https://crad.ict.ac.cn
62(10): 2512−2522, 2025

融合联邦学习与量子卷积神经网络的入侵检测模型

李冬芬　向秋雨　胡志康　袁宇航　孙雨晨　徐　菡　宋征宇　韩浩民　白冬雪　多　滨　周　让
（成都理工大学计算机与网络安全学院（示范性软件学院）　成都　610051）
（lidongfen17@cdut.edu.cn）

An Intrusion Detection Model Integrating Federated Learning and Quantum Convolutional Neural Networks

Li Dongfen, Xiang Qiuyu, Hu Zhikang, Yuan Yuhang, Sun Yuchen, Xu Han, Song Zhengyu, Han Haomin, Bai Dongxue, Duo Bin, and Zhou Rang
（*College of Computer and Network Security*, *Chengdu University of Technology* (*Pilot Software College*), *Chengdu* 610051）

Abstract　Intrusion detection system (IDS) is a pivotal component in ensuring the security of network environments. However, conventional deep learning methodologies are characterised by elevated false alarm rates when confronted with infrequent attack features and challenges related to data imbalance. Additionally, these methodologies possess a limited capacity to effectively model high-dimensional sparse features. The ubiquity of the Internet of things (IoT) and edge devices has led to the emergence of intrusion detection data that exhibits distributed and heterogeneous trends. The centralised training of this data is hindered by privacy protection requirements, necessitating alternative approaches for data analysis and interpretation. In this regard, we put forward a federated classical hybrid quantum convolutional intrusion detection system (FedCQIDS), which involves the incorporation of a lightweight quantum convolutional neural network within the client-side local model. The convolutional layer is incorporated into the client-local model with the objective of enhancing resource utilisation through quantum bit multiplexing, augmenting the capacity to express low-frequency sparse attack features, and facilitating multi-client collaborative modelling and privacy protection by means of federated learning architecture. A series of related experiments are conducted on two distinct datasets, NSL-KDD and UNSW-NB15, and the findings indicate that FedCQIDS exhibits superior performance compared with conventional federated models with regard to accuracy and loss value. This is particularly evident in scenarios involving the identification of a limited number of classes of attacks, thereby underscoring its potential for application in the domain of privacy protection and efficient deployment.

Key words　intrusion detection; quantum computing; federated learning; deep learning; quantum federated learning

摘　要　入侵检测系统（intrusion detection system, IDS）是保障网络环境安全的重要手段，但传统深度学习方法在应对非频繁攻击特征与数据不平衡问题时存在高误报率，且对高维稀疏特征建模能力有限. 随着物联网与边缘设备的普及，入侵检测数据呈现出分布式与异构化趋势，且因隐私保护要求，原始数据难以集中训练. 为此，提出了一种融合联邦学习与量子卷积神经网络的入侵检测模型 FedCQIDS（federated

收稿日期：2025-06-06；**修回日期**：2025-07-13
基金项目：国家自然科学基金项目（62172060）；国家重点研发计划项目（2022YFB3304303）；四川省科技计划项目（2023YFG0374, 24JBGS0007）；成都市经济与信息化局项目（AZ2024-0216）；成都市科学技术局项目（2024ZHCG0064）
This work was supported by the National Natural Science Foundation of China (62172060), the National Key Research and Development Program of China (2022YFB3304303), the Project of Sichuan Provincial Science and Technology Plan (2023YFG0374, 24JBGS0007), the Project of Chengdu Municipal Bureau of Economy and Information Technology (AZ2024-0216), and the Chengdu Science and Technology Bureau Project (2024ZHCG0064).
通信作者：向秋雨（1033809675@qq.com）

classical hybrid quantum convolutional intrusion detection system)，在客户端本地模型中引入轻量化的量子卷积层，通过量子比特复用技术提升资源利用率，增强对低频稀疏攻击特征的表达能力，并借助联邦学习架构实现多客户端间的协同建模与隐私保护. 在 NSL-KDD 与 UNSW-NB15 两个数据集上开展了相关的实验，结果表明 FedCQIDS 在准确率与损失值方面均优于传统联邦模型，特别是在少数类攻击识别任务中表现出更高的检测性能与训练稳定性，展示了其在隐私保护与高效部署下的应用潜力.

关键词 入侵检测；量子计算；联邦学习；深度学习；量子联邦学习

中图法分类号 TP393.08；TP18；TP387

DOI: 10.7544/issn1000-1239.202550413 **CSTR:** 32373.14.issn1000-1239.202550413

随着数字化转型的推进，网络安全问题日益凸显，成为保障社会基础设施、金融系统和个人隐私的关键因素. 入侵检测系统(intrusion detection system, IDS)作为网络安全防御体系的重要组成部分，主要通过分析网络流量、用户行为和系统日志等信息，识别潜在的恶意攻击行为，其检测性能高度依赖于对复杂网络行为的有效建模能力[1]. 尤其是在物联网环境下，分布式设备如智能摄像头、传感器和边缘节点产生大量异构日志数据，这些数据难以集中处理且高度敏感，进一步突出了入侵检测中的隐私保护与建模难度. 目前主流的研究方法基于集中式深度学习架构，将多源数据集中至云端服务器进行模型训练，通过卷积神经网络(CNN)、长短期记忆网络(LSTM)等深层结构实现自动化特征提取和攻击分类. 然而，这类方法在实际部署中面临 2 方面挑战.

一方面，集中训练依赖于将来自不同机构或设备的多源敏感数据(如医疗记录、金融日志)集中到云端建模，存在严重的隐私泄露风险[2-4]. 另一方面，随着攻击方式日益隐蔽化，如 APT 攻击和零日漏洞等往往呈现低频率、高稀疏性与微弱异常信号等特征，传统深度模型在高维稀疏空间中的特征提取能力有限，容易出现过拟合或忽略关键信号，导致误报或漏报. 虽然已有研究尝试分别引入联邦学习与量子计算以应对上述问题，但仍存在显著局限. 联邦学习通过分布式训练保护数据隐私[5-6]，但其底层模型多采用传统神经网络，在处理高维稀疏特征方面能力不足，且通信开销大、客户端异构性强等问题也制约了其大规模应用. 而量子深度学习在理论上具备并行计算与特征映射优势[7-8]，但相关方法多停留于理论研究或小规模仿真，缺乏在分布式隐私计算场景下的系统性研究.

为同时兼顾特征建模能力、训练效率与数据隐私保护，本文提出一种融合联邦学习与量子卷积神经网络的入侵检测模型 FedCQIDS(federated classical hybrid quantum convolutional intrusion detection system). 该模型在客户端构建轻量化的量子卷积模块，通过量子叠加与纠缠机制增强对低频攻击特征的表达能力；同时引入量子比特复用技术降低量子模块对硬件资源的需求，实现了对资源受限设备的友好适配. 在服务器端，采用联邦聚合策略对多个客户端模型进行融合，在保证数据隐私的前提下提升整体模型性能与训练稳定性. 实验结果显示，FedCQIDS 在 NSL-KDD 与 UNSW-NB15 两个数据集上均取得优于经典联邦模型的检测性能，尤其在少数类攻击识别任务中表现出显著优势.

