Computer Science and Application 计算机科学与应用, 2026, 16(6), 51-61
Published Online June 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.166208

Hans汉斯

量子联邦学习研究综述：融合、挑战与未来展望

李宏欣[1]，姚　希[2*]，山　灵[3]，李　杰[1]

[1]洛阳师范学院通信工程学院，河南　洛阳
[2]中国人民解放军国防科技大学外国语学院，江苏　南京
[3]河南科技大学党委组织部，河南　洛阳

收稿日期：2026年5月4日；录用日期：2026年6月4日；发布日期：2026年6月11日

摘　要

量子联邦学习是量子计算与联邦学习交叉融合的前沿领域，旨在利用量子计算的并行性、纠缠等特性，解决分布式机器学习中的数据隐私、计算效率与模型性能等核心挑战。本文首先介绍了量子联邦学习产生的背景与核心定义，即多个量子客户端在保护数据隐私的前提下协作训练共享量子模型；然后从联邦架构、网络拓扑、通信方案、优化技术与安全机制五个维度系统梳理现有技术框架与分类体系；重点综述其在医疗健康、物联网与智能车联、卫星网络、元空间等关键领域的应用实践与性能优势；深入分析了当前面临的主要挑战，包括硬件限制与噪声、系统与数据的异质性、通信开销、安全与隐私威胁。最后，展望了量子错误缓解、个性化训练、鲁棒聚合算法、标准化评估基准等未来研究方向，为这一新兴领域的持续发展提供系统性参考。

关键词

量子联邦学习，量子机器学习，隐私保护，分布式学习，异质性

A Comprehensive Survey on Integration, Challenges, and Future Prospects of Quantum Federated Learning

Hongxin Li[1], Xi Yao[2*], Ling Shan[2], Jie Li[1]

[1]School of Communications Engineering, Luoyang Normal University, Luoyang Henan
[2]College of Foreign Languages, National University of Defense Technology PLA, Nanjing Jiangsu
[3]Organization Department of the Party Committees, Henan University of Science and Technology, Luoyang Henan

文章引用: 李宏欣, 姚希, 山灵, 李杰. 量子联邦学习研究综述: 融合、挑战与未来展望[J]. 计算机科学与应用, 2026, 16(6): 51-61. DOI: 10.12677/csa.2026.166208

Received: May 4, 2026; accepted: June 4, 2026; published: June 11, 2026

Abstract

Quantum Federated Learning (QFL) is an emerging interdisciplinary field that integrates quantum computing with federated learning. It aims to leverage quantum properties such as superposition and entanglement to address core challenges in distributed machine learning including data privacy, computational efficiency, and model performance. This paper first outlines the background and core definition of QFL, which enables multiple quantum clients to collaboratively train a shared quantum model while preserving data privacy. Subsequently, we systematically review existing technical frameworks and taxonomies from five dimensions: federation architecture, networking topology, communication schemes, optimization techniques, and security mechanisms. Furthermore, we focus on surveying its application practices and performance advantages in critical domains such as healthcare, Internet of Things (IoT) & intelligent vehicular networks, satellite networks, and the metaverse. This paper provides an in-depth analysis of the current major challenges, including hardware limitations and noise, system and data heterogeneity, communication overhead, and security and privacy threats. Finally, we prospect future research directions such as quantum error mitigation, personalized training, robust aggregation algorithms, and standardized evaluation benchmarks, offering a systematic reference for the continued development of this burgeoning field.

Keywords

Quantum Federated Learning, Quantum Machine Learning, Privacy Preservation, Distributed Learning, Heterogeneity

1. 引言

在当今数字时代，智能手机、物联网设备、社交媒体等技术的普及催生了前所未有规模的大数据时代[1]。这些大数据为人工智能与数据驱动的机器学习技术带来了巨大机遇。然而，集中式的机器学习面临两大难题：一是处理海量或多地分布数据时的性能瓶颈；二是数据集中化带来的固有泄露风险。为解决这些挑战，联邦学习应运而生，其核心思想是将模型训练与直接访问原始数据的需求分离，允许在分布式设备上进行计算，同时显著降低隐私和安全风险[2]。

与此同时，量子计算研究在过去几十年经历了指数级增长[3]。利用纠缠、叠加等量子特性执行计算，理论上已被证明在特定机器学习任务中具有更高效率，由此催生了量子机器学习这一学科[4]。量子机器学习通过量子神经网络、量子核方法等技术，能够在理论上实现指数级加速，特别是在处理高维数据、优化复杂函数等方面展现出独特优势。此外，基于量子算法(如量子密钥分发)可实现更安全、更高效的通信[5]。然而，当前的量子硬件(处于噪声中等规模量子时代)尚难以支撑这些理论方案的大规模实现[3]。

一个新兴的知识体系开始研究这两大研究方向的结合，从而产生了量子联邦学习这一领域[6]。QFL允许多个拥有量子计算能力(量子处理器或模拟器)的客户端协作训练一个共享的量子模型，而无需共享其私有的量子或经典数据[7]。它旨在同时利用联邦学习的隐私保护优势和量子计算的潜在计算优势。近

