When the Future Attacks the Past: QML for Anomaly Detection against SNDL Threats in IIoT

Mohtasin Golam, Jae-Min Lee, and Dong-Seong Kim
ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, South Korea
(gmoh248, ljmpaul, and dskim)@kumoh.ac.kr

***Abstract*—The rapid emergence of quantum computing introduces unprecedented risks to current cryptographic infrastructures, particularly through the Store-Now-Decrypt-Later (SNDL) paradigm, posing serious threats to long-term industrial data. This research proposes a Quantum Machine Learning (QML) framework for identifying SNDL-related anomalies in Industrial Internet of Things (IIoT) networks. Leveraging quantum feature spaces and hybrid quantum–classical models, QML identifies subtle, high-dimensional irregularities in encrypted traffic and access behavior that are often missed by classical systems. The proposed approach combines QML-based anomaly detection and post-quantum cryptography methods, providing proactive protection against quantum-era data harvesting. This study introduces QML as a foundation for quantum-resilient cybersecurity, assuring data integrity and providing future-proof protection for IIoT infrastructure.**

***Index Terms*—Anomaly detection, Quantum machine learning (QML), and Store-Now-Decrypt-Later (SNDL).**

I. Introduction

The advent of large-scale quantum computing marks a significant transformation in computational capabilities, undermining the core security assumptions of classical cryptographic systems. Quantum algorithms such as Shor's and Grover's substantially reduce the computational difficulty of integer factorization and symmetric-key search, respectively, thereby rendering traditional public-key cryptosystems, including RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and Diffie–Hellman, vulnerable to compromise [1]. In this shifting threat environment, the Store-Now-Decrypt-Later (SNDL) model has emerged as a prominent attack vector, in which adversaries capture and archive encrypted communications with the intention of decrypting them once sufficient quantum computational resources become available [2]. This deferred-decryption strategy is particularly consequential in the context of the Industrial Internet of Things (IIoT), where critical telemetry, control commands, and proprietary data are retained for extended periods. The enduring sensitivity of industrial data, coupled with the widespread use of resource-limited edge devices, heightens the risk of SNDL attacks that threaten the confidentiality and longevity of operational information [3].

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (IITP-2026-RS-2020-II201612, 40%), the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2018R1A6A1A03024003, 30%), and supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(RS-2025-25431637, 30%)

A robust defensive paradigm is essential to counteract quantum decryption and to anticipate and detect pre-quantum adversarial activities. Within this framework, Quantum Machine Learning (QML) offers a promising solution for anomaly detection in encrypted or high-dimensional IIoT data streams [4]. By leveraging Hilbert-space feature embeddings, quantum kernel estimators, and variational quantum circuits (VQCs), QML enables the identification of nonlinear correlations that classical learning models struggle to efficiently resolve. This research proposes a QML-based anomaly-detection framework integrated with post-quantum cryptographic protocols to detect latent indicators of SNDL reconnaissance, including abnormal key-exchange frequencies, anomalous ciphertext entropy, and deviations in quantum-resistant handshakes. The objective is to develop a hybrid quantum–classical detection pipeline that enhances real-time situational awareness and strengthens the quantum resilience of IIoT infrastructures, thereby providing early warning against SNDL-driven data exploitation before the emergence of full-scale quantum attacks.

II. Proposed Methodology

A. System Overview

The proposed framework employs a QML-based anomaly-detection system to identify Store-Now-Decrypt-Later (SNDL) threats in IIoT networks. The architecture comprises five layers: data acquisition, preprocessing, quantum feature encoding, QML-based analysis, and decision-making. Data streams from IIoT nodes, including encrypted communication logs and network telemetry, are preprocessed and normalized. These processed inputs are transformed into quantum-compatible formats to facilitate feature embedding within a high-dimensional Hilbert space. A hybrid QML model, integrating quantum and classical components, conducts feature correlation analysis and assigns anomaly scores. The decision layer subsequently determines anomaly probabilities and flags potential SNDL-preparatory activities for further investigation.

B. Quantum Feature Encoding

In this layer, classical IIoT data vectors are transformed into quantum states using unitary transformations. For a normalized data vector $x \in \mathbb{R}^n$, the encoding process generates a quantum state as

$$\psi(x)\rangle = U(x)|0\rangle^{\otimes n}, \tag{1}$$

where $U(x)$ denotes a unitary operation that maps classical features to quantum amplitudes or angles. **Amplitude**

TABLE I: Performance Comparison between Classical and Quantum Models on the CICIoT2023 Dataset

Model	Accuracy (%)	F1 Score	ROC	Training Time (s)	Inference Time (s/sample)	Qubit Count	Scaling Complexity
Classical SVM	89.53	0.88	0.91	42.1	0.012	N/A	$O(n^2)$
Random Forest	91.36	0.90	0.93	58.7	0.015	N/A	$O(n \log n)$
QSVM	**94.07**	**0.94**	**0.97**	**73.4**	**0.007**	**8**	$O(\log n)$
VQC	**94.74**	**0.95**	**0.98**	**81.2**	**0.008**	**10**	$O(\log n)$

encoding allows efficient representation of high-dimensional data with fewer qubits, whereas **Angle encoding** enhances interpretability for features associated with anomalies. This approach enables the QML model to leverage quantum parallelism to learn complex inter-feature dependencies from encrypted and unknown data streams.