本文的主要创新与贡献有 3 点：

1) 提出了将量子卷积神经网络嵌入联邦学习架构的网络入侵检测模型，构建了“客户端量子特征提取+服务器全局聚合”的混合训练范式，实现隐私保护与高维特征提取的双重突破；

2) 在 NSL-KDD 和 UNSW-NB15 两个公开数据集上开展对比实验，结果表明 FedCQIDS 在准确率和损失值指标上显著优于仅采用经典卷积层的联邦基线模型 FedCIDS，特别在少数类入侵检测中取得了更优表现，验证量子卷积层对稀疏特征提取的有效性；

3) 在资源受限的设备上通过量子比特复用技术实现轻量化设计以降低资源需求，证明量子模型可通过轻量化技术适配经典硬件，突破量子计算依赖专用设备的限制，推动了量子深度学习从实验室到工业应用的跨越.

1 相关工作

1.1 量子深度学习

随着量子计算技术的快速发展，其在人工智能领域中的应用潜力受到广泛关注. 量子计算以其并行处理能力和量子叠加特性，在处理大规模数据和复杂问题时展现出优越的效率[9]. 在此背景下，量子计算

与深度学习的结合已在许多应用领域凸显出巨大的潜力. Ngo 等人[10]探讨了量子生成对抗网络(QuGANs)的结构优化和训练策略，强调其在生成复杂分布数据方面的独特优势. Melnikov 等人[11]系统分析了量子增强算法、变分量子电路和量子强化学习等关键 QML 方法，展示其在提升经典 AI 性能及解决量子物理问题方面的应用潜力. Tian 等人[12]将量子神经网络(QNN)用于生成学习领域，提出多种量子生成学习模型(QGLM)，包括量子电路 Born 机器(QCBM)、量子生成对抗网络(QGAN)、量子玻尔兹曼机(QBM)和量子变分自编码器(QVAE)，展示了在传统机器学习任务和量子物理中的潜在应用前景. 在实际应用方面，Correll 等人[13]将 QNN 用于解决复杂的车辆路径优化问题，提出融合量子正交网络与强化学习的调度算法，显示出在小规模工业调度中的应用前景. 此外，Nicesio 等人[14]对量子深度学习在网络安全中的应用进行了系统综述，表明尽管量子模型在流量分类和入侵检测中表现出潜力，但仍多停留在单机仿真阶段，实际部署面临成本、噪声干扰、隐私风险等挑战.

1.2 联邦学习

联邦学习(federated learning, FL)由 Google 公司在 2016 年提出[15]，已经在多个领域获得广泛关注和应用. 该方法允许各个客户端在本地保留数据，通过共享模型参数而非原始数据完成联合训练，有效降低了隐私泄露风险. Thein 等人[16]提出了一种基于个性化联邦学习的入侵检测系统(pFL-IDS)，该系统通过引入本地模型训练的个性化方法和服务器端的投毒客户端检测机制，有效提高了联邦学习在入侵检测中的鲁棒性. 刘炜等人[17]提出了一种基于区块链和动态评估的隐私保护联邦学习模型 SPFLChain，利用区块链去中心化特性、稀疏化、差分隐私和联邦学习技术解决了隐私和安全问题. de Caldas Filho 等人[18]通过融合 HIDS 与 NIDS 并引入联邦学习，实现了分布式物联网(IoT)环境中的 botnet 攻击检测与缓解，增强了 IoT 设备的安全性. Campos 等人[19]则综述了联邦学习在物联网安全中的研究进展与挑战，指出非独立同分布(non-IID)数据对模型收敛与泛化能力存在显著影响，并提出基于 IBMFL 的优化方案. 尽管上述研究显著提升了入侵检测系统的隐私性与部署灵活性，但多数模型仍依赖经典神经网络，其在面对高维稀疏特征(如少数类攻击)时表达能力不足，存在性能瓶颈；在数据异构或小样本分布条件下，面对全局模型的收敛稳定性和判别能力仍不理想等挑战.

1.3 量子联邦学习

近年来，融合量子计算与联邦学习的研究逐渐兴起. 如 Chehimi 等人[20]提出了一种量子联邦学习(QFL)框架，支持分布式量子电路参数共享，并构建了量子联邦数据集. 该框架利用经典通信网络完成模型聚合，避免了量子数据传输的复杂性，在量子数据分类任务中表现出良好的适应性. Larasati 等人[21]从理论层面对 QFL 的概念、优势及挑战进行了系统性总结，强调量子纠错与可扩展性是制约 QFL 实际应用的关键难点，并探讨了多种混合架构与分布式部署路径. Ren 等人[22]进一步提出 QFL 的技术分类体系，围绕量子技术基础、模型结构与典型应用场景展开分析，为后续研究提供了系统化的理论框架. 然而，当前 QFL 的研究多集中于概念验证与小规模任务，尚未深入探讨如何将其应用于如入侵检测这类对模型鲁棒性和计算效率要求较高的实际场景中.

综上所述，从现有研究可以看出，量子计算在增强神经网络的特征表达能力方面展现出潜力，而联邦学习则有效缓解了集中式训练中的数据隐私风险. 然而，当前量子联邦学习在网络入侵检测这一任务中尚缺乏针对性探索，尤其在应对高维稀疏攻击特征提取与数据不可集中训练等双重挑战时，仍存在理论与应用的空白. 本文提出的 FedCQIDS 聚焦解决高维稀疏入侵特征难以建模与隐私保护不可兼得的问题. 该模型在客户端本地引入轻量化量子卷积层，有效增强对低频攻击模式的建模能力，同时借助联邦学习机制在不共享原始数据的前提下实现分布式协同训练. 该方法不仅在设计上实现了量子计算与联邦学习的有效融合，也为量子深度学习在网络安全领域中的落地应用探索了新的可行路径.

2 预备知识

为了便于读者理解本文所使用的关键技术，本节将简要介绍联邦学习、量子计算以及量子变分电路(VQC)的基础知识.

2.1 联邦学习

联邦学习旨在在不集中数据的前提下实现跨设备或跨组织的协同建模. 与传统集中式方法不同，联邦学习允许多个客户端(如边缘设备、机构节点)在本地使用私有数据独立训练模型，仅将模型参数(而非原始数据)上传至中央服务器进行聚合，从而有效缓解了数据隐私泄露问题，图 1 展示了联邦学习的基本工作流程.