年来，QFL 在理论框架、算法设计、隐私增强和特定领域应用方面取得了显著进展[8]。

从技术发展脉络来看，量子联邦学习经历了三个主要发展阶段：概念提出阶段(2020~2022 年)、框架设计阶段(2022~2024 年)和应用探索阶段(2024 年至今)。在概念提出阶段，研究者主要探讨了量子计算与联邦学习结合的理论可能性；在框架设计阶段，出现了多种 QFL 系统架构和算法设计；在当前的应用探索阶段，QFL 开始向医疗健康、物联网、卫星通信等具体领域渗透，并展现出实际应用价值[9]。量子联邦学习的兴起是分布式人工智能与量子计算两大技术浪潮交汇的必然产物。它试图在严守数据隐私这一现代计算伦理底线的同时，探索利用量子力学原理突破经典计算范式的性能极限。当前研究已从早期的概念验证，逐步深入到针对具体挑战(如通信效率、数据异质性)的算法创新和面向垂直行业(如医疗、物联网)的应用落地尝试。

本文旨在对 QFL 领域进行系统性研究综述。第 2 节介绍 QFL 的基础概念、工作流程与分类体系。第 3 节详细综述关键技术进展，包括架构、优化与安全机制。第 4 节探讨 QFL 在多个领域的应用。第 5 节深入分析当前面临的核心挑战。第 6 节总结全文并展望未来研究方向。

2. 量子联邦学习基础

2.1. 核心定义与工作流程

量子联邦学习是联邦学习在量子计算领域的扩展[10]。在一个典型的 QFL 系统中，包含一个中央服务器和多个量子客户端(如 NISQ 设备或模拟器)。每个客户端持有私有数据，并具备运行参数化量子电路(即量子神经网络)的能力。QFL 的目标是联合训练一个全局共享的量子模型，其工作流程迭代进行，通常包含以下步骤[11]：

(1) 初始化与分发：服务器初始化全局量子模型参数(如量子电路的旋转角)，并将其分发给所有参与的客户端。这一步骤中，参数初始化策略对后续训练收敛性有重要影响。

(2) 本地量子训练：每个客户端使用其本地私有数据，在本地量子设备上执行训练，更新其本地模型参数。这通常涉及计算损失函数关于量子参数的梯度(如使用参数偏移规则)，并应用经典或量子优化算法(如量子梯度下降)。本地训练过程中，客户端需要处理量子噪声、退相干等实际问题。

(3) 模型参数上传：客户端将更新后的本地模型参数(而非原始数据)上传至中央服务器。这一步骤中，参数压缩、量化等技术可用于减少通信开销。

(4) 量子联邦聚合：服务器使用聚合算法(如量子联邦平均)将所有客户端的本地更新聚合，形成新的全局模型参数。聚合算法的设计需要考虑客户端数据的异质性、更新质量差异等因素。

(5) 迭代：服务器将更新后的全局参数分发回客户端，重复步骤 2~4，直到模型收敛或达到预定轮次。

QFL 的工作流程继承了经典联邦学习的核心范式——“数据不动，模型动”，但其技术内涵发生了质变。本地训练从经典优化问题转变为在噪声量子设备上执行参数化量子电路的优化过程；模型参数从经典向量扩展为描述量子电路的参数集；聚合过程也可能涉及量子态或量子信息的处理。这一转变带来了新的机遇(如潜在的计算加速)和挑战(如量子噪声的影响)。

2.2. 分类体系

根据量子计算与经典计算在系统中的角色、网络组织方式及通信媒介，QFL 可被多维度分类[12]：

(1) 联邦架构

a) 完全 QFL：客户端和服务器均使用量子模型(如 QNN)进行计算和聚合[6]。这种架构理论上能最大化量子优势，但对硬件要求最高，目前主要处于理论研究阶段。

b) 混合 QFL：客户端使用量子–经典混合模型(例如，经典神经网络嵌入变分量子电路)，服务器进

行经典聚合[13]。这是当前 NISQ 时代更主流的实用架构，能够在现有硬件条件下实现量子增强。

(2) 网络拓扑

a) 集中式：星型拓扑，一个中央服务器协调所有客户端[2]。这是最经典的联邦学习拓扑，结构简单但存在单点故障风险。

b) 分层式：引入边缘服务器等中间层，减轻中心压力。适用于大规模分布式系统。

c) 对等式/链式：无中心服务器，客户端以链式或对等网络直接交换模型，增强鲁棒性[14]。

(3) 通信方案

a) 经典通信：传输经典的模型参数(数字)。这是当前最实用的方案，技术成熟度高。

b) 量子通信：通过量子信道传输量子态(如量子模型的状态)，通常结合量子隐形传态，安全性更高但技术挑战大[15]。

(4) 数据模态

a) 单模态 QFL：所有客户端处理同类型数据。

b) 多模态 QFL：客户端处理不同类型数据(如图像、音频)，需设计融合机制[16]。

QFL 的分类体系反映了其作为交叉领域的复杂性和多样性。架构选择体现了在理论理想与现实约束间的权衡；拓扑结构决定了系统的可扩展性和韧性；通信方案则直接关联到系统的安全性和实用性。当前研究呈现出从集中式、经典通信的混合架构，向更分布式、安全通信的完全量子架构演进的趋势，这一演进路径与量子硬件和通信技术的发展紧密相关。

