicts around $633 billion market for quantum technologies in financial use cases. Being one of the critical and sensitive areas of the field, it becomes crucial to investigate state-of-the-art algorithms using quantum federated learning to address such problems for improved performance and accuracy.

### 19.6.2 Problem of interest

We designed this QFL model to create a robust framework for fraud detection in online transactional systems. Various design decisions were taken at different stages to create a system that improves performance, via increased accuracy, recall, and reduced false positives. It is also scalable for data and model sizes, and provides for security against various attacks possible in a generalized federated framework. In the solution methodology described in the following section, we will only discuss the modeling strategy for the QFL framework and the underlying ML model used, with a brief discussion on some basic results in the results section.

### 19.6.3 Solution methodology

Fig. 19.4 presents an overall training pipeline of the proposed solution with key aspects of the federated framework, the enhanced model, and the privacy-preserving merging strategy. The boxes in blue (light gray in print version) indicate the QLSTM model trained on local data, whereas the yellow ones (mid gray in print version) are part of the merging strategy. The whole system is designed as a pseudo-centralized federated model where the global model is used for aggregation, but doesn't necessarily have the whole information of a consensus model.

The process starts by preprocessing the dataset. For experiment simulation, we have divided the whole data based on an IID distribution among multiple nodes (parties). But in real-life scenarios, each node will bring its own data. Each node then preprocesses the data and puts it for training. Once all the local models are trained for one epoch, each node samples the weights and shares only a subset of the weights to the global server. Which then merge the common parameters, sample the merged parameters, and send them back to each node for the next round of training. This sampling is done to minimize the exposure to inference and poisoning attacks. This happens for multiple epochs until an accepted convergence.

As noted earlier, it consists of a quantum-enhanced LSTM model. In Fig. 19.5, we have the structure of a general LSTM model with three cells. Each cell (see Fig. 19.6) is designed to have four main NN structures, namely forget, input, update, and output. These help in learning the linear structure from the input dataset sequence. Details on the LSTM model can be seen in the original work by Hochreiter et al. [58]. For each of these functions, we use a VQC to replace a NN. And as one can see, these VQCs are where our quantum models lie, providing enhancement and guarantees to the problems we set for us in this study.

The parameterized structure of the VQC is designed using universal rotation unitaries and CNOT gates for full entanglement. Angle encoding using RX gates is used as the encoding layer. This design of VQC helps in increasing expressivity of the features in Hilbert's space and to capture complex relations between input features (see Fig. 19.7). The universal Rot gate is defined as:

$$R(\phi, \theta, \omega) = RX(\phi)\, RY(\theta)\, RZ(\omega) \tag{19.2}$$

### 19.6.4 Results and discussion

This study used a real-life fraud detection bank dataset with 20K rows and 120 encoded numerical features (Dataset 1), and a synthetic financial dataset (Dataset 2) with 5M rows and five categorical features, available at [59], [60], respectively. The results discussed in this study were obtained on 20K data points from both datasets. Best results are obtained for (number of qubits, depth, sequence length) as (9, 10, 10) for Dataset 1 and (9, 4, 5) for Dataset 2, respectively.

Figs. 19.8, 19.9, 19.10 project the comparison between a classical analogous LSTM model and a traditional non-neural network-based SVM model with the proposed QLSTM model, under a federated setup with five nodes. We observed that One-Class SVM performs poorly, with accuracy scores of only 0.61 for Dataset 1 and 0.73 for Dataset 2. More importantly, the QLSTM model outperforms the classical LSTM by approximately 2% in AUC, 5% in Accuracy, and 10% in Recall for Dataset 1; and by 3% in AUC, 6% in Accuracy, and 4% in Recall for Dataset 2.

Fig. 19.11 plots the performance of the proposed model under federated expansion. We observed a decreasing trend with the increasing number of nodes. This is primarily due to the smaller dataset available per node for training, which limits the local convergence of each model. This may not be the case in real-life scenarios where an additional node brings