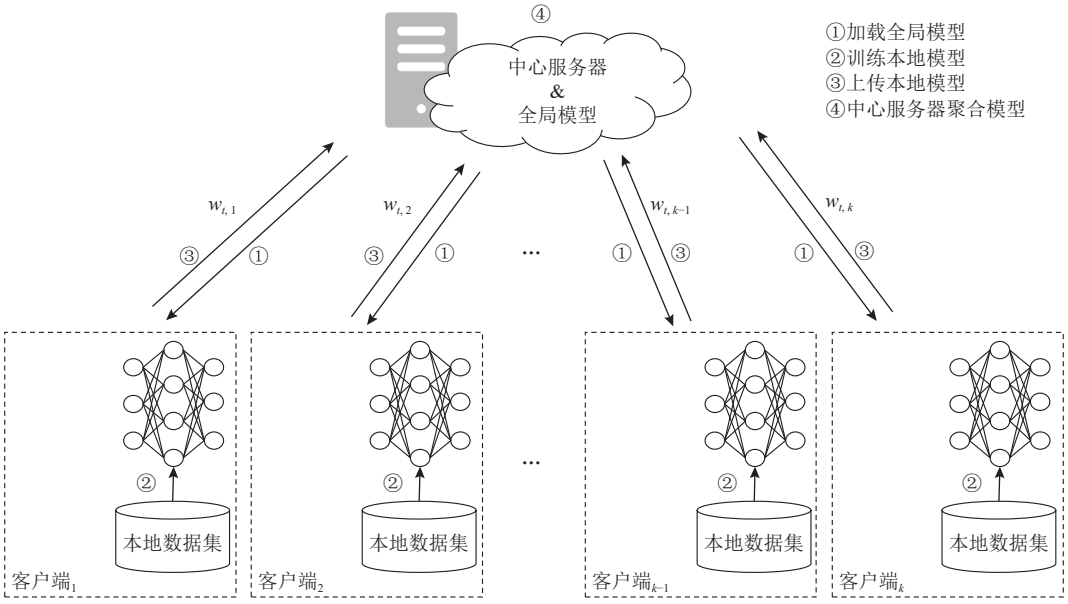


Fig. 1 Basic workflow diagram of federal learning

图 1 联邦学习基本工作流程图

联邦学习中最经典的算法为联邦平均算法(federated averaging, FedAvg). 其基本流程是：中央服务器初始化一个全局模型并分发给各客户端，各客户端使用本地数据独立训练模型后，将更新后的模型参数上传至服务器，服务器通过加权平均这些参数来更新全局模型，然后重复这一过程直至满足停止条件. FedAvg 通过减少数据传输量(仅传输模型参数而非整个数据集)和分散计算资源，有效提高了联邦学习的效率和可扩展性.

2.2 量子计算

量子计算是一种基于量子力学原理的新型计算范式，与传统二进制的 0 或 1 比特不同，量子比特(qubit)可处于叠加态，即“同时为 0 和 1”，并可通过纠缠态增强多个量子比特之间的信息传递. 量子计算的基本运算可以用量子态矢量和量子门操作表示. 以下将介绍常用的量子比特门.

1)Hadamard 门(创建叠加态). 用于将量子比特从经典基态变换为叠加态，是实现量子并行计算的基础，其矩阵形式为：

$$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}. \tag{1}$$

2)CNOT 门(受控非门). 实现量子比特间的纠缠，也是构建量子并行计算的关键. 当控制量子比特为|1⟩时，翻转目标量子比特的状态，其矩阵形式为：

$$\boldsymbol{CNOT}=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}. \tag{2}$$

3)RX 门(绕 X 轴旋转). 通过绕 X 轴的旋转改变量子态来实现参数化变换，常用于 VQC.

$$\boldsymbol{RX}(\theta)=\begin{pmatrix}\cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right)\\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right)\end{pmatrix}. \tag{3}$$

4)RY 门(绕 Y 轴旋转). RY 门是另一种常用的参数化旋转门，常与 RX 门配合使用，增强量子神经网络对输入特征的表达能力.

$$\boldsymbol{RY}(\theta)=\begin{pmatrix}\cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right)\\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right)\end{pmatrix}. \tag{4}$$

通过将多个量子门组成量子电路，并调节参数实现类似于神经网络的表示学习能力.

5)叠加态. 单量子比特通过 H 门或 RY 门变成叠加态，可同时探索多个计算路径，可以表示为：

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle,|\alpha|^2+|\beta|^2=1, \tag{5}$$

其中，α 和β 为复数概率幅度，| ⟩ 表示量子态.

6)纠缠态. 通过 CNOT 门操作多个量子比特变成纠缠态，例如生成贝尔几态(Bell state)：

$$|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle). \tag{6}$$

使 2 个量子比特状态完全关联，即使空间分离，测量结果仍保持强相关性.

2.3 VQC

VQC 也称为参数化量子电路(PQC)[23]，是由一系列量子门(如旋转门和纠缠门)操作组成的量子电

路，其参数(如旋转角度)是可调节的. VQC 的输出通常是一个量子态，其测量结果可以用于经典计算. VQC 是当前最常用的混合量子-经典计算框架之一，尤其适合在 NISQ(noisy intermediate-scale quantum)时代进行可行的量子学习任务，其基本结构包括：

1)编码模块. 将经典数据 x 映射至量子态，例如通过旋转门 RY：

$$|x\rangle = \boldsymbol{RY}(x_i)|0\rangle, \tag{7}$$

2)纠缠模块. 由可调参数 θ 控制的旋转门和纠缠门组成，例如：

$$U(\theta) = \prod_{i=1}^{n} \boldsymbol{RY}(\theta_i) \cdot CNOT_{i,i+l}, \tag{8}$$

3)测量与优化. 测量量子态得到期望值 $\langle Z\rangle$，并利用经典优化器(如梯度下降)更新参数.

3 融合联邦学习与量子卷积神经网络的网络入侵检测模型

3.1 模型架构概述与设计目标

为应对网络入侵检测中存在的数据分布不均、高维稀疏特征难以建模以及隐私保护需求等问题，本文提出一种融合联邦学习与量子计算的混合卷积神经网络模型 FedCQIDS(federated classical hybrid quantum convolutional intrusion detection system). 该模型在整体结构上采用典型的联邦学习架构，由中心服务器与多个本地客户端组成，各客户端在不共享原始数据的前提下完成本地训练并上传模型参数，由服务器进行聚合更新. FedCQIDS 的设计目标包括：实现对少数类系数攻击样本的有效建模；保证客户端本地数据的隐私性；通过引入轻量化的量子特征提取模块，在资源受限终端上提升模型表达能力. 用于入侵检测的联邦学习框架如图 2 所示.

3.2 客户端模型设计

FedCQIDS 由经典卷积特征提取模块、量子卷积模块、特征融合与分类模块 3 部分构成. 整体结构如图 3 所示.

3.2.1 经典卷积特征提取模块

该模块主要用于提取网络流量数据的低阶空间特征. 输入样本为预处理后的流量矩阵 $\boldsymbol{I} \in \mathbb{R}^{B\times C\times H\times W}$，其中 B 为批量大小，C 为通道数，H 和 W 为预处理后的输入高度与宽度.