2.3. 量子联邦学习的潜在优势与挑战剖析

量子联邦学习的核心吸引力在于其理论上能同时融合联邦学习的隐私保护架构与量子计算的性能潜力。然而，这些优势在不同层面上的显现程度和实现路径存在显著差异，且与当前 NISQ 时代的严峻挑战紧密交织。

(1) 本地计算优势：理论加速潜力与噪声约束

- **理论基础**：量子计算的核心特性，如叠加与纠缠，使其在求解特定问题上具有理论上的指数级加速潜力[1.引言]。在 QFL 中，这意味着客户端在本地训练量子神经网络处理优化问题(如组合优化、量子化学模拟)时，可能比经典算法更高效。
- **现实挑战**：这一优势的发挥严重受制于 5.1 节所述硬件限制。当前 NISQ 设备有限的比特数、短暂的相干时间和高噪声，使得实现深度、容错的量子计算极为困难。著名的“贫瘠高原”问题会使得 QNN 训练变得停滞不前。因此，在通用机器学习任务上，QFL 的本地计算优势更多是一种长期理论前景，而非短期可实现的特征。

(2) 模型表达优势：高维表示能力与架构探索

- **理论基础**：量子态存在于高维希尔伯特空间，因此，参数化量子电路(即 QNN)可能具有比经典神经网络更强的函数近似和表征复杂数据分布的能力。这在处理高维、结构复杂的数据(如医疗影像、分子结构、金融时序)时可能带来潜在的性能提升。
- **现实挑战**：这种表达优势的实现，依赖于精心设计的量子电路架构(Ansatz)。在噪声影响下，如何设计既强大又易于训练的 QNN，本身就是一个前沿研究课题。目前，在 4.1 节医疗健康和 4.4 节异常检测等应用中的初步探索，正是对这种优势的实证性检验，但结论尚不具普适性。

(3) 通信与安全优势：基于物理定律的增强

- **理论基础**：这是 QFL 区别于经典 FL 最具特色的优势，主要体现在两个方面：

1. 安全聚合新范式：利用量子同态加密等原语，有望实现更高效或更安全的安全聚合协议。

2. 面向未来的信道安全：利用量子密钥分发可实现信息论安全的密钥分发，其安全性基于量子力学原理，能抵御未来量子计算机的攻击，为联邦学习通信链路提供“前瞻性”的安全保障。

- **现实挑战**：如 5.2 节所指，量子通信(无论是用于 QKD 还是传输量子态)目前面临保真度、距离和成本的重大挑战。基于量子通信的协议(如盲量子计算)短期内难以实用。因此，当前阶段更可行的路径是基于经典通信的混合安全框架，同时为未来量子互联网成熟后的应用进行理论储备。

综上所述，QFL 的“量子优势”是一个多层次、有条件、且大部分仍处于演进中的图景。在 NISQ 时代，其首要价值并非立即实现全面的性能碾压，而在于开启了一个全新的设计空间：探索基于量子特性的新优化算法(如自然梯度)、利用量子电路探索新的模型表达、以及基于量子物理原理构建更坚固的安全基石。认清这些优势与挑战的共生关系，对于引导该领域朝着务实且创新的方向发展至关重要。

3. 量子联邦学习关键技术进展

3.1. 通信与优化效率提升

通信开销是 FL 的核心瓶颈，QFL 通过算法和架构创新进行优化[17]。在经典联邦学习中，通信成本通常占总成本的 60%~80%，而在 QFL 中，由于量子参数的特殊性和量子通信的高成本，这一问题更加突出。

(1) 高效优化算法：联邦量子自然梯度下降算法利用量子 Fisher 信息矩阵，相比经典 SGD 方法能以更少的训练轮次和通信轮次实现收敛，显著降低总通信开销[18]。量子自然梯度考虑了量子态空间的黎曼几何结构，能够更有效地更新参数，特别是在存在量子噪声的环境中表现优异。

(2) 动态与可瘦身模型：为适应不稳定通信环境(如无人机、卫星网络)，提出了动态量子联邦学习和可瘦身量子联邦学习框架[19] [20]。它们采用可动态调整电路深度或参数规模的量子神经网络，在信道条件差时使用“瘦身”模式传输更少参数，实现通信效率与模型性能的权衡。

(3) 聚合算法创新：针对非独立同分布数据，提出了 Q 加权联邦平均等算法，根据客户端本地训练损失动态调整其在聚合中的权重，提升了模型在数据异质场景下的性能[21]。

上述三类代表性算法特点对比如表 1 所示。

Table 1. Comparison of representative optimization algorithms for quantum federated learning
表 1. 量子联邦学习代表性优化算法比较