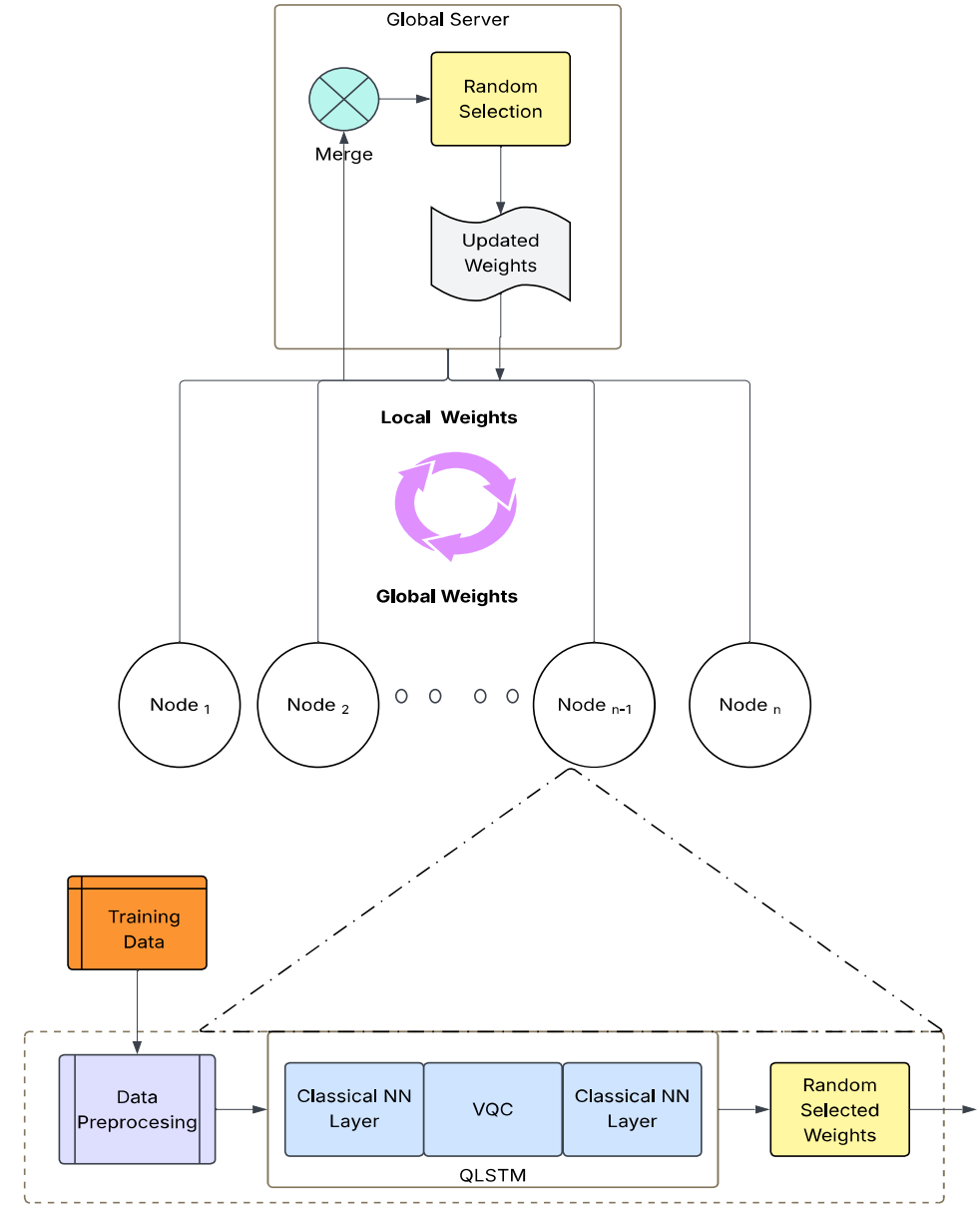


**FIGURE 19.4** Training workflow of our framework demonstrating local quantum-enhanced computations, federated aggregation, and secure update exchanges.

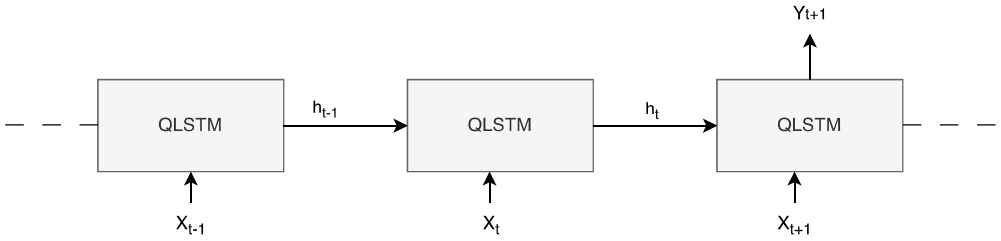


**FIGURE 19.5** QLSTM model demonstrating a 3-sequence architecture with output taken only at the last cell. Each cell processes the input at that time step (t) as $\mathbf{X}_t$ and generates a hidden state $\mathbf{h}_t$ and the output $\mathbf{Y}_t$.