第 1 个卷积层由 $K_1 = 32$ 个卷积核构成，每个卷积核的尺寸为 3×3，步长为 1，填充为 1. 卷积操作定义为：

$$\boldsymbol{x}_{\text{conv}} = ReLu(I * K_1 + b_1), \tag{9}$$

其中 $*$ 表示卷积操作，b_1 是偏置项. 输出张量展平为向量 $\boldsymbol{x}_{\text{cnn}} \in \mathbb{R}^d$.

该模块旨在提取常见攻击模式中的空间局部特征，并为后续量子模块提供基础表达.

3.2.2 量子卷积模块

为增强模型对稀疏、低频入侵模式的建模能力，本模块引入一个基于 4 量子比特的 VQC. 该电路接收一个输入向量 $\boldsymbol{x}_{\text{cnn}}$ 并输出一组量子比特的 Pauli-Z 期望值. 量子电路设计如下：

1)初始化. 每个量子比特 q_i 被初始化到 Hadamard 基态：

$$|\boldsymbol{H}_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{10}$$

2)参数编码. 输入特征通过量子门被编码到量子态中. 对于每个量子比特，应用旋转门 RY 进行处理，将经典特征映射至量子态：

$$\boldsymbol{RY}(\theta_i)|0\rangle = \cos\left(\frac{\theta_i}{2}\right)|0\rangle + \sin\left(\frac{\theta_i}{2}\right)|1\rangle, \tag{11}$$

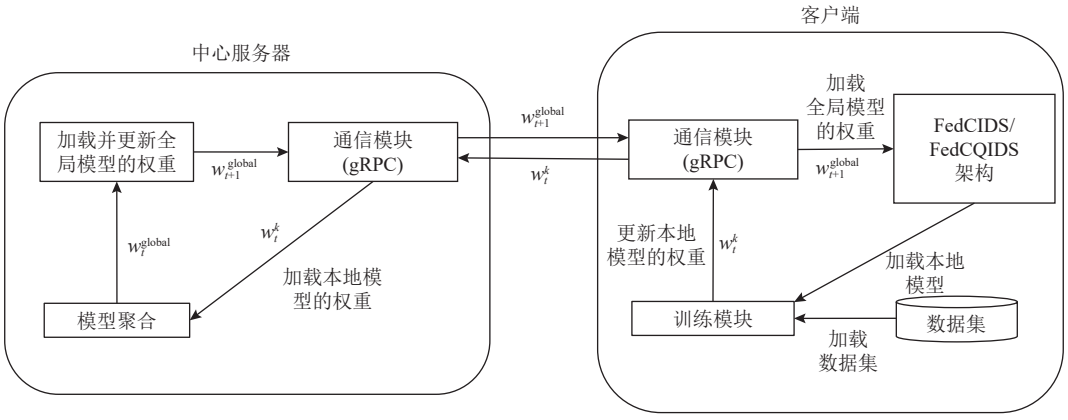


Fig. 2 Schematic diagram of the model framework

图 2 模型框架示意图

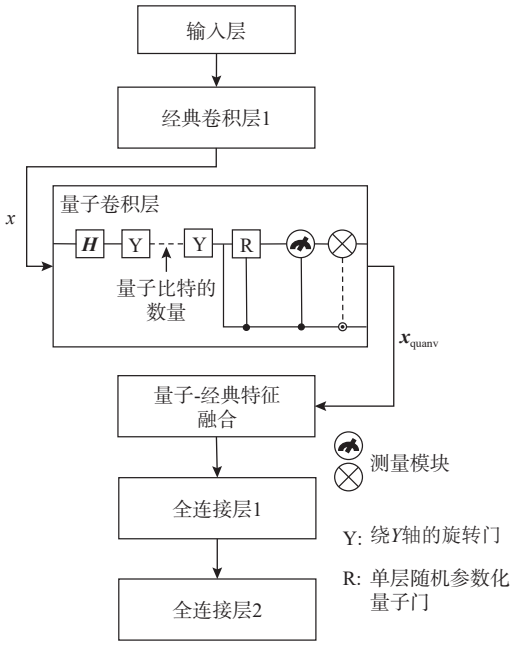


Fig. 3 Structure diagram of FedCQIDS

图 3 FedCQIDS 结构图

其中，θ_i是与输入特征相关的编码参数，$i=1,2,3,4$，通常是通过量子特征映射生成的.

3)随机量子层. 单层随机参数化量子门(RandomLayers)的参数范围为$[0,2\pi]$，可增强非线性表达能力.

4)期望值测量. 电路输出是每个量子比特的Pauli-Z算符的期望值：

$$\langle Z\rangle=\langle\psi|Z|\psi\rangle, \tag{12}$$

其中，Pauli-Z算符为：

$$Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}, \tag{13}$$

测量得到的结果将存储到输出张量$\boldsymbol{x}_{quanv}$中，获取的4维经典输出是：

$$\boldsymbol{x}_{quanv}=(\langle Z_1\rangle,\langle Z_2\rangle,\langle Z_3\rangle,\langle Z_4\rangle)\in\mathbb{R}^4.$$

相比于传统卷积网络，本文采用了轻量化的VQC结构，结合Hadamard初始化与RY编码层，使得输入特征可被映射至高维量子希尔伯特空间，在理论上能够增强对微弱、非线性特征的表达能力. 尤其在处理低频攻击样本时，通过Pauli-Z测量期望值构建的输出具有更强的区分性. 此外，本文引入了量子比特复用策略，使得量子电路可在资源受限设备上高效运行.

3.2.3 特征融合与分类模块

经典特征向量$\boldsymbol{x}_{cnn}$与量子卷积层输出向量$\boldsymbol{x}_{quanv}$在特征维度上拼接为联合向量：

$$\boldsymbol{x}_{cat}=Concat\left(\boldsymbol{x}_{cnn},\boldsymbol{x}_{quanv}\right). \tag{14}$$

随后送入2层全连接神经网络：

1)全连接层1. 将融合后的特征$\boldsymbol{x}_{cat}$，通过一个全连接层将特征映射到d维，操作定义为：

$$\boldsymbol{x}_{fc1}=ReLU\left(\boldsymbol{x}_{cat}\cdot\boldsymbol{W}_{fc1}+\boldsymbol{b}_{fc1}\right)\in\mathbb{R}^{B\times d}, \tag{15}$$

其中，$\boldsymbol{W}_{fc1}$是权重矩阵，$\boldsymbol{b}_{fc1}$是偏置项，d是全连接层1的输出通道数.

2)全连接层2. 最终的分类层将d维特征映射到n维输出，操作定义为：

$$\boldsymbol{y}_{out}=\boldsymbol{W}_{fc2}\cdot\boldsymbol{x}_{fc1}+\boldsymbol{b}_{fc2}\in\mathbb{R}^{B\times n}, \tag{16}$$

其中$\boldsymbol{W}_{fc2}$和$\boldsymbol{b}_{fc2}$分别是权重和偏置项，n表示包括正常及不同攻击类型的总数.