C. Quantum Model Design

The anomaly detection layer employs a hybrid QML model comprising Variational Quantum Circuits (VQCs) and Quantum Support Vector Machines (QSVMs). For the QSVM, the decision function is based on a quantum kernel defined as

$$K(x_i, x_j) = |\langle \phi(x_i) | \phi(x_j) \rangle|^2, \tag{2}$$

which measures the inner product of two data points embedded in the quantum Hilbert space. In the VQC, a parameterized quantum circuit learns to minimize a loss function

$$L(\theta) = \sum_i \ell(f_\theta(x_i), y_i), \tag{3}$$

where $f_\theta(x_i)$ denotes the model's predicted anomaly score and ℓ is a differentiable cost function. The circuit parameters θ are optimized using a classical optimizer, such as Adam, thereby establishing a feedback loop between the quantum and classical subsystems.

D. Hybrid Optimization and Detection Logic

The hybrid optimization process integrates quantum inference with classical gradient-based updates. During training, the quantum processor executes parameterized circuits, and the classical processor iteratively adjusts parameters to minimize the anomaly-detection loss. The system's decision rule is expressed as

$$A(x) = \begin{cases} 1, & \text{if } f(x) > \tau, \\ 0, & \text{otherwise,} \end{cases} \tag{4}$$

where $f(x)$ represents the model's anomaly score and τ is the threshold derived from training distributions. A value of $A(x) = 1$ indicates a potential SNDL-related anomaly. The hybrid model operates continuously on encrypted IIoT traffic, providing a proactive defense mechanism that flags anomalous data patterns indicative of quantum-preparatory data harvesting.

III. Performance Evaluation

Table I demonstrates that QML models substantially outperformed classical approaches in detecting Store-Now-Decrypt-Later (SNDL) threats within the Industrial IIoT ecosystem. Both the QSVM and VQC achieved 94% accuracy, exceeding classical baselines and maintaining higher F1-scores (0.94–0.95) and ROC values (0.97–0.98). These findings suggest enhanced sensitivity and precision in identifying subtle, encrypted anomalies characteristic of pre-quantum reconnaissance. While QML models required marginally longer training times, **logarithmic scaling**, with $O(\log n) \approx 10$–20, for datasets with 10^3–10^6 features, enabling efficient real-time anomaly detection in large-scale IIoT networks. This combination of detection accuracy and computational efficiency underscores the potential of QML as a scalable, quantum-resilient defense mechanism against emerging SNDL-based cyber threats in industrial settings.

A. Security Resilience

The proposed QML-based system enhances security through a two-tiered approach. First, pattern-based anomaly detection applied to encrypted, previously unseen data reduces the risk of adversarial reconnaissance prior to SNDL attacks. Second, quantum-enhanced kernel mappings render it computationally infeasible for classical attackers to replicate the model's behavior, thereby intrinsically obscuring the detection logic. This hybrid architecture is operationally feasible on current Noisy Intermediate-Scale Quantum (NISQ) devices and aligns near-term QML capabilities with the long-term objective of achieving quantum-resilient security in IIoT networks.

IV. Conclusion

This research proposed a QML framework to detect Store-Now-Decrypt-Later (SNDL) threats in IIoT networks. The QSVM and VQC models achieved superior results on the CICIoT2023 dataset, with accuracies exceeding 94%, F1-scores of 0.95, and ROC values of 0.98, surpassing classical baselines. Quantum feature embeddings allowed these models to identify complex, nonlinear relationships within encrypted network traffic. Furthermore, logarithmic inference scaling $O(\log n)$) enabled efficient analysis of high-dimensional IIoT data. These results suggest that QML provides a scalable and quantum-resilient solution for proactive anomaly detection against emerging SNDL-based cyber threats.

References

[1] A. Sahoo, I. K. AK, and S. M. Rajagopal, "Comparative study of cryptographic algorithms in post quantum computing landscape," in *2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*. IEEE, 2024, pp. 36–40.

[2] W. Allgyer, T. White, and T. A. Youssef, "Securing the future: A comprehensive review of post-quantum cryptography and emerging algorithms," *SoutheastCon 2024*, pp. 1282–1287, 2024.

[3] M. Golam, M. M. Alam, M. R. Subhan, D.-S. Kim, and J.-M. Lee, "Blind-twin: Blockchain-assisted llm-based cds for digital twin-enhanced industrial aiot," in *ICC 2025-IEEE International Conference on Communications*. IEEE, 2025, pp. 4981–4986.

[4] E. A. Tuli, M. Golam, M. M. H. Somrat, R. Khafagy, and D.-S. Kim, "Hybrid quantum machine learning for detecting gps spoofing attacks in military mission," in *2025 International Conference on Mobile, Military, Maritime IT Convergence (ICMIC)*, 2025, pp. 190–193.