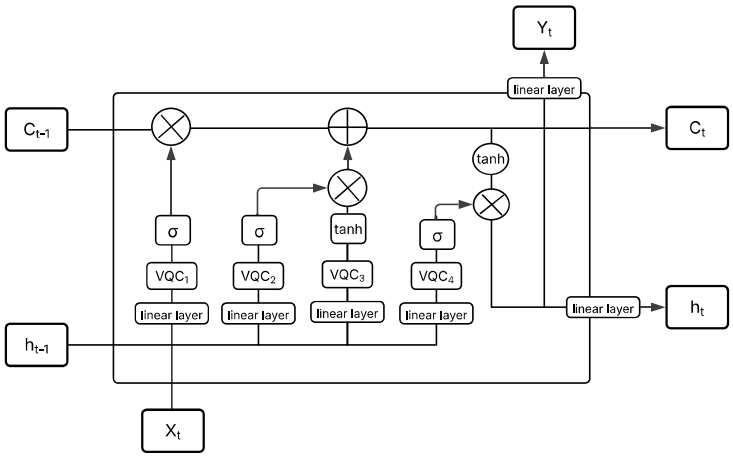


**FIGURE 19.6** Architecture of a single QLSTM cell for the model depicted in Fig. 19.5.

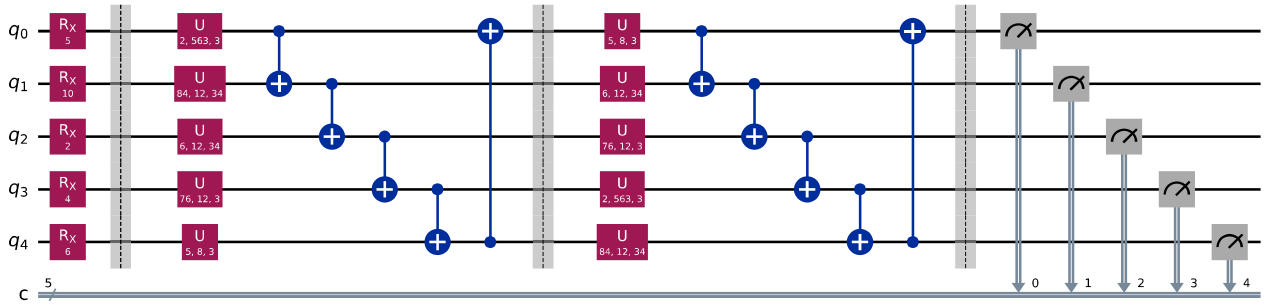


**FIGURE 19.7** A sample five-qubit structure of the designed VQC with two layers. It can be generalized recursively for a larger number of qubits and layers as well.

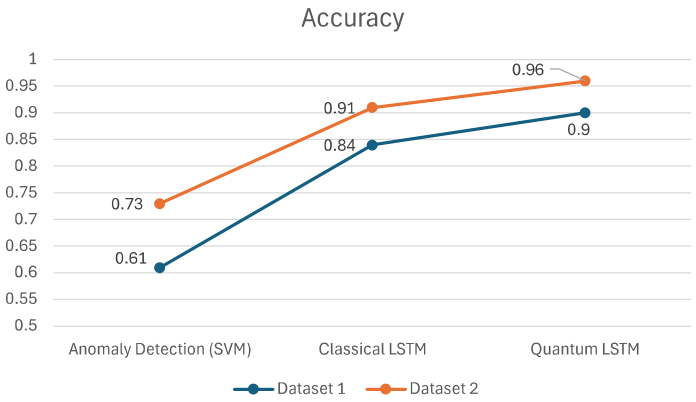


**FIGURE 19.8** Performance accuracy comparisons of different models under a 5-node federated setup for datasets 1 and 2.

more data for training in practical use cases. There are mixed results on the impact of node counts on federated performance in the existing literature. But trends shown in Fig. 19.11 are expected for our experiment setup.

## 19.7 Case study 2: sat-QFL—secure quantum federated learning for low orbit satellites

The popularity of lower Earth orbit (LEO) satellite networks has experienced significant growth over time, with companies such as SpaceX investing substantial resources to facilitate internet accessibility in remote regions. Consequently,