经典特征提取层保留了对局部模式的基本感知能力，而量子卷积层则提供了对高维非线性特征的补充建模能力. 通过拼接两者输出，可在保持结构简洁的基础上实现多尺度特征融合，从而提高模型的判别能力与泛化性能. 这种融合策略尤其适用于类别不平衡或高稀疏数据分布的场景.

3.3 联邦训练与聚合策略

FedCQIDS采用经典的FedAvg算法进行模型参数的聚合. 每轮通信中，中心服务器从客户端中选取部分参与者发送当前全局模型，客户端使用本地数据执行若干轮训练，并上传更新后的模型参数，服务器依据客户端数据量进行加权聚合.

该策略在不传输原始数据的前提下，实现模型训练与全局收敛，满足实际部署中对隐私保护和通信开销控制的双重需求. 实验中所有客户端使用统一学习率与训练轮次，确保比较公平性.

4 实验与讨论

4.1 实验设置

4.1.1 实验数据集

本文采用UNSW-NB15[24]和NSL-KDD[25]数据集. UNSW-NB15数据集通过IXIA PerfectStorm工具模拟多样化网络协议，结合Tcpdump捕获100 GB原始流量(PCAP格式)，最终转换为包含49个特征的CSV文件，这49个特征涵盖数据包与流特征，按数据类型被划分为Object(协议类型)、Integer(数据包长度)、Float(流量速率)、Timestamp(连接时间戳)及Binary(登录状态)，攻击类别包括9类异常行为(Analysis、Backdoor、DoS、Exploits、Fuzzers、Generic、Reconnaissance、Shellcode、Worms)和正常行为(Normal). NSL-KDD是KDD99数据集的改进版本，解决了原始数据冗余、重复记录及类别分布偏差问题. 其通过调整训练集与测试集的记录比例，提升模型评估的准确性

与可比性. 数据集包含 41 个特征，这些特征可分为基本特征(Basic)、流量特征(Traffic)和内容特征(Content)，攻击类别包括 4 类异常行为(DoS、Probe、U2R、R2L)与 1 类正常行为(Normal). 数据集被划分为 KDDTrain+(完整训练集)、KDDTest+(测试集). 表 1 列出了实验数据集的详细信息.

Table 1 Dataset Information

表 1 数据集信息

内容	UNSW-NB15	NSL-KDD
特征数量	49 个（包与流特征结合）	41 个（侧重基础流量统计）
攻击类型	9 类现代攻击（含物联网威胁）	4 类传统攻击
数据规模	2 540 044 条	148 517 条
数据集划分	每个客户端，训练集 175 341 条，测试集 82 332 条	每个客户端，训练集 125 973 条，测试集 22 544 条

4.1.2 实验配置

实验采用了 PyTorch 深度学习框架[26]、PennyLane 量子计算框架[27] 和 Flower 联邦学习框架[28]. 实验环境与配置如表 2 所示.

Table 2 Experimental Environment and Configuration Parameters

表 2 实验环境与配置参数

参数	配置环境
操作系统与平台	Windows Server
处理器（CPU）	Intel Xeon E5-2680 v4 @ 2.40GHz，28 核
内存（RAM）	32 GB
图形处理器（GPU）	NVIDIA GeForce RTX 3 090，显存约 40 GB

为全面评估所提出模型的有效性，本文设置以下对比方法.

1)FedCIDS. 采用经典卷积神经网络作为本地模型，在联邦学习框架下进行训练，其不含量子结构，用于验证量子层引入的性能增益.

2)CIDS. 在集中式架构下使用传统卷积神经网络统一训练，用于衡量联邦学习带来的性能差异.

3)CQIDS. 集中式架构下的量子混合卷积神经网络，加入量子卷积层进行特征提取，用于验证量子计算在非分布式环境中的建模能力.

所有对比方法均在相同的超参数配置和训练轮次下运行，确保结果具有可比性.

在本文中，选择了准确率(*Accuracy*)，损失值(*Loss*)作为评估指标，以评估所提出模型的性能.

准确率定义为正确预测的样本数量占总样本数量的比例，其计算公式为：

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}. \tag{17}$$

准确率是一个通用的性能评估指标，适合衡量类别分布均衡数据集中的整体性能. 作为最直观的性能评估标准，准确率为模型提供了一个基础的整体表现评估.

损失值表示模型在训练或测试阶段的误差大小，通常使用交叉熵损失(*Cross-Entropy Loss*)来度量分类问题的误差，其计算公式为：

$$Cross\text{-}EntropyLoss = -\frac{1}{N}\sum_{i=1}^{N}\left[y_i\log(p_i)+(1-y_i)\log(1-p_i)\right]. \tag{18}$$

损失值是衡量模型优化效果的重要指标，能够反映模型的学习进程和收敛程度. 通过观察训练和测试阶段的损失值变化，可以评估模型是否过拟合或欠拟合.

本文在 1 个服务器和 10 个客户端之间进行训练，批量大小为 32. 采用 Adam 优化器，学习率设置为 0.001. 客户端本地训练次数设置为 10，与服务器的通信轮次设为 20. 2 个模型的具体参数见表 3 和表 4.

Table 3 Local Training Model Architecture of FedCIDS

表 3 FedCIDS 本地训练模型架构

数据集	过程
NSL-KDD	$2\times7\times3 \xrightarrow[\text{stride = 1, ReLU}]{\text{Conv1}} 2\times7\times32 \xrightarrow[\text{stride = 1, ReLU}]{\text{Conv2}} 2\times7\times64 \xrightarrow{\text{flatten}} 896 \xrightarrow[\text{ReLU}]{\text{FC1}} 128 \xrightarrow{\text{FC2}} 5$
UNSW-NB15	$7\times2\times3 \xrightarrow[\text{stride=1, ReLU}]{\text{Conv1}} 7\times2\times32 \xrightarrow[\text{stride = 1,ReLU}]{\text{Conv2}} 7\times2\times64 \xrightarrow{\text{flatten}} 896 \xrightarrow[\text{ReLU}]{\text{FC1}} 32 \xrightarrow{\text{FC2}} 10$

Table 4 Local Training Model Architecture of FedCQIDS

表 4 FedCQIDS 本地训练模型架构

数据集	过程
NSL-KDD	$2\times7\times3 \xrightarrow[\text{stride = 1, ReLU}]{\text{Conv1}} 2\times7\times32 \xrightarrow{\text{flatten}} 448 \xrightarrow{\text{QConv}} 4\text{D 量子态} \xrightarrow{\text{Splicingfeatures}} 448+4\text{D} \xrightarrow[\text{ReLU}]{\text{FC1}} 128 \xrightarrow{\text{FC2}} 5$
UNSW-NB15	$7\times2\times3 \xrightarrow[\text{stride=1, ReLU}]{\text{Conv1}} 7\times2\times32 \xrightarrow{\text{flatten}} 448 \xrightarrow{\text{QConv}} 4\text{D 量子态} \xrightarrow{\text{Splicingfeatures}} 448+4\text{D} \xrightarrow[\text{ReLU}]{\text{FC1}} 32 \xrightarrow{\text{FC2}} 10$

4.2 实验结果分析

本文评估了 2 种联邦学习架构 FedCIDS 和 FedCQIDS 在入侵检测任务中的性能表现，使用 NSL-KDD 和 UNSW-NB15 两个标准数据集开展实验. 为便于全面对比，本研究同时引入了集中式训练方法作为性能基线，无隐私保护机制. 我们从准确率与损失值 2 个维度对集中式模型与联邦模型进行了系统评估. 表 5 展示了 FedCIDS，FedCQIDS 及其对应的集中式版本在 2 个数据集上的准确率对比结果. 实验结果表明，引入量子卷积层的模型无论在集中式还是联邦架构下均表现优越，充分体现了量子计算在特征提取与表示能力方面对提升入侵检测性能的积极作用.