框架 / 算法	核心思想	降低通信开销机制	对数据异质性鲁棒性
联邦量子自然梯度下降	利用量子 Fisher 信息矩阵，在量子态黎曼几何空间进行更高效的优化	减少模型收敛所需的总通信轮次	一般，需与加权聚合等方法结合
Q 加权联邦平均	根据客户端本地训练损失动态调整其在全局聚合中的权重	通过提升聚合质量，间接减少达到目标性能所需的轮次	强，可缓解非独立同分布数据带来的客户端漂移
动态/可瘦身 QFL 框架	使用深度或宽度可动态调整的量子神经网络	在信道条件差时，传输“瘦身”后更少的模型参数	一般，模型容量变化可能影响对不同分布的拟合能力
经典联邦平均	对客户端模型更新进行直接平均	无专门优化机制	弱，在非独立同分布数据下性能下降显著

表 1 对比了几种代表性的 QFL 优化算法。尽管这些方法从不同角度(如更优的收敛轨迹、自适应的模型复杂度、智能的聚合权重)提升了效率，但其在 NISQ 时代的实际效能仍面临根本性制约。首先，硬件噪声是共同挑战：自然梯度的计算精度、可瘦身 QNN 的性能底线均受量子噪声影响；“贫瘠高原”问

题可能使任何优化算法的收敛变得困难。其次，评估尚不全面：现有研究多在仿真或同构噪声假设下验证，缺乏在真实、异构的量子硬件集群上的系统性评估。未来研究需致力于跨层协同设计，将算法创新与底层错误缓解技术紧密结合，并建立涵盖异构硬件和数据的标准化评估基准。

提升通信与优化效率是 QFL 走向实用的关键。现有研究主要从三个层面入手：一是设计更符合量子优化问题几何特性的算法(如自然梯度)，从根本上减少迭代次数；二是设计自适应模型，根据环境动态调整复杂度，这是一种“以退为进”的实用主义策略；三是改进聚合规则，使全局更新更能代表有价值的本地信息。这些方法在一定程度上缓解了通信压力，但如何将它们有机结合，并推广到更复杂的量子模型和网络环境中，仍是待解难题。

3.2. 隐私与安全增强机制

QFL 通过结合量子物理特性和密码学原语，提供更强大的隐私安全保障[22]。

(1) 盲量子计算协议：客户端可以将加密(或“盲化”)的量子数据发送给强大的量子服务器进行训练，服务器执行计算但无法得知输入数据、算法细节及最终结果，为实现完全量子化的隐私保护联邦学习提供了理论基础[23]。

(2) 量子差分隐私：在模型更新中加入量子噪声(满足特定差分隐私定义)，以形式化保证抵御成员推理等隐私攻击的能力，即使攻击者拥有量子计算能力[24]。

(3) 量子同态加密与安全聚合：结合量子同态加密，允许服务器对加密的模型更新直接执行聚合操作[25]。

(4) 量子密钥分发：用于加密客户端与服务器之间的经典通信信道，提供信息论安全性的密钥分发，抵御未来的量子计算攻击[15]。

四类安全机制特性对比分析如表 2 所示。

Table 2. Comparison of security and privacy enhancement techniques for quantum federated learning
表 2. 量子联邦学习安全与隐私增强技术比较

机制 \ 特性	隐私保证	通信需求	计算开销	技术成熟度	现实可行性
盲量子计算	信息论安全的计算过程保密性	需双向量子通信	极高(需通用量子计算服务器)	理论研究阶段	极低，理论框架
量子差分隐私	形式化、可证明的隐私保证	经典通信	低至中(取决于噪声注入机制)	算法设计阶段	较高，是 NISQ 时代较可行方案
量子同态加密	允许服务器对加密后的模型更新直接执行聚合操作，实现密文计算	经典通信	高(同态加密与解密操作)	早期探索阶段	中等，面临计算开销与实用性的权衡
量子密钥分发	为经典通信信道提供信息论安全的密钥分发	需量子信道分发密钥，后续用经典信道传输加密数据	低(密钥生成后，对称加密开销低)	相对成熟	高，是构建“量子安全联邦学习”信道的基础

表 2 系统比较了 QFL 中主要的安全隐私技术。当前研究呈现出“混合安全”与“分层防御”的趋势(3.2 节)，即结合多种技术应对不同威胁。例如，可使用 QKD 保护信道，用量子差分隐私保护模型更新，再探索同态加密实现安全聚合。然而，全面评估仍然缺失：大多数方案仅针对特定攻击(如模型逆向、窃听)，缺乏在统一威胁模型下的综合测评(5.4 节)。此外，量子模型本身的安全特性(如是否比经典模型更易受对抗样本攻击)仍是开放问题。未来的安全框架需是端到端、可证明安全的，并能明确量化在 NISQ

硬件噪声下，各种密码学原语的实际安全边界。

QFL 在安全隐私方面展现出“双重优势”：一方面，它继承了联邦学习“数据不出域”的天然隐私保护特性；另一方面，它能够引入量子密码学原语，提供经典方法难以企及的信息论安全性。当前的研究热点在于如何将这些量子安全技术(如盲量子计算、QKD)与联邦学习流程高效、低成本地结合。一个值得注意的趋势是“混合安全”，即同时使用经典密码学(如同态加密)和量子技术来构建纵深防御体系，以应对不同层面的威胁。

