FedQ: A Secure Collaborative Cyber Defense Framework for Internet of Medical Things Based on Quantum and Federated Learning

Vivian Ukamaka Ihekoronye, Esmot Ara Tuli, Urslla Uchechi Izuazu, Jae Min Lee, Dong-Seong Kim
Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea
Kumoh National Institute of Technology Gumi, South Korea
(ihekoronyevivian, uursla8)@gmail.com,(dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—This study introduces FedQ, a quantum-based security scheme for defending against cyber attacks in the Internet of Medical Things (IoMT). By integrating quantum key distribution (QKD) with privacy-preserving federated learning (FL), FedQ ensures secure communication between hospital management units (HMUs) and the FL server. QKD encrypts FL transmissions, enhancing security. The FedQ ML model achieves exceptional performance, with 93% accuracy and 90.25% precision, outperforming classical federated averaging techniques**

***Index Terms*—Federated Learning, Quantum Computing, Quantum Key Distribution, Internet of Medical Things, Secure Privacy-Preserving Computation**

I. Introduction

The COVID-19 pandemic has heightened awareness of physical and mental health challenges, leading to an intentional focus on individual healthcare management [1]. Also, advancements in Internet of Things (IoT) technology have facilitated connectivity among diverse healthcare entities, including hospitals, wearable devices, implantable devices, and ingestible sensors. This integration of IoT with healthcare services is referred to as the Internet of Medical Things (IoMT). IoMT offers intelligent medical services such as remote patient monitoring and telemedicine, enhancing real-time health status monitoring. However, despite its benefits in healthcare effectiveness and efficiency, the widespread adoption of IoMT is hindered by privacy and security challenges [2].

Federated Learning (FL) is a decentralized ML framework utilized in the IoMT ecosystem to train security models for autonomous attack detection. IoMT devices transmit only local model parameters to the federal server, thus, preserving sensitive healthcare data. Despite its privacy benefits over centralized ML systems, FL remains vulnerable to cyber threats [1]. Currently, quantum computing is leveraged to mitigate the security vulnerabilities in FL [3], [4] and enhance the security of the IoMT ecosystem. We propose **FedQ**, a novel quantum-based authentication and registration technique to enhance communication security in the IoMT ecosystem. **FedQ** leverages the quantum entanglement and superposition principle of quantum mechanics for robust communication channels based on the quantum key distribution (QKD) protocol. Also, **FedQ** integrates differential privacy to mitigate collaborative training attacks in a federated setup.

II. Proposed Privacy Prioritizing Quantum Federated Cyber Defense Framework

As highlighted in Fig.1, the proposed framework comprises hospital management units (HMUs) acting as clients and the FL server. Clients consist of IoMT devices within each HMU's LAN, while the FL server aggregates data across HMUs via a WAN. The B92 protocol of QKD ensures secure communication between the FL server and HMUs. It establishes a quantum channel to generate a unique key pair for each HMU and the server, verifying clients' integrity. Classical bits C_n are converted to qubits Q_n and encoded into quantum states $|0\rangle$ and $|+\rangle$, along with shared measurement bases B_n. A QKD key pair is generated if the measurement result R_n meets a predefined threshold T_R, otherwise, the client is labeled an eavesdropper and isolated from the network.

Once secure communication is established the FL task of detecting attacks in the IoMT network proceeds. Firstly, the server distributes the global model W_g parameters to a randomly selected subset of K authorized clients. W_g is trained using the clients' data D to compute the local loss function θ. To avoid eavesdropping and inference attacks, the Laplace mechanism M is locally implemented to add noise and perturb the clients' models, thereby preempting data compromise [5]. M satisfies ϵ-DP for a given function: f: $W^n \rightarrow J$, for all set of possible outputs J based on Equation 1.

$$M(W) = f(W) + Lap(\frac{\Delta f}{\epsilon}) \tag{1}$$

where $M(W)$ is the output of the perturbed model, Δf is the sensitivity of f, $Lap(\frac{\Delta f}{\epsilon})$ is the Laplacian noise and ϵ is the privacy budget that guarantees the level of privacy provided by the mechanism. Furthermore, clients' perturbed models are sent to the FL server where it is aggregated using the averaging principle of FedAVG (Equation 2) to compute the optimized global model W_{g+1}.

$$W_{g+1} = \frac{1}{N}\sum_{i=1}^{N} M(W_g^i) \tag{2}$$

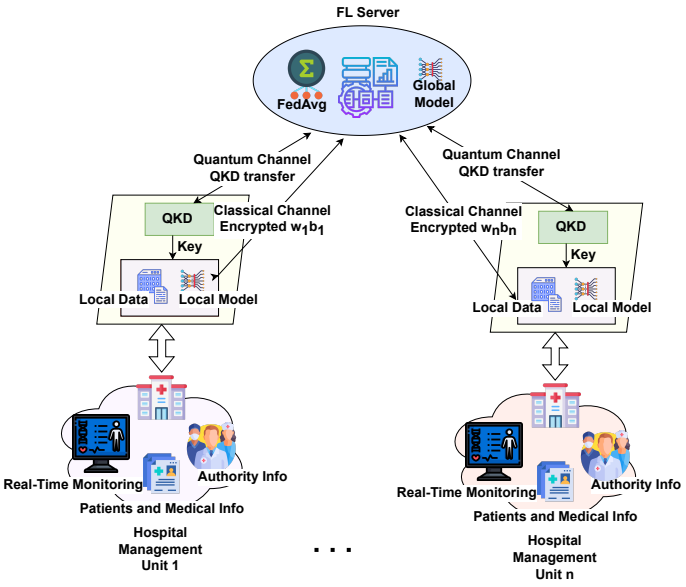

Fig. 1. Framework of Proposed Federated Quantum Mechanism for Secure IoMT Ecosystem