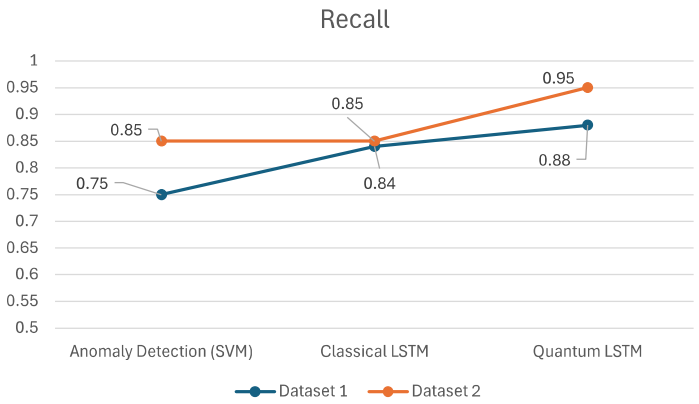


**FIGURE 19.9** Performance recall comparisons of different models under a 5-node federated setup for datasets 1 and 2.

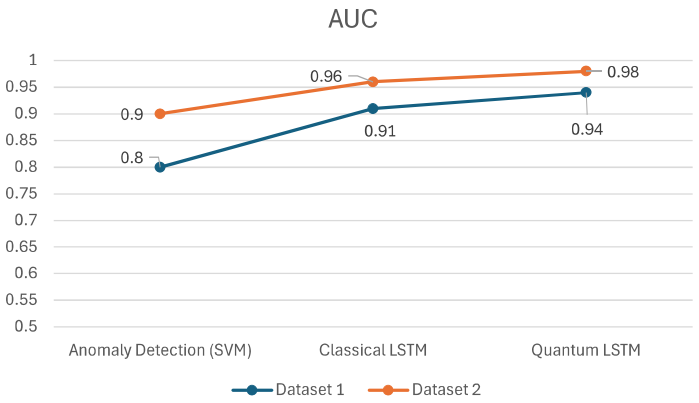


**FIGURE 19.10** Performance AUC comparisons of different models under a 5-node federated setup for datasets 1 and 2.

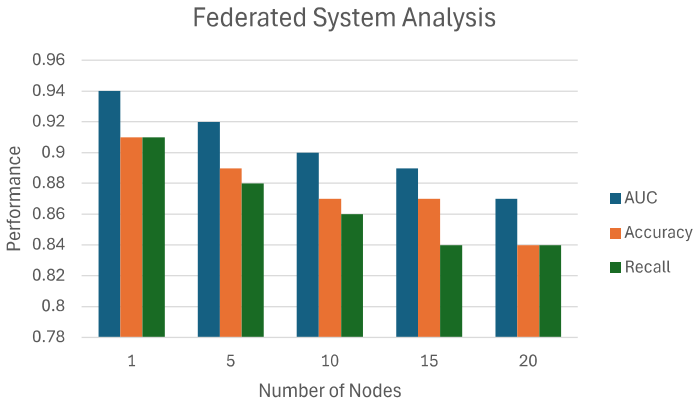


**FIGURE 19.11** Federation analysis of the QLSTM model for dataset 1.

researchers have been investigating the potential adaptation of technologies like federated learning and quantum federated learning, which were initially developed for traditional networks, to satellite networks. Satellite networks encounter unique challenges, including fluctuating ground links due to orbital motion, rapidly changing client participation, and stringent latency and energy constraints. These challenges have led to the development of sat-QFL [25], a hierarchical access-aware quantum federated learning framework. Sat-QFL models satellites and ground stations as a time-varying line-of-sight graph $H(t)$ and assigns two distinct roles: primary satellites that currently possess a direct line of sight to the ground and secondary satellites that must relay data through their neighboring satellites. At any given time $t$, only nodes with a feasible path to a

ground station are permitted to participate in the training process. Instead of waiting for all nodes to participate, sat-QFL aggregates the updates that actually arrive. The proposed method, referred to as *sat-QFL*, organizes training sessions around the periods when links are available. It offers three distinct modes for transferring model updates: sequential, simultaneous, and asynchronous. In the sequential mode, secondary satellites transmit weights along a chain until a primary satellite can forward them to the ground station. In the simultaneous mode, multiple secondaries train concurrently and transmit their updates to a primary satellite that performs a local average. In the asynchronous mode, satellites transmit updates whenever a link becomes available, and the receiver aggregates the updates at the conclusion of the link period. These diverse modes contribute to the reduction of idle time caused by strict lockstep rounds and enhance the alignment with the dynamic nature of contact opportunities in orbit.

Security is inherently integrated into the system's design. Quantum key distribution is employed to establish symmetric keys, and authenticated encryption is utilized to safeguard model exchanges. The study further investigates quantum teleportation as a viable approach for transferring parameter information when prior entanglement is available. These enhancements are intended to provide confidentiality and integrity against quantum-capable eavesdroppers without altering the learning objective or the loss being optimized. The implementation utilizes Qiskit-based quantum learning workloads and operates on derived constellation traces. Results are presented on the Statlog and EuroSAT datasets, comparing the three scheduling modes and their secure variants, including versions that incorporate teleportation, QKD exclusively, and QKD in conjunction with standard authenticated encryption. The primary trade-off is straightforward. A fully synchronized baseline may appear faster when only round time is considered, but it assumes conditions that Low Earth Orbit (LEO) does not provide. The sat-QFL modes introduce some communication time due to adherence to access windows and the application of security measures, yet they maintain model quality competitiveness and render the overall procedure feasible on orbit. Certain secure runs exhibit variability that warrants further investigation, and the communication-time summaries delineate the anticipated balance between practicality and speed.