3.3. 应对系统与数据异质性

现实场景中，客户端在数据分布、硬件能力、噪声水平上存在差异，是 QFL 实用化的关键挑战[26]。

(1) 个性化 QFL：不追求单一的全局最优模型，而是允许每个客户端在全局协作的基础上，发展适合自身数据特性和硬件条件的个性化模型[27]。

(2) 异质性感知的聚合与分组：通过聚类分析方法，将具有相似数据分布或硬件特性的客户端分组，在组内进行聚合，避免异质客户端间的负迁移[28]。

(3) 稳健聚合算法：设计能够容忍客户端间更新差异的聚合规则，例如，基于余弦相似性筛选更新，或采用量子协调平均等旨在寻找帕累托最优解的算法[29]。

异质性是分布式系统的固有属性，在 QFL 中因量子硬件的多样性而被进一步放大。应对策略从早期的“一视同仁”式平均聚合，发展为更加精细化的“分而治之”和“因材施教”。个性化 QFL 承认并利用差异，旨在为每个参与者找到其独特的最优点；分组聚合则试图在差异中寻找共性，在相似的子群体内进行有效协作。未来的挑战在于如何自动、动态地识别这些异质性模式，并设计出能同时适应数据分布和硬件噪声差异的通用算法框架。

4. 应用领域与实证研究

4.1. 医疗健康

医疗数据高度敏感且分散。QFL 为协同训练诊断模型提供了理想方案[30]。

(1) 数字孪生辅助诊断：数字孪生辅助的 QFL 算法利用 5G 网络为患者创建数字孪生，在其上进行 VQNN 训练，既保护真实数据隐私，又通过数字空间加速探索，实现了与数据集中化训练相当的准确性[21]。

(2) 心理健康监测：在心理健康监测、基因组学分析等领域，基于 VQC 的 QFL 框架也展示了在保护隐私前提下的有效分类能力[21] [31]。

(3) 隐私保护框架：隐私保护混合联邦学习框架结合聚类和量子方法，为心理健康应用提供了解决方案[32]。

医疗健康是 QFL 最具前景的应用领域之一，这源于其对隐私保护的极端要求与跨机构数据协作的迫切需求。现有应用探索表明，QFL 不仅能够满足合规要求，还能通过量子处理潜在提升对高维、复杂医疗数据(如医学影像、基因组序列)的特征提取能力。然而，将实验室成果转化为临床实践，仍需解决模型可解释性、临床验证、以及与现有医院信息系统的集成等实际问题。

4.2. 物联网与智能车联

物联网设备产生海量数据但计算能力有限。QFL 使得边缘设备能够协同学习而不暴露数据[33]。

(1) 智能车联网：在车联网和车辆元空间中，量子增强的联邦学习框架被用于轨迹预测、异常检测等任务，通过量子强化学习进行动态模式切换以降低通信成本，并利用量子启发的 PCA 提升内存效率，表

现出优于经典方法的性能[34] [35]。

(2) 雷达目标跟踪：基于雷达的物联网目标跟踪系统，采用混合角度－幅度编码和 VQC 的量子辅助联邦学习方案，在低信噪比下仍保持高精度[32]。

(3) 从 FL 到 QFL 的过渡：有综述系统探讨了物联网中从联邦学习向量子联邦学习的过渡路径与挑战[26]。

物联网环境中的 QFL 研究侧重于应对资源约束和动态性。通过引入量子计算，研究试图在边缘侧实现更高效的数据压缩、特征提取和实时决策。智能车联是其中的典型场景，对低延迟和高可靠性的要求推动了动态 QFL、上下文感知分组等技术的发展。当前应用仍以仿真和特定硬件平台上的原型验证为主，大规模部署需要量子传感、低功耗量子处理器等底层技术的同步突破。

4.3. 卫星通信与无人机网络

低地球轨道卫星可实现全球覆盖。动态 QFL 用于星地集成系统，利用可瘦身 QNN 和叠加编码技术，适应卫星链路时延大、带宽变化的特点，在遥感图像处理等任务中实现了通信与计算效率的提升[20]。在无人机自主侦察中，基于 DQNN 的动态量子联邦学习框架，通过动态控制电路层深度，有效应对了无线信道不稳定和计算资源限制的挑战[19]。

空天场景将 QFL 的挑战推向极致：长延时、间歇连接、高动态拓扑。该领域的研究极具前瞻性，旨在为未来空天一体化智能网络奠定基础。核心技术思路是“弹性”，即让 QFL 系统能够根据可用的通信带宽和计算资源，弹性地调整其模型复杂度和协作策略。这类研究不仅对卫星、无人机网络有意义，其方法论也对地面移动边缘计算具有借鉴价值。