Subsequently, clients download W_{g+1} to perform network intrusion detection on another batch of network traffic. This iterative process of local training and model perturbation is done over multiple SGD steps, epochs E, and rounds R until the model converges to an optimal solution.

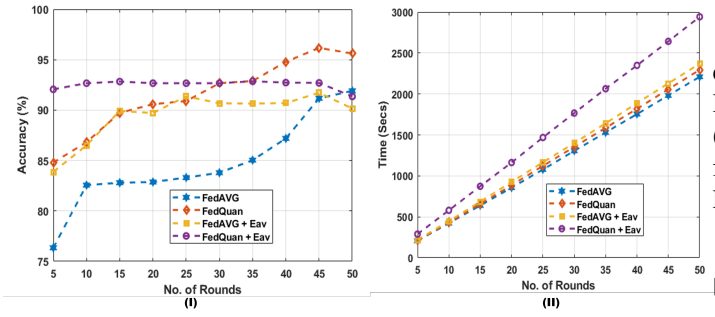

Fig. 2. Performance Comparison of FedQ and FedAVG when $K = 20$ and $\epsilon = 0.5$ under Eavesdropping and No Eavesdropping Attacks (I) Accuracy Performance (II) Detection Time Performance

III. Experimental Setup and Result Analysis

The proposed security model is a shallow neural network with an input layer, 2 hidden layers of size (64, 64), and an output layer. The model was trained using the WUSTL-EHMS-2020 dataset [6] and preprocessed adequately. Fig. 2 displays the accuracy and time detection performance of FedQ and the classical FedAVG when K = 20, a privacy budget of 0.5, when 10% of the clients are simulated as eavesdroppers. It is obtained that FedQ consistently achieved over 93% accuracy in detecting attacks, outperforming FedAVG even in the presence of eavesdroppers. Similarly, Fig.2 (II) illustrates the attack detection time comparison. Both algorithms demonstrated similar efficiency in detection. However, FedQ, with its authentication and verification scheme, expended a longer time, especially in the presence of eavesdroppers. Similar outstanding performance was achieved by FedQ based on other metrics as detailed in Table I.

TABLE I
Average Attack Detection Performance Based on Essential Metrics

Model	Acc.(%)	Prec.(%)	Rec.(%)	F1 (%)
FedAVG + Eve	90.02	68.20	66.24	67.20
FedQ + Eve	91.49	81.04	86.53	83.65
FedAVG	81.69	75.77	63.42	69.02
FedQ	92.52	90.25	92.84	91.48

IV. Conclusion

This study integrated quantum computing and federated learning (FL) to enhance cybersecurity in the Internet of Medical Things (IoMT). By employing the B92 Quantum Key Distribution (QKD) protocol, FL communications are encrypted, ensuring security against classical and quantum threats. The proposed federated-quantum model demonstrated resilience to attacks and outperformed classical methods. Future work will focus on optimizing the efficiency of the QKD protocol for practical deployment.

Acknowledgment

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2024-2020-0-01612) supervised by the IITP (Institute for Information and Communications Technology Planning and Evaluation)

References

[1] V. K. Prasad, P. Bhattacharya, D. Maru, S. Tanwar, A. Verma, A. Singh, A. K. Tiwari, R. Sharma, A. Alkhayyat, F.-E. Țurcanu, and M. S. Raboaca, "Federated learning for the internet-of-medical-things: A survey," *Mathematics*, vol. 11, no. 1, 2023. [Online]. Available: https://www.mdpi.com/2227-7390/11/1/151

[2] Z. Xu, Y. Guo, C. Chakraborty, Q. Hua, S. Chen, and K. Yu, "A simple federated learning-based scheme for security enhancement over internet of medical things," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, pp. 652–663, 2023.

[3] P. Hyunwoo and L. Jaedong, "Hqk-fl: Hybrid-quantum-key-based secure federated learning for distributed multi-center clinical studies," *Human-Centric Computing and Information Sciences*, 2023.

[4] E. A. Tuli, J.-M. Lee, and D.-S. Kim, "Integration of quantum technologies into metaverse: Applications, potentials, and challenges," *IEEE Access*, vol. 12, pp. 29 995–30 019, 2024.

[5] V. U. Ihekoronye, D.-S. Kim, and J. M. Lee, "Federated learning with differential privacy for intrusion detection in internet of flying things: A robust approach," in *2023 14th International Conference on Information and Communication Technology Convergence (ICTC)*, 2023, pp. 932–937.

[6] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion detection system for healthcare systems using medical and network data: A comparison study," *IEEE Access*, vol. 8, pp. 106 576–106 584, 2020.