Hybrid Quantum Machine Learning for Threat Detection in Industrial Internet of Things

Esmot Ara Tuli†, Raneem Khafagy*, Md Mehedi Hasan Somrat*, and Dong-Seong Kim§
†ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, South Korea.
*Networked Systems Laboratory, Department of IT Convergence Engineering,
§Networked Systems Laboratory (NSLab Inc.), Kumoh National Institute of Technology, South Korea
(esmot, raneemkhafagy, mehedi, dskim) @kumoh.ac.kr

***Abstract*—Industrial internet of things (IIoT) networks are often targeted by cyberattacks due to their economic importance to a country. A quantum-classical hybrid deep learning model $Pure - HQML$ is developed in this study to detect malicious traffic in the IIoT network. To reduce complexity and enhance model performance, this work employs analysis of variance F-test (ANOVA F-test) statistical technique to select relevant features. The results of our proposed model demonstrate exceptional performance, achieving high accuracy and low-complexity model structure in only a few epochs.**

***Index Terms*—Data security, industrial internet of things, intrusion detection system, quantum machine learning, feature selection.**

I. Introduction

The Industrial Internet of Things (IIoT) refers to a specialized network of interconnected devices designed for factory automation, smart manufacturing, and industrial execution processes. IIoT integrates various advanced technologies such as sensors, digital twins, artificial intelligence, and blockchain, among others, to enhance manufacturing efficiency and streamline industrial operations. Compared to general IoT networks, IIoT networks are mission-critical due to their connection with production equipment. Beacuse of large-scale heterogeneous connectivity of the IIoT network, it is vulnerable to security threats [1]. Traditional intrusion detection systems (IDS) for IIoT have relied mainly on classical machine learning (ML) and deep learning (DL) methods to analyze network traffic and detect anomalies. For example, [2] proposed ML-based method for anomaly detection for IIoT control and data acquisition (SCADA) network. The Chi-square feature selection method was applied to select important features for the model training. Along with centralized learning, collaborative IDS also effective [3].

Recent advances in quantum machine learning (QML) have opened new way for improving IDS in IIoT networks by exploiting quantum parallelism and entanglement properties to capture complex data patterns more effectively than classical models alone [4]. Hybrid quantum-classical architectures, combine classical factorization machines with quantum neural networks to leverage the strengths of both paradigms for predictive learning tasks [5]. The contributions of this paper can be summarized as follows:

1) We design and implement a hybrid quantum-classical deep learning model ($Pure - HQML$) that combines classical factorization machines with quantum neural networks, facilitating enhanced feature interaction modeling for IIoT intrusion detection.
2) We incorporate ANOVA F-test based feature selection to reduce model complexity and training time, improving efficiency without compromising detection accuracy.
3) We evaluate the proposed model on the WUSTL-IIoT-2021 dataset, demonstrating superior performance in only a few training epochs.

II. Hybrid Quantum Machine Learning For Threat Detection In IIOT

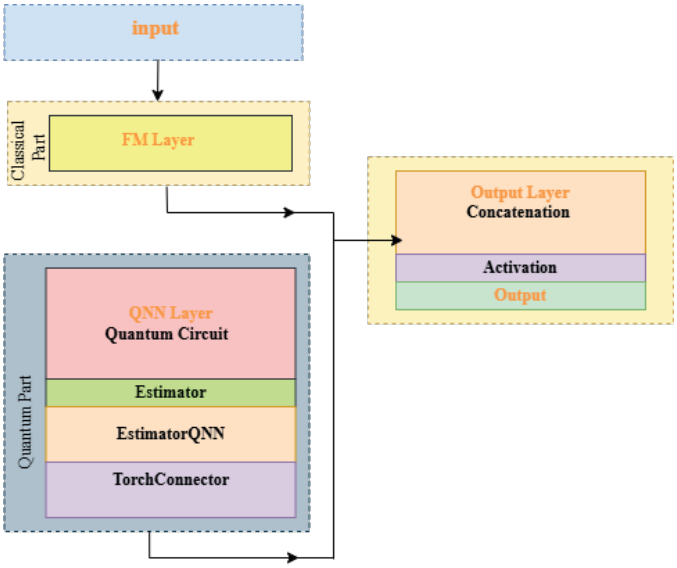

Fig. 1: Proposed $Pure - HQML$ Model Architecture for IDS in IIoT.

The $Pure - HQML$ model is a hybrid quantum-classical architecture designed to enhance predictive learning tasks by combining classical factorization machine (FM) layers with quantum neural networks (QNNs). As shown in figure 1, it begins with a classical FM layer implemented using a fully connected neural network, which processes the input features to model linear feature interactions. A quantum circuit, built using the RealAmplitudes circuit with parameterized rotations and linear entanglement, extracts quantum features from the input. This quantum output is processed by an EstimatorQNN, which utilizes the SparsePauliOp observable and a quantum estimator to evaluate the expectation values of the quantum

state. The quantum neural network is integrated with the classical framework through the TorchConnector, allowing the quantum weights to be optimized along with the classical ones. In the forward pass, the outputs of both the FM layer and the quantum network are concatenated and passed through a final linear output layer, producing a prediction that is activated by a sigmoid function. This hybrid approach captures both classical and quantum feature interactions, potentially improving accuracy for tasks involving complex data. The $Pure{-}HQML$ model offers a novel way to leverage quantum computing for machine learning tasks while maintaining the interpretability and structure of classical models.