In essence, sat-QFL pairs a straightforward role division with window-aware scheduling and built-in security. By grounding participation in $H(t)$ and safeguarding updates over the available links, it transforms quantum federated learning into a process that aligns with the actual connectivity and communication patterns of LEO constellations.

## 19.8 Challenges and future research directions

**Expansion of Machine Learning Tasks:** Most of the research works on QFL focused on classification tasks, thus limiting its potential in other applications [61]. Hence, it is crucial to explore beyond classification tasks. Tasks like time-series analysis, optimization, complex decision making, object detection, semantic segmentation, and named entity recognition can greatly benefit from the QFL framework. Expanding QFL applications into these areas could foster innovation in both federated learning and quantum domains, also revealing the advantages of quantum computing. Another important challenge in this regard is that the research papers lack a clear justification for using quantum resources—what is the need to use quantum techniques when the same problem is already being efficiently solved by classical methods?

**Quantum techniques for Adversarial attacks:** Although implementing adversarial attacks in QFL setups is more challenging than in FL setups, the recent research shows that it's still possible. Byzantine attacks and gradient inversion attacks are more researched types of adversarial attacks. In Byzantine attacks, malicious clients send corrupted updates for the global model aggregation, while gradient inversion attacks focus on reconstructing clients' data from the gradients shared in the QFL process. Future work can focus on exploiting quantum techniques for building mitigation protocols against adversarial attacks. Existing works are still focusing on classical techniques only to build attack-resistant algorithms.

**Realistic hardware implementation:** Most of the works in the domain of QFL are currently at the level of simulation only. Very few papers explored the hardware implementations of their proposed QFL frameworks. Hence, research must be directed into hardware implementations, considering realistic scenarios like noise. The resilience of the QFL models could be checked by incorporating noise into simulations. Particularly, dephasing or depolarizing noise could be added to local computations. Important inferences on how different types of quantum noise affect global aggregation and local training steps could be inferred, paving the way to real-world deployment of QFL systems.

**Deployment of quantum communication protocols:** Multiple QFL works covered in this chapter utilized quantum key distribution techniques to secure communications. However, the existing quantum hardware is still in a very early stage, making the practical deployment of quantum communication protocols a critical challenge. It requires very costly and sophisticated equipment to create and manipulate entangled particles over long distances. On top of it, building and scaling communication networks in realistic federated learning setups is a great obstacle.

**Aggregation of different quantum models:** Research works covered in this chapter all aggregate the same type of local models to obtain a global mode. However, in classical FL scenarios, research has been undertaken in terms of the aggregation of different local models. For instance, Scale-FL [62] proposes to aggregate different local models at different scales. Hence, research efforts can be directed to exploring whether different quantum models could learn from one another. If that were to be proved feasible, strategies could be proposed to leverage the unique strength of each quantum model to produce a robust quantum global model.

**Quantum Split Learning as an alternative to QFL:** Split learning is a collaborative learning framework that serves as an alternative to FL, particularly in scenarios with resource-constrained clients. The main idea of split learning is to cut the neural network between clients and server (and then train the neural network in parts) in such a way that there is less computational load on the clients' side. It can be effectively introduced in place of FL to enable Quantum Split Learning. QSL partitions the model so that clients train only the front classical layers or light-weight quantum layers and send the intermediate activations to a server, which does the major part of the quantum layers' training (which is generally computationally heavy). QSL also improves reliability by centralizing the compute-intensive and deeper layers on stable server hardware while allowing heterogeneous clients to train in a flexible fashion. QSL is a better fit when bandwidth is tight, devices are weak, and quantum hardware access is intermittent.

## 19.9 Summary

This chapter presented a survey of quantum federated learning with a systematic taxonomy covering quantum architecture, data processing method, network topology, and quantum security mechanisms. The design choices across these dimensions depend on the deployment needs of the institutions participating in QFL. The progression from classical FL to QFL shows how the scarce quantum resources should be targeted at high points of leverage like aggregation, secure communication, and feature mapping. Through the representative case study, we validate the end-to-end feasibility of QFL systems. Our findings from the applications of QFL in healthcare, vehicular networks, wireless networks, and network security revealed that the QFL can match or even outperform classical FL models while reducing the time for convergence, and enhancing the communication safety. One of our insights from the recent research in QFL is that the proposed systems are mostly focusing on improving performance compared to classical baselines. However, other dimensions of security and deployment should be researched well to develop practical QFL systems. Another key insight is that split learning in QFL scenarios would be better suited for resource-limited clients because it can keep all data local, transmit compact activations instead of full gradients, and shift deep computation to resource-heavy servers, thus easing bandwidth constraints. In practical scenarios, the clients in the QFL setup are not expected to have a good amount of quantum computational power. Hence, techniques like shadow tomography should be researched, which delegates the quantum computation to resource-heavy systems. Despite encouraging results, several critical challenges remain in building deployable QFL systems. Apart from realistic hardware deployments, integration of quantum techniques for building adversarial-resistant quantum systems, and the development of standard benchmarks remain a strong direction for future work.