4.4. 网络安全与异常检测

QFL 可用于构建分布式、隐私保护的威胁检测系统。

(1) 个性化异常检测：个性化 QFL 异常检测框架通过为每个量子客户端定制模型，显著提升了在非 IID 和异构硬件条件下的异常检测性能[27]。

(2) 入侵检测模型：将量子神经网络与联邦学习结合的入侵检测模型，展示了其增强对低频攻击特征提取的能力[33]。

在网络安全领域应用 QFL 具有双重意义：一方面，其分布式和隐私保护特性非常适合构建协同防御体系；另一方面，量子模型可能具备探测新型、复杂攻击模式(如基于量子计算的攻击)的潜力。现有工作初步验证了 QFL 在异常检测任务上的有效性，但面对高级持续性威胁等复杂攻击，如何设计更具判别力的量子特征映射和更鲁棒的联邦训练机制，是未来研究的重点。

5. 核心挑战与开放问题

尽管前景广阔，QFL 走向大规模实用化仍面临严峻挑战。

5.1. NISQ 硬件限制

当前量子设备比特数有限、相干时间短、噪声水平高，严重限制了可训练模型的复杂度[3]。量子噪声会导致训练过程不稳定、梯度消失(贫瘠高原)等问题。开发适用于 QFL 的量子错误缓解技术至关重要。

5.2. 通信的实用化困境

虽然量子通信能提供超安全传输，但其目前保真度低、损耗大、成本高昂[15]。在 QFL 中大规模传输量子态不现实。因此，如何设计基于经典通信的高效安全协议，或为未来量子互联网做准备，是重要

的研究课题。

5.3. 异质性的系统化处理

现有工作多关注数据异质性，对系统异质性(如不同厂商的量子处理器、不同的噪声模型、不同的量子比特拓扑结构)的鲁棒性研究尚处于起步阶段[26]。需要开发能自动感知并适应这种跨平台异质性的算法。

5.4. 安全与隐私的全面评估

现有 QFL 安全方案多集中于防御特定攻击。需要建立更全面的威胁模型，并形式化分析组合多种隐私技术后的整体安全边界。量子模型本身是否比经典模型更易受对抗样本或后门攻击，也是一个待探索的问题。

5.5. 缺乏标准化评估框架

社区缺少统一的仿真平台、基准数据集和评估指标来公平比较不同 QFL 算法[34]。开发集成可视化模拟器是积极的一步，但需要更广泛的基准测试，涵盖收敛性、通信成本、隐私–效用权衡、跨平台泛化性等多个维度。

QFL 的挑战是多层次、交织在一起的。硬件限制是根本性约束，通信和异质性是分布式系统固有的工程难题，安全隐私是应用落地的生命线，而评估框架的缺失则阻碍了领域的健康发展。这些挑战并非孤立，例如，硬件噪声会影响模型更新的质量，进而影响安全聚合协议的有效性；通信限制又会迫使采用更简单的模型，从而与处理复杂数据的需求产生矛盾。因此，未来的突破很可能依赖于跨层的协同设计，而非单点技术的优化。

6. 结论与未来展望

量子联邦学习作为一个充满活力的交叉学科前沿，为解决分布式智能中的隐私、效率与算力瓶颈提供了革命性的思路。本文系统回顾了 QFL 的基础原理、技术进展、多元应用及核心挑战。当前研究已从概念验证走向针对特定挑战(如异质性、通信效率)的深度算法设计和在医疗、物联网等领域的初步应用探索。

展望未来，QFL 的研究将向更深层次和更广范围拓展：

(1) 算法层面：开发更高效的量子联邦优化器、能从根本上缓解噪声影响的抗噪声训练算法，以及适用于复杂数据关系的量子图神经网络联邦学习。

(2) 系统层面：构建量子–经典混合的联邦学习操作系统，实现量子计算资源与经典边缘/云资源的无缝调度与管理。

(3) 安全与隐私层面：深入研究后量子密码学与 QFL 的结合，探索量子零知识证明在联邦学习验证中的应用，构建端到端的可证明安全 QFL 框架。

(4) 跨领域融合：与数字孪生、区块链、6G 通信等技术深度融合，打造新一代可信、高效、智能的分布式计算范式[21] [26]。

总之，量子联邦学习正处于从理论走向实践的关键阶段。跨越硬件、算法和系统的多重挑战需要量子计算、机器学习、网络安全、分布式系统等多领域学者的紧密协作。随着量子硬件的进步和算法的不断创新，QFL 有望在严守数据隐私红线的前提下，真正释放分布式量子智能的巨大潜能，赋能千行百业的智能化转型。

基金项目

国家社科基金项目(No. 23BYY200)：基于多层次特征融合的日语作文自动评分方法研究。

参考文献

[1] Oussous, A., Benjelloun, F., Ait Lahcen, A. and Belfkih, S. (2018) Big Data Technologies: A Survey. *Journal of King Saud University-Computer and Information Sciences*, **30**, 431-448. https://doi.org/10.1016/j.jksuci.2017.06.001

[2] Yang, Q., Liu, Y., Chen, T. and Tong, Y. (2019) Federated Machine Learning. *ACM Transactions on Intelligent Systems and Technology*, **10**, 1-19. https://doi.org/10.1145/3298981

[3] Preskill, J. (2018) Quantum Computing in the NISQ Era and Beyond. *Quantum*, **2**, Article 79. https://doi.org/10.22331/q-2018-08-06-79