Table 5 Comparison of Maximum Accuracy of Intrusion Detection of Centralised Models and Federated Learning Models

表 5 集中式模型与联邦学习模型的入侵检测最高准确率对比 %

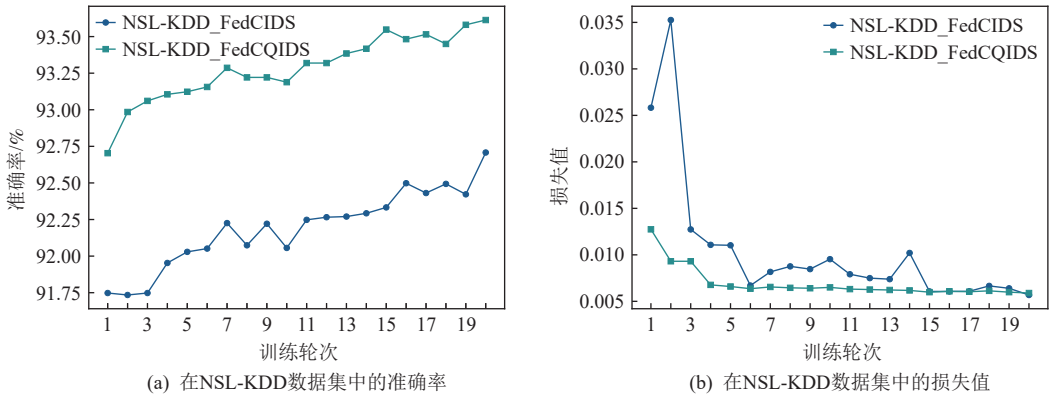
数据集	集中式模型		联邦模型	
	CIDS	CQIDS	FedCIDS	FedCQIDS
NSL-KDD	92.01	92.94	92.71	93.58
UNSW-NB15	61.04	64.26	77.85	79.82

图 4 与图 5 分别展示了 FedCQIDS 与传统联邦模型 FedCIDS 在 NSL-KDD 与 UNSW-NB15 两个数据集上的准确率与损失值变化趋势. 整体来看，FedCQIDS 在模型性能与训练稳定性方面均优于基线模型 FedCIDS，尤其在高维稀疏特征和类别严重不均衡的场景中表现出显著优势. 在 NSL-KDD 数据集中，整个训练过程中 FedCQIDS 的准确率始终高于 FedCIDS 的准确率，且曲线更平滑，波动更小. FedCQIDS 平均准确率达到 93.33%，相比 FedCIDS 提升了约 1.11 个百分点. 其平均损失值为 0.007 1，低于 FedCIDS 的 0.010 1，降幅约为 29.7%，显示出量子特征映射机制在特征表达和收敛路径控制上的优势，即使在结构简单、数据相对均衡的场景中也展现出更强的训练效率.

在特征维度更高、类别分布更加不均的 UNSW-NB15 数据集中，FedCQIDS 的优势更为明显. 实验结果显示，FedCQIDS 准确率同样始终高于 FedCIDS，且平均准确率为 79.09%，相较 FedCIDS 提升了 7.5 个百分点；同时，平均损失值由 0.068 1 下降至 0.060 6，整体下降约 11%. 从图 5 可以知道，FedCQIDS 在前 10 轮训练阶段即实现快速准确率提升，并在随后的通信轮次中保持稳定趋势，而 FedCID 在训练过程中的损失值与准确率存在较大波动. 这一趋势反映出，FedCQIDS 通过量子特征映射机制，有效增强了模型对低频攻击与复杂特征的建模能力，缓解了传统联邦平均策略因客户端异构性带来的训练不稳定问题，展现出更强的泛化能力与收敛效率. 尤其值得注意的是，FedCQIDS 在当前实验中已展现出较强的性能提升，说明其在联邦学习环境中具备良好的适应性与实用性.

为进一步验证 FedCQIDS 在稀疏、低频入侵流量识别方面的性能优势，我们对 UNSW-NB15 数据集中 2 类样本稀缺攻击类型（Shellcode 和 Worms）进行了独自的准确率对比分析. 从表 6 可以看出，FedCQIDS 在处理样本极度不均衡的攻击类别时依然展现出更高的识别准确率，其中对 Worms 攻击的检测准确率提升 6.8 个百分点. 这一结果表明，量子卷积模块在特征空间中能够更有效识别微弱信号与稀疏模式，进一步印证了其在高维稀疏攻击识别任务中的优势，也支撑了模型对复杂网络场景的适应能力.

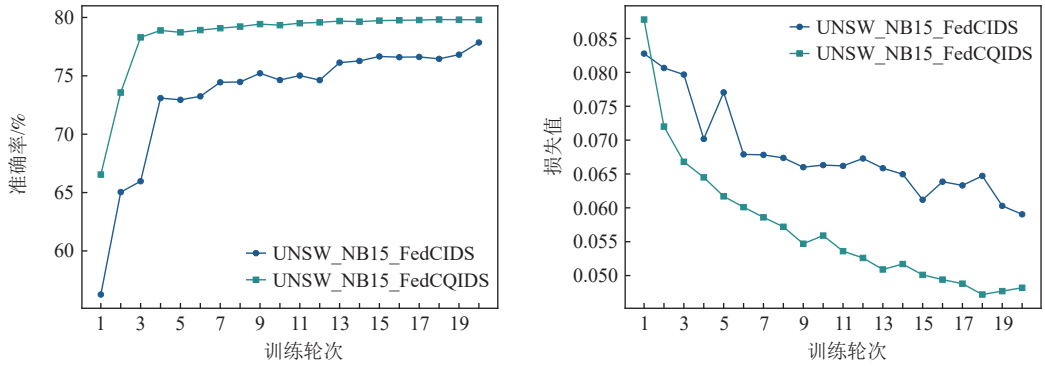
量子层的引入显著提升了模型在复杂数据集上的特征提取能力：在 UNSW-NB15 数据集中，FedCQIDS 相较于传统联邦模型 FedCIDS 在平均准确率上提升