III. Performance Evaluation and Discussion

The proposed $Pure - HQML$ model was developed using qiskit machine learning version 0.8.2. The proposed model run on Pytorch environment with NVIDIA GeForce RTX 4060 GPU, 64 GB RAM, Intel(R) Core (TM) i7-14700F 2.10 GHz machine on a Windows 10 operating system.

The performance of $Pure{-}HQML$ framework is evaluated using WUSTL-IIOT-2021 dataset [6]. This dataset capture real-world IIoT network operations and frequent attack in IIoT network. This dataset contains is highly imbalanced data total 1,194,464 samples and 48 features. ANOVA F-test select 10 features based on the score.

TABLE I: Parameter Configuration for Simulation Environment

Parameter Configuration	Values
Quantum Framework	Qiskit Machine Learning 0.8.2
Optimizer	Adam
Loss Function	Binary Cross Entropy
Number of Epoch	10

Table I shows the simulation parameter. The model achieved a training loss of 0.3108 and an accuracy of 98.40%, alongside a validation loss of 0.2623 with an accuracy of 98.63%. On the test set, the model yielded a loss of 0.3202 and an accuracy of 98.43%, all within a training duration of only 10 epochs.

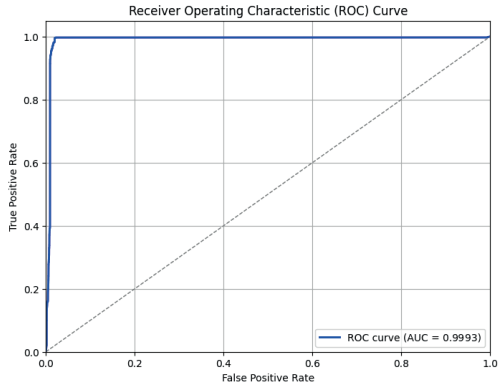

Fig. 2: ROC score for validation data.

Figure 2 and 3 demonstrate the receiver operating characteristic (ROC) curve performance of the proposed model on the validation and test dataset respectively. Figure 2 shows the the classification performance with an areas under the curve (AUC) of 0.9993. Similarly, the ROC curve in the figure 3 proof of the predictive capability with an AUC of 0.9977.

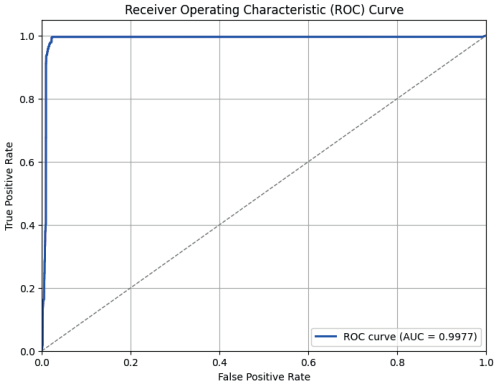

Fig. 3: ROC score for test data.

IV. Conclusion

This paper proposes a hybrid quantum machine learning model for network intrusion detection for industrial IoT. The proposed model has two parts quantum and classical are combined together in the output layer. This hybrid approach enables practical utilization of near-term quantum devices, offering promising improvements in learning performance and computational speed. The proposed model outperforms benchmark models by achieving an accuracy of 98.63%, a loss of 0.2623, and an ROC score 98.77%.

Acknowledgment

This work was supported in part by the Ministry of Science and ICT (MSIT), Korea, under the Innovative Human Resource Development for Local Intellectualization program, supervised by the Institute for Information and Communications Technology Planning and Evaluation (IITP) (IITP-2025-RS-2020-II201612, 34%) in part by the Priority Research Centers Program (2018R1A6A1A03024003, 33%), in part by the Information Technology Research Center (ITRC) (IITP-2025-RS-2024-00438430, 33%)

References

[1] A. Zainudin, L. A. C. Ahakonye, R. Akter, D.-S. Kim, and J.-M. Lee, "An efficient hybrid-dnn for ddos detection and classification in software-defined iiot networks," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8491–8504, 2023.

[2] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Scada intrusion detection scheme exploiting the fusion of modified decision tree and chi-square feature selection," *Internet of Things*, vol. 21, p. 100676, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660522001573

[3] A. Zainudin, R. Akter, D.-S. Kim, and J.-M. Lee, "Federated learning inspired low-complexity intrusion detection and classification technique for sdn-based industrial cps," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2442–2459, 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] M. Liu, J. Liu, R. Liu, H. Makhanov, D. Lykov, A. Apte, and Y. Alexeev, "Embedding learning in hybrid quantum-classical neural networks," in *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2022, pp. 79–86.

[6] M. Zolanvari, "Wustl-iiot-2021," 2021. [Online]. Available: https://dx.doi.org/10.21227/yftq-n229