[4] Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N. and Lloyd, S. (2017) Quantum Machine Learning. *Nature*, **549**, 195-202. https://doi.org/10.1038/nature23474

[5] Bennett, C.H. and Brassard, G. (2014) Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theoretical Computer Science*, **560**, 7-11. https://doi.org/10.1016/j.tcs.2014.05.025

[6] Ballester, R., Cerquides, J. and Artiles, L. (2025) Quantum Federated Learning: A Comprehensive Literature Review of Foundations, Challenges, and Future Directions. *Quantum Machine Intelligence*, **7**, Article No. 73. https://doi.org/10.1007/s42484-025-00292-2

[7] Ren, C., Yan, R., Zhu, H., Yu, H., Xu, M., Shen, Y., *et al*. (2025) Toward Quantum Federated Learning. *IEEE Transactions on Neural Networks and Learning Systems*, **36**, 15580-15600. https://doi.org/10.1109/tnnls.2025.3552643

[8] Uddin, M.R., Shaon, S., Rahman, R., Nguyen, D.C., Dobre, O.A. and Niyato, D. (2026) Quantum Federated Learning: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, **28**, 3942-3975. https://doi.org/10.1109/comst.2025.3644750

[9] Qayyum, T., Khan, M.W.H., Tariq, A., Serhani, M.A., Sallabi, F.M., Trabelsi, Z., *et al*. (2024) Quantum Federated Learning: Bridging Quantum Computing and Distributed AI. 2024 *IEEE*/*ACM* 17*th International Conference on Utility and Cloud Computing* (*UCC*), Sharjah, 16-19 December 2024, 327-335. https://doi.org/10.1109/ucc63386.2024.00053

[10] Gurung, D. and Pokhrel, S.R. (2025) Chained Continuous Quantum Federated Learning Framework. *Future Generation Computer Systems*, **169**, Article 107800. https://doi.org/10.1016/j.future.2025.107800

[11] Innan, N., Khan, M.A., Marchisio, A., Shafique, M. and Bennai, M. (2024) FedQNN: Federated Learning Using Quantum Neural Networks. 2024 *International Joint Conference on Neural Networks* (*IJCNN*), Yokohama, 30 June 2024-5 July 2024, 1-9. https://doi.org/10.1109/ijcnn60899.2024.10651123

[12] Hisamori, K., Chiang, Y., Lin, H. and Ji, Y. (2024) Hybrid Quantum-Classical Computing in Federated Learning with Data Heterogeneity. 2024 *IEEE* 35*th International Symposium on Personal*, *Indoor and Mobile Radio Communications* (*PIMRC*), Valencia, 2-5 September 2024, 1-6. https://doi.org/10.1109/pimrc59610.2024.10817181

[13] Chehimi, M. and Saad, W. (2023) Quantum Federated Learning with Quantum Data. *Proceedings of IEEE Global Communications Conference* (*GLOBECOM*) *Workshops*, Singapore, 23-27 May 2022, 1-6.

[14] Qu, Z., Li, Y., Liu, B., Gupta, D. and Tiwari, P. (2026) DTQFL: A Digital Twin-Assisted Quantum Federated Learning Algorithm for Intelligent Diagnosis in 5G Mobile Network. *IEEE Journal of Biomedical and Health Informatics*, **30**, 17-26. https://doi.org/10.1109/jbhi.2023.3303401

[15] Qi, J., Zhang, X. and Tejedor, J. (2023) Optimizing Quantum Federated Learning Based on Federated Quantum Natural Gradient Descent. *ICASSP* 2023-2023 *IEEE International Conference on Acoustics*, *Speech and Signal Processing* (*ICASSP*), Rhodes Island, 4-10 June 2023, 1-5. https://doi.org/10.1109/icassp49357.2023.10094634

[16] Kannan, E., Ravikumar, S., Carmel Mary Belinda, M.J., Vijay, K., *et al*. (2024) Revolutionizing Machine Learning Security: The Role of Quantum-Enhanced Federated Learning. 2024 *International Conference on Emerging Research in Computational Science* (*ICERCS*), Coimbatore, 12-14 December 2024, 1-6. https://doi.org/10.1109/icercs63125.2024.10895237

[17] Park, S., Son, S.B., Jung, S. and Kim, J. (2025) Dynamic Quantum Federated Learning for UAV-Based Autonomous Surveillance. *IEEE Transactions on Vehicular Technology*, **74**, 8158-8170. https://doi.org/10.1109/tvt.2025.3526809

[18] Jiang, J., Luo, M. and Ma, S. (2024) Quantum Network Capacity of Entangled Quantum Internet. *IEEE Journal on Selected Areas in Communications*, **42**, 1900-1918. https://doi.org/10.1109/jsac.2024.3380091

[19] Pokharel, A., Rahman, R., Morris, T. and Nguyen, D.C. (2025) Quantum Federated Learning for Multimodal Data: A Modality-Agnostic Approach. 2025 *IEEE*/*CVF Conference on Computer Vision and Pattern Recognition Workshops* (*CVPRW*), Nashville, 11-12 June 2025, 545-554. https://doi.org/10.1109/cvprw67362.2025.00059