## References

[1] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, Y. Gao, A survey on federated learning, Knowledge-Based Systems 216 (2021) 106775.
[2] Z. Li, K. Xue, J. Li, L. Chen, R. Li, Z. Wang, N. Yu, D.S. Wei, Q. Sun, J. Lu, Entanglement-assisted quantum networks: mechanics, enabling technologies, challenges, and research directions, IEEE Communications Surveys and Tutorials 25 (4) (2023) 2133–2189.
[3] V. Rishiwal, U. Agarwal, M. Yadav, S. Tanwar, D. Garg, M. Guizani, A new alliance of machine learning and quantum computing: concepts, attacks, and challenges in IoT networks, IEEE Internet of Things Journal 12 (12) (2025) 18865–18886.
[4] M. Kjaergaard, M.E. Schwartz, J. Braumüller, P. Krantz, J.I.-J. Wang, S. Gustavsson, W.D. Oliver, Superconducting qubits: current state of play, Annual Review of Condensed Matter Physics 11 (1) (2020) 369–395.
[5] C.D. Bruzewicz, J. Chiaverini, R. McConnell, J.M. Sage, Trapped-ion quantum computing: progress and challenges, Applied Physics Reviews 6 (2) (2019).
[6] M. Morgado, S. Whitlock, Quantum simulation and computing with Rydberg-interacting qubits, AVS Quantum Science 3 (2) (2021).
[7] F. Flamini, N. Spagnolo, F. Sciarrino, Photonic quantum information processing: a review, Reports on Progress in Physics 82 (1) (2018) 016001.
[8] F.A. Zwanenburg, A.S. Dzurak, A. Morello, M.Y. Simmons, L.C. Hollenberg, G. Klimeck, S. Rogge, S.N. Coppersmith, M.A. Eriksson, Silicon quantum electronics, Reviews of Modern Physics 85 (3) (2013) 961–1019.
[9] J. Alicea, New directions in the pursuit of Majorana fermions in solid state systems, Reports on Progress in Physics 75 (7) (2012) 076501.
[10] M. Schuld, F. Petruccione, Supervised learning with quantum computers, Quantum Science and Technology 17 (2018).
[11] D.C. Nguyen, M.R. Uddin, S. Shaon, R. Rahman, O. Dobre, D. Niyato, Quantum federated learning: a comprehensive survey, arXiv:2508.15998, 2025.