(a) 在NSL-KDD数据集中的准确率 (b) 在NSL-KDD数据集中的损失值

Fig. 4 Experimental results of FedCIDS and FedCQIDS on NSL-KDD dataset

图 4 FedCIDS 和 FedCQIDS 在 NSL-KDD 数据集上的实验结果



(a) 在UNSW_NB15数据集中的准确率 (b) 在UNSW_NB15数据集中的损失值

Fig. 5 Experimental results of FedCIDS and FedCQIDS on UNSW_NB15 dataset

图 5 FedCIDS 和 FedCQIDS 在 UNSW_NB15 数据集上的实验结果

Table 6 Detection Accuracy Comparison of Two Models on Sparse and Low-Frequency Attack Types

表 6 稀疏、低频攻击类型下 2 种模型的检测准确率对比

攻击类别	样本数量	FedCIDS 准确率/%	FedCQIDS 准确率/%	提升百分点数
Shellcode	378	66.7	71.4	4.7
Worms	44	59.1	65.9	6.8

了约 7.5 个百分点，同时平均损失值下降了约 11%，验证了量子计算通过叠加态与纠缠态特性对高维稀疏特征的并行处理优势，其非线性表示能力有效缓解了类别分布严重失衡场景下的模式捕捉难题，这一特性在联邦学习的分布式架构中尤为重要，能够协同应对数据异构性带来的优化困难，并减少因过拟合带来的性能波动. 此外，FedCQIDS 在 NSL-KDD 数据集上同样实现了约 1.11 个百分点的准确率提升与近 30% 的损失值下降，尽管该数据集结构较为均衡，仍验证了该方法在不同数据规模和特征复杂度下的适应能力. 通过对比可见，量子特征增强机制不仅提升了单轮训练效率，也显著改善了模型在长期训练中的稳定性与泛化能力，具备良好的实际应用基础.

此外，为提升模型在实际设备上的可部署性，本文设计阶段引入了量子比特复用机制. 在量子模拟平台上，我们对比了等价输入规模下单量子比特与多量子比特卷积模块的运行效率，结果表明，FedCQIDS 的多量子比特结构的平均运行时间缩短约 12%. 该设计不仅降低了模拟复杂度，也为后续部署至 NISQ 设备提供了可行性基础，体现出一定的资源友好性与可扩展性.

同时，FedCQIDS 展现出广阔的实际应用前景，尤其适用于物联网设备日志等高维网络流量的实时分析，可提升对 APT 攻击等隐蔽威胁的早期检测能力，同时，其对隐私友好的设计也使其在医疗、金融等数据敏感领域具备良好的适配性. 然而，研究仍存在局限性：当前实验仍基于理想化的量子模拟环境，未充分考虑真实 NISQ 设备下的量子噪声与硬件限制. 未来研究可在真实量子平台上进一步验证模型的鲁棒性，同时结合量子纠错、量子注意力机制等前沿技术优化量子电路结构，提升在资源受限终端上的部署效率与适应能力.

5 结 论

本文提出了一种融合联邦学习与量子卷积神经网络的入侵检测模型 FedCQIDS，旨在在保障数据隐私的前提下提升对复杂、稀疏攻击特征的识别能力. 通过在客户端引入轻量化的量子卷积模块，显著增强了对高维稀疏特征的建模能力，并结合“本地量子特征提取 + 服务器全局聚合”的联邦训练范式，实现了多方协同下的高效入侵检测. 在 NSL-KDD 与 UNSW-NB15 两个标准数据集上的实验验证了该方法在准确率、损失值及训练稳定性方面均优于传统卷积神经网络构建的联邦模型，特别是在应对类别不均与复杂攻击模式方面展现出更强的泛化能力. 此外，模型引入量子比特复用机制，在不依赖专用量子硬件的条件下实现了初步轻量化部署，为量子神经网络在边缘设备和现实应用场景中的推广提供了可行路径.

尽管取得了初步成效，本研究仍存在一定的局限性. 首先，由于当前多数联邦入侵检测方法仍采用经典网络结构，缺乏对稀疏特征的量子增强机制，故本文主要对比了最具代表性的经典卷积联邦模型 FedCIDS 作为基线. 后续可进一步与如 pFL-IDS 等强化版联邦模型进行深入对比. 其次，实验基于理想化量子模拟环境，未充分考虑当前 NISQ 设备下的量子

噪声干扰. 未来工作可进一步在真实量子硬件上验证模型的鲁棒性, 并结合量子纠错与参数压缩等技术, 优化模型的部署效率与实用性. 还可探索跨域迁移机制, 以提升模型在异构网络场景下的适应性与推广能力.

作者贡献声明: 李冬芬提出研究方向并指导修改论文; 向秋雨撰写论文和设计实验; 胡志康、袁宇航参与数据收集和部分数据分析; 孙雨晨参与文献调研并提供相关文献资料; 徐菡参与实验操作并协助完成实验; 宋征宇、韩浩民参与数据分析和部分图表绘制; 白冬雪参与研究过程讨论并提出了部分研究观点; 多滨、周让指导实验并提出论文修改建议.

参 考 文 献

[1] Lampe B, Meng W. Intrusion detection in the automotive domain: A comprehensive review[J]. IEEE Communications Surveys and Tutorials, 2023, 25(4): 2356−2426

[2] Antunes R S, Costa C A, Kuderle A, et al. Federated learning for healthcare: Systematic review and architecture proposal[J]. ACM Transactions on Intelligent Systems and Technology, 2022, 13(4): 1−23

[3] Nevrataki T, Iliadou A, Ntolkeras G, et al. A survey on federated learning applications in healthcare, finance, and data privacy/data security[C]//Proc of AIP Conf Proceedings. Melville, NY: AIP Publishing LLC, 2023: 120015

[4] Sun Nan, Wang Wei, Tong Yongxin, et al. Blockchain based federated learning for intrusion detection for Internet of things[J]. Frontiers of Computer Science, 2024, 18(5): 185328−185338 (in Chinese)
(孙楠, 王伟, 童永信, 等. 基于区块链的物联网入侵检测联邦学习方法[J]. 计算机科学前沿, 2024, 18(5): 185328−185338)

[5] Wen Jie, Zhang Zhixia, Lan Yang, et al. A survey on federated learning: Challenges and applications[J]. International Journal of Machine Learning and Cybernetics, 2023, 14(2): 513−535

[6] Lin Weiwei, Shi Fang, Zeng Lan, et al. Survey of federated learning open-source frameworks[J]. Journal of Computer Research and Development, 2023, 60(7): 1551−1580 (in Chinese)
(林伟伟, 石方, 曾岚, 等. 联邦学习开源框架综述[J]. 计算机研究与发展, 2023, 60(7): 1551−1580)

[7] Cerezo M, Verdon G, Huang H Y, et al. Challenges and opportunities in quantum machine learning[J]. Nature Computational Science, 2022, 2(9): 567−576

[8] Zeguendry A, Jarir Z, Quafafou M. Quantum machine learning: A review and case studies[J]. Entropy, 2023, 25(2): 287−327