[20] Park, S., Jung, S. and Kim, J. (2024) Dynamic Quantum Federated Learning for Satellite-Ground Integrated Systems Using Slimmable Quantum Neural Networks. *IEEE Access*, **12**, 58239-58247. https://doi.org/10.1109/access.2024.3392429

[21] Li, W., Lu, S. and Deng, D. (2021) Quantum Federated Learning through Blind Quantum Computing. *Science China Physics*, *Mechanics & Astronomy*, **64**, Article No. 100312. https://doi.org/10.1007/s11433-021-1753-3

[22] Ullah, S., Ravi, G.B., Shareef, D.K., *et al*. (2023) Quantum Enhanced Federated Learning with Differential Privacy. *Proceedings of IEEE International Conference on Privacy*, *Security and Trust* (*PST*), Copenhagen, 21-23 August 2023, 1-6.

[23] Ganesh Babu, R., Geetha, T.S., Nedumaran, A., *et al*. (2026) Integrating Quantum Computing with Federated Learning for Enhanced Security and Privacy in IoT Networks. *Results in Engineering*, **29**, Article 108500. https://doi.org/10.1016/j.rineng.2025.108500

[24] Shareef, D.K., Hazarika, B., Qiao, C., *et al*. (2025) Integrating Federated Learning in Quantum Computing for Secure and Scalable Model Training. *Proceedings of International Conference on Intelligent Methods*, *Instrumentation and Applications* (*ICIMIA*), Tirupur, 3-5 September 2025, 920-925.

[25] Hazarika, B., Singh, K., Dobre, O.A., Li, C. and Duong, T.Q. (2025) Quantum-Enhanced Federated Learning for Metaverse-Empowered Vehicular Networks. *IEEE Transactions on Communications*, **73**, 4168-4183. https://doi.org/10.1109/tcomm.2024.3502667

[26] Qiao, C., Li, M., Liu, Y. and Tian, Z. (2025) Transitioning from Federated Learning to Quantum Federated Learning in Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, **27**, 509-545. https://doi.org/10.1109/comst.2024.3399612

[27] Nguyen, D.H., Nguyen, M.D. and Hwang, W. (2025) Personalized Quantum Federated Learning: Performance Analysis. 2025 *Fifteenth International Conference on Mobile Computing and Ubiquitous Networking* (*ICMU*), Busan, 10-12 September 2025, 1-2. https://doi.org/10.23919/icmu65253.2025.11219146

[28] Rahman, R., Shaham, S. and Nguyen, D.C. (2026) Toward Personalized Quantum Federated Learning for Anomaly Detection. *IEEE Transactions on Network Science and Engineering*, **13**, 3335-3350. https://doi.org/10.1109/tnse.2025.3631526

[29] Rahman, R., Nguyen, D.C., Thomas, C.K. and Saad, W. (2025) Toward Heterogeneous Quantum Federated Learning: Challenges and Solutions. *IEEE Network*, 1-9. https://doi.org/10.1109/mnet.2025.3638798

[30] Gupta, A., Kumar Maurya, M., Dhere, K. and Kumar Chaurasiya, V. (2024) Privacy-Preserving Hybrid Federated Learning Framework for Mental Healthcare Applications: Clustered and Quantum Approaches. *IEEE Access*, **12**, 145054-145068. https://doi.org/10.1109/access.2024.3464240

[31] Khan, K. and Khan, K. (2025) DT-QFL: Dual-Timeline Quantum Federated Learning with Time-Symmetric Updates, Temporal Memory Kernels, and Reversed Gradient Dynamics. *IEEE Transactions on Quantum Engineering*, **6**, 1-21. https://doi.org/10.1109/tqe.2025.3607689

[32] Jabbar, A., Jianjun, H., Jabbar, M.K., ur Rehman, K. and Mahmood, T. (2025) Quantum-Assisted Federated Learning for Radar-Based Object Tracking in IoT-Enabled Environments. *EPJ Quantum Technology*, **12**, Article No. 141. https://doi.org/10.1140/epjqt/s40507-025-00440-4

[33] 李冬芬, 向秋雨, 胡志康, 等. 融合联邦学习与量子卷积神经网络的入侵检测模型[J]. 计算机研究与发展, 2025, 62(10): 2512-2522.

[34] Rahman, R., Pokharel, A., Uddin, M.R. and Nguyen, D.C. (2025) SimQFL: A Quantum Federated Learning Simulator with Real-Time Visualization. 2025 *IEEE International Conference on Quantum Computing and Engineering* (*QCE*), Albuquerque, 30 August 2025-5 September 2025, 520-529. https://doi.org/10.1109/qce65121.2025.00064

[35] Hazarika, B., Singh, K., Duong, T.Q. and Dobre, O.A. (2024) Quantum-Driven Context-Aware Federated Learning in Heterogeneous Vehicular Metaverse Ecosystem. *Proceedings of the* 59*th IEEE International Conference on Communications* (*ICC* 2024), Denver, 9-13 June 2024, 1533-1538. https://doi.org/10.1109/ICC51166.2024.10623010