[12] R. Huang, X. Tan, Q. Xu, Quantum federated learning with decentralized data, IEEE Journal of Selected Topics in Quantum Electronics 28 (4: Mach. Learn. in Photon. Commun. and Meas. Syst.) (2022) 1–10.
[13] S. Park, H. Lee, S. Jung, J. Park, M. Bennis, J. Kim, Entanglement-controlled quantum federated learning, IEEE Internet of Things Journal (2025).
[14] Z. Abou El Houda, H. Moudoud, B. Brik, M. Adil, A privacy-preserving framework for efficient network intrusion detection in consumer network using quantum federated learning, IEEE Transactions on Consumer Electronics (2024).
[15] C. Ren, R. Yan, M. Xu, H. Yu, Y. Xu, D. Niyato, Z.Y. Dong, QFDSA: a quantum-secured federated learning system for smart grid dynamic security assessment, IEEE Internet of Things Journal 11 (5) (2023) 8414–8426.
[16] K. Hisamori, Y.-H. Chiang, H. Lin, Y. Ji, Hybrid quantum-classical computing in federated learning with data heterogeneity, in: 2024 IEEE 35th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2024, pp. 1–6.
[17] C. Ren, R. Yan, H. Zhu, H. Yu, M. Xu, Y. Shen, Y. Xu, M. Xiao, Z.Y. Dong, M. Skoglund, D. Niyato, L.C. Kwek, Toward quantum federated learning, IEEE Transactions on Neural Networks and Learning Systems 36 (9) (2025) 15580–15600.
[18] C.-H.H. Yang, J. Qi, S.Y.-C. Chen, Y. Tsao, P.-Y. Chen, When BERT meets quantum temporal convolution learning for text classification in heterogeneous computing, in: ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2022, pp. 8602–8606.
[19] C.-H.H. Yang, J. Qi, S.Y.-C. Chen, P.-Y. Chen, S.M. Siniscalchi, X. Ma, C.-H. Lee, Decentralizing feature extraction with quantum convolutional neural network for automatic speech recognition, in: ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2021, pp. 6523–6527.
[20] W.J. Yun, H. Baek, J. Kim, Quantum split neural network learning using cross-channel pooling, arXiv preprint, arXiv:2211.06524, 2022.
[21] Y. Li, R.-G. Zhou, R. Xu, J. Luo, W. Hu, P. Fan, Implementing graph-theoretic feature selection by quantum approximate optimization algorithm, IEEE Transactions on Neural Networks and Learning Systems 35 (2) (2022) 2364–2377.
[22] X. He, L. Sun, C. Lyu, X. Wang, Quantum locally linear embedding for nonlinear dimensionality reduction, Quantum Information Processing 19 (9) (2020) 309.
[23] Y. Zhang, C. Zhang, C. Zhang, L. Fan, B. Zeng, Q. Yang, Federated learning with quantum secure aggregation, arXiv preprint, arXiv:2207.07444, 2022.
[24] B. Narottama, S.S. Yang, Quantum federated learning for wireless communications. Available: https://journal-home.s3.ap-northeast-2.amazonaws.com/site/2020kics/presentation/0480.pdf. (Accessed 1 October 2025).
[25] D. Gurung, S.R. Pokhrel, sat-QFL: secure quantum federated learning for low orbit satellites, arXiv preprint, arXiv:2509.16504, 2025.
[26] D. Gurung, S.R. Pokhrel, G. Li, Decentralized quantum federated learning for metaverse: analysis, design and implementation, arXiv preprint, arXiv:2306.11297, 2023.
[27] D. Gurung, S.R. Pokhrel, Chained continuous quantum federated learning framework, Future Generation Computer Systems 169 (2025) 107800.
[28] S. Ravikumar, E. Chandralekha, K. Vijay, K. Antony Kumar, C. Pretty Diana Cyril, Quantum-secured collaborative machine learning: facilitating privacy-protecting quantum federated learning, in: International Conference on Computing and Communication Networks, Springer, 2023, pp. 537–550.
[29] M.S. Peelam, S. Sai, V. Chamola, Explorative implementation of quantum key distribution algorithms for secure consumer electronics networks, IEEE Transactions on Consumer Electronics 70 (3) (2024) 5576–5584.
[30] Z.-P. Liu, X.-Y. Cao, H.-W. Liu, X.-R. Sun, Y. Bao, Y.-S. Lu, H.-L. Yin, Z.-B. Chen, Practical quantum federated learning and its experimental demonstration, arXiv preprint, arXiv:2501.12709, 2025.
[31] C. Chu, L. Jiang, F. Chen, CryptoQFL: quantum federated learning on encrypted data, in: 2023 IEEE International Conference on Quantum Computing and Engineering (QCE), vol. 1, IEEE, 2023, pp. 1231–1237.
[32] W. Li, D.-L. Deng, Quantum delegated and federated learning via quantum homomorphic encryption, Research Directions. Quantum Technologies 3 (2025) e3.
[33] Z. Qu, X. Zhao, L. Sun, G. Muhammad, DAQFL: dynamic aggregation quantum federated learning algorithm for intelligent diagnosis in Internet of medical things, IEEE Internet of Things Journal (2025).
[34] M. Balasubramani, M. Srinivasan, W.-H. Jean, S.-Z. Fan, J.-S. Shieh, A novel framework for quantum-enhanced federated learning with edge computing for advanced pain assessment using ECG signals via continuous wavelet transform images, Sensors 25 (5) (2025) 1436.
[35] A.S. Bhatia, S. Kais, M.A. Alam, Federated quanvolutional neural network: a new paradigm for collaborative quantum learning, Quantum Science and Technology 8 (4) (2023) 045032.
[36] Amandeep Singh Bhatia, David E. Bernal Neira, Federated learning with tensor networks: a quantum AI framework for healthcare, Machine Learning: Science and Technology 5 (4) (2024) 045035.
[37] B. Hazarika, K. Singh, O.A. Dobre, C.-P. Li, T.Q. Duong, Quantum-enhanced federated learning for metaverse-empowered vehicular networks, IEEE Transactions on Communications 73 (6) (2025) 4168–4183.
[38] W. Yamany, N. Moustafa, B. Turnbull, OQFL: an optimized quantum-based federated learning framework for defending against adversarial attacks in intelligent transportation systems, IEEE Transactions on Intelligent Transportation Systems 24 (1) (2023) 893–903.
[39] Z. Qu, Z. Chen, S. Dehdashti, P. Tiwari, QFSM: a novel quantum federated learning algorithm for speech emotion recognition with minimal gated unit in 5G IoV, IEEE Transactions on Intelligent Vehicles 9 (10) (2024) 6512–6523.
[40] Vu Khanh Quy, Nguyen Minh Quy, Tran Thi Hoai, Shaba Shaon, Md Raihan Uddin, Tien Nguyen, Dinh C. Nguyen, Aryan Kaushik, Periklis Chatzimisios, From federated learning to quantum federated learning for space-air-ground integrated networks, in: 2024 IEEE Conference on Standards for Communications and Networking (CSCN), IEEE, 2024, pp. 402–407.