[9] Bu Kaifeng. Quantum computing meets federated Learning[J]. Science China Physics, Mechanics & Astronomy, 2022, 65(1): 210331

[10] Ngo T A, Nguyen T, Thang T C. A survey of recent advances in quantum generative adversarial networks[J]. Electronics, 2023, 12(4): 856−876

[11] Melnikov A, Kordzanganeh M, Alodjants A, et al. Quantum machine learning: From physics to software engineering[J]. Advances in Physics: X, 2023, 8(1): 2165452−2165502

[12] Tian Jinkai, Sun Xiaoyu, Du Yuxuan, et al. Recent advances for quantum neural networks in generative learning[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 45(10): 12321−12340

[13] Correll R, Weinberg S J, Sanches F, et al. Quantum neural networks for a supply chain logistics application[J]. Advanced Quantum Technologies, 2023, 6(1): 2200183−2200197

[14] Nicesio O K, Leal A G, Gava V L. Quantum machine learning for network intrusion detection systems, a systematic literature review[C]//Proc of the 2nd IEEE Int Conf on AI in Cybersecurity. Piscataway, NJ: IEEE, 2023: 1−6

[15] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proc of the 20th Int Conf on Artificial Intelligence and Statistics. Fort Lauderdale, FL: PMLR, 2017, 54: 1273−1282

[16] Thein T T, Shiraishi Y, Morii M. Personalized federated learning-based intrusion detection system: Poisoning attack and defense[J]. Future Generation Computer Systems, 2024, 153: 182−192

[17] Liu Wei, Tang Congke, Ma Jie, et al. A privacy-preserving federated learning model based on blockchain and dynamic evaluation[J]. Journal of Computer Research and Development, 2023, 60(11): 2583−2593 (in Chinese)
(刘炜, 唐琮轲, 马杰, 等. 基于区块链和动态评估的隐私保护联邦学习模型[J]. 计算机研究与发展, 2023, 60(11): 2583−2593)

[18] de Caldas Filho F L, Soares S C M, Oroski E, et al. Botnet detection and mitigation model for IoT networks using federated learning[J]. Sensors, 2023, 23(14): 6305−6339

[19] Campos E M, Saura P F, González-Vidal A, et al. Evaluating federated learning for intrusion detection in Internet of things: Review and challenges[J]. Computer Networks, 2022, 203: 108661−108676

[20] Chehimi M, Saad W. Quantum federated learning with quantum data[C]//Proc of ICASSP 2022. Piscataway, NJ: IEEE, 2022: 8617−8621

[21] Larasati H T, Firdaus M, Kim H. Quantum federated learning: Remarks and challenges[C]//Proc of the 9th IEEE Int Conf on Cyber Security and Cloud Computing/8th IEEE Int Conf on Edge Computing and Scalable Cloud. Piscataway, NJ: IEEE, 2022: 1−5

[22] Ren Chao, Yan Rudai, Zhu Huihui, et al. Toward quantum federated learning[J]. arXiv preprint, arXiv: 2306.09912, 2023

[23] Shi Jinjing, Wang Wenxuan, Lou Xiaoping, et al. Parameterized hamiltonian learning with quantum circuit[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 45(5): 6086−6095

[24] More S, Idrissi M, Mahmoud H, et al. Enhanced intrusion detection systems performance with UNSW-NB15 data analysis[J]. Algorithms, 2024, 17(2): 64−79

[25] Masoodi F, Bamhdi A M, Teli T A. Machine learning for classification analysis of intrusion detection on NSL-KDD dataset[J]. Turkish Journal of Computer and Mathematics Education, 2021, 12(10): 2286−2293

[26] Ansel J, Yang E, He H, et al. Pytorch 2: Faster machine learning through dynamic Python bytecode transformation and graph compilation[C]//Proc of the 29th ACM Int Conf on Architectural Support for Programming Languages and Operating Systems. New York: ACM, 2024: 929−947

[27] Schuld M, Bergholm V, Gogolin C, et al. PennyLane: Automatic differentiation of hybrid quantum-classical computations[J]. Quantum, 2018, 2: 56−70

[28] Beutel D J, Topal T, Mathur A, et al. Flower: A friendly federated learning framework[J]. arXiv preprint, arXiv: 2209.06970, 2022



Li Dongfen, born in 1979. Postdoc professor, master supervisor. Member of CCF. His main research interests include network security, artificial intelligence, quantum cryptography communication, and mobile Internet security.

李冬芬, 1979 年生. 博士后，教授，硕士生导师. CCF 会员. 主要研究方向为网络安全、人工智能、量子密码通信、移动互联网安全.



Xiang Qiuyu, born in 2000. Master candidate. Her main research interests include quantum deep learning and quantum federated learning.

向秋雨, 2000 年出生. 硕士研究生. 主要研究方向为量子深度学习、量子联邦学习.



Hu Zhikang, born in 2000. Master candidate. His main research interest includes quantum image processing.

胡志康, 2000 年生. 硕士研究生. 主要研究方向为量子图像处理.



Yuan Yuhang, born in 2001. Master candidate. His main research interest includes quantum machine learning.

袁宇航, 2001 年生. 硕士研究生. 主要研究方向为量子机器学习.



Sun Yuchen, born in 1999. Master candidate. Her main research interest includes quantum deep learning.

孙雨晨, 1999 年生. 硕士研究生. 主要研究方向为量子深度学习.



Xu Han, born in 2001. Master candidate. Her main research interests include quantum machine learning.

徐　菡, 2001 年生. 硕士研究生. 主要研究方向为量子机器学习.



Song Zhengyu, born in 2001. Master candidate. His main research interest includes quantum machine learning.

宋征宇, 2001 年生. 硕士研究生. 主要研究方向为量子机器学习.



Han Haomin, bom in 2001. Master candidate. His main research interest includes quantum machine learning.

韩浩民, 2001 年生. 硕士研究生. 主要研究方向为量子机器学习.



Bai Dongxue, born in 2001. Master candidate. His main research interest includes quantum machine learning.

白冬雪, 2001 年生. 硕士研究生. 主要研究方向为量子机器学习.



Duo Bin, born in 1982. Postdoc, professor, master supervisor. Member of CCF. His main research interests include fully autonomous robot technology and equipment intelligence, unmanned trunking intelligent networking and cooperative communication key technology, 6G-enabled unmanned trunking industry solutions, and IoT information security technology.

多　滨, 1982 年生. 博士后，教授，硕士生导师. CCF 会员. 主要研究方向为全自主机器人技术与装备智能化、无人集群智能组网与协同通信关键技术、6G 赋能的无人集群行业解决方案、物联网信息安全技术.



Zhou Rang, born in 1987. PhD, professor, master supervisor. His main research interests include data security and privacy protection, IoT security, and blockchain security.

周　让, 1987 年生. 博士，研究员，硕士生导师. 主要研究方向为事数据安全与隐私保护、物联网安全、区块链安全.