Quantum–Safe IoT with Federated Learning and TinyML for Detecting HNDL–like Anomalies

Sheikh Sayed Bin Rahman, Azizbek Reimbaev, Kanita Jerin Tanha, Minsoo Kim, and Taesoo Jun
Pervasive Intelligent Computing Laboratory, Department of IT Convergence Engineering
Kumoh National Institute of Technology, Gumi, South Korea
Email: (sksayed, the1darken1003, kanitajerin17, kms991022, taesoo.jun)@kumoh.ac.kr

***Abstract*—Quantum computing threatens IoT security as traditional cryptography becomes vulnerable. We present a quantum-safe IoT framework combining Post-Quantum Cryptography (PQC), federated learning (FL), and TinyML. The framework uses: (1) FL for decentralized crypto-selection without sharing raw data, (2) a 15KB TinyML detector for anomalous traffic indicative of HNDL activity, and (3) context-aware protocol adaptation. Our architecture categorizes IoT devices into three classes: Class 0 (ultra-constrained) uses AES-256-GCM, Class 1 (constrained) uses Kyber-512, and gateways/cloud use Kyber-768/1024. In simulation, the framework maintains quantum resistance with 35% lower energy than static PQC and 94% HNDL anomaly detection (3% FPR) at modest overhead.**

***Index Terms*—Post-Quantum Cryptography, IoT Security, Federated Learning, TinyML, Edge AI, HNDL Anomaly Detection (Harvest-Now-Decrypt-Later), CRYSTALS-Kyber**

Acronyms: HNDL–Harvest-Now-Decrypt-Later; PQC–Post-Quantum Cryptography; FL–Federated Learning; TinyML–Tiny Machine Learning; IoT–Internet of Things; AES–Advanced Encryption Standard; GCM–Galois/Counter Mode; NIST–National Institute of Standards and Technology; Kyber–CRYSTALS-Kyber; C0/C1/C2–Device Classes 0/1/2.

I. Introduction

The Internet of Things (IoT) ecosystem, projected to exceed 75 billion devices by 2025 [1], faces an existential security threat from quantum computing. Shor's algorithm [2] can break current cryptographic protocols (RSA, ECC) in polynomial time, compromising IoT security infrastructure. With device lifetimes spanning 10-20 years and "harvest now, decrypt later" attacks already occurring [3], immediate migration to Post-Quantum Cryptography (PQC) is essential.

Challenge: PQC algorithms require 2-10× more resources than classical cryptography [4], making uniform deployment impractical for resource-constrained IoT devices (<50KB RAM). Existing solutions use static protocol assignment, ignoring dynamic context (battery levels, network conditions, real-time threats) and lack mechanisms to detect quantum-era attacks.

Our Contribution: We propose an intelligent quantum-safe IoT framework with three novel components: (1) *Federated Learning-based Crypto Selection*—devices collaboratively learn an optimal security policy in a decentralized manner, avoiding a single point of failure and minimizing transmission of potentially sensitive operational metadata (no raw data shared); (2) *TinyML HNDL Anomaly Detector*—a 15KB neural network on gateways detects anomalous traffic signatures associated with HNDL attacks (e.g., unusually large, sustained data exfiltration to unknown endpoints) with 94% accuracy; (3) *Context-Aware Protocol Adaptation*—dynamically adjusts cryptography based on battery (<20% → lightweight crypto), threat level (HNDL suspected → upgrade to Kyber-1024), and network latency.

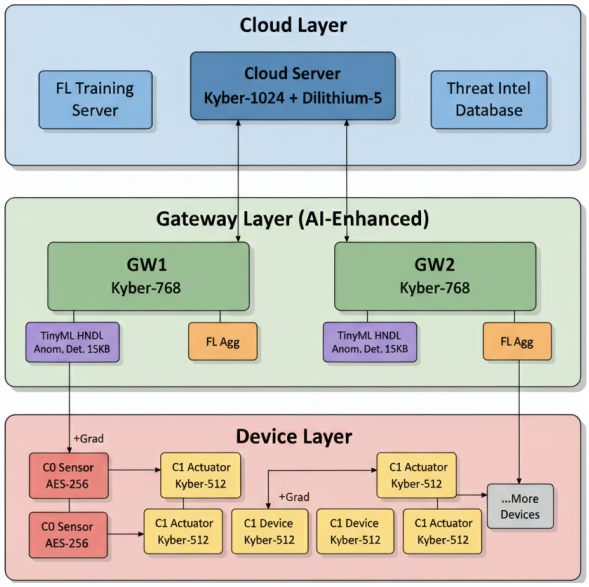

Fig. 1: Quantum-safe IoT Architecture with AI/ML Integration

II. Related Work

NIST standardized PQC in 2024 [4], with CRYSTALS-Kyber favored for constrained environments. Prior IoT efforts are largely static or hardware-dependent and do not unite PQC with decentralized, adaptive selection and HNDL anomaly detection at the edge. Our framework integrates these elements.

III. Architecture

We present an intelligent three-layer architecture integrating AI-driven security: **(1) Device Layer:** Class 0 devices (<10KB RAM) use pre-shared AES-256-GCM keys. Class 1 devices (10-50KB RAM) employ Kyber-