[41] S. Chaudhary, I. Budhiraja, R. Chaudhary, N. Kumar, D. Garg, A.M. Almuhaideb, Quantum federated reinforcement-learning-based joint mode selection and resource allocation for STAR-RIS-aided VRCS, IEEE Internet of Things Journal 11 (22) (2024) 36242–36256.
[42] G. Subramanian, M. Chinnadurai, Hybrid quantum enhanced federated learning for cyber attack detection, Scientific Reports 14 (1) (2024) 32038.
[43] W.E. Maouaki, N. Innan, A. Marchisio, T. Said, M. Bennai, M. Shafique, QFAL: quantum federated adversarial learning, https://doi.org/10.48550/arXiv.2502.21171, 2025.
[44] R. Rofougaran, S. Yoo, H.-H. Tseng, S.Y.-C. Chen, Federated quantum machine learning with differential privacy, in: ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2024, pp. 9811–9815.
[45] A. Pokharel, R. Rahman, S. Shaon, T. Morris, D.C. Nguyen, Differentially private federated quantum learning via quantum noise, arXiv preprint, arXiv:2508.20310, 2025.
[46] P. Drmota, D. Nadlinger, D. Main, B. Nichol, E. Ainley, D. Leichtle, A. Mantri, E. Kashefi, R. Srinivas, G. Araneda, et al., Verifiable blind quantum computing with trapped ions and single photons, Physical Review Letters 132 (15) (2024) 150604.
[47] W. Li, S. Lu, D.-L. Deng, Quantum federated learning through blind quantum computing, Science in China. Physics, Mechanics and Astronomy 64 (10) (2021) 100312.
[48] A. Sawaika, S. Krishna, T. Tomar, D.P. Suggisetti, A. Lal, T. Shrivastav, N. Innan, M. Shafique, A privacy-preserving federated framework with hybrid quantum-enhanced learning for financial fraud detection, arXiv preprint, arXiv:2507.22908, 2025.
[49] A. Reurink, Financial fraud: a literature review, in: Contemporary Topics in Finance: A Collection of Literature Surveys, 2019, pp. 79–115.
[50] G. Sun, T. Li, Y. Ai, Q. Li, Digital finance and corporate financial fraud, International Review of Financial Analysis 87 (2023) 102566.
[51] K.G. Al-Hashedi, P. Magalingam, Financial fraud detection applying data mining techniques: a comprehensive review from 2009 to 2019, Computer Science Review 40 (2021) 100402.
[52] Y. Cheng, J. Guo, S. Long, Y. Wu, M. Sun, R. Zhang, Advanced financial fraud detection using GNN-CL model, in: 2024 International Conference on Computers, Information Processing and Advanced Education (CIPAE), IEEE, 2024, pp. 453–460.
[53] A. Ali, S. Abd Razak, S.H. Othman, T.A.E. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, A. Saif, Financial fraud detection based on machine learning: a systematic literature review, Applied Sciences 12 (19) (2022) 9637.
[54] N. Innan, A. Sawaika, A. Dhor, S. Dutta, S. Thota, H. Gokal, N. Patel, M.A.-Z. Khan, I. Theodonis, M. Bennai, Financial fraud detection using quantum graph neural networks, Quantum Machine Intelligence 6 (1) (2024) 7.
[55] E. Paquet, F. Soleymani, QuantumLeap: hybrid quantum neural network for financial predictions, Expert Systems with Applications 195 (2022) 116583.
[56] N. Innan, A. Marchisio, M. Shafique, M. Bennai, QFNN-FFD: quantum federated neural network for financial fraud detection, arXiv preprint, arXiv:2404.02595, 2024.
[57] M. Gschwendtner, N. Morgan, H. Soller, Quantum technology use cases as fuel for value in finance, McKinsey Digital (2025).
[58] S. Hochreiter, J. Schmidhuber, Long short-term memory, Neural Computation 9 (8) (1997) 1735–1780.
[59] Fraud detection bank dataset 20K records binary. Available: https://www.kaggle.com/datasets/volodymyrgavrysh/fraud-detection-bank-dataset-20k-records-binary.
[60] Synthetic Financial Datasets for Fraud Detection. Available: https://www.kaggle.com/datasets/ealaxi/paysim1.
[61] R. Ballester, J. Cerquides, L. Artiles, Quantum federated learning: a comprehensive literature review of foundations, challenges, and future directions, Quantum Machine Intelligence 7 (2) (2025) 1–29.
[62] F. Ilhan, G. Su, L. Liu, ScaleFL: resource-adaptive federated learning with heterogeneous clients, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2023, pp. 24532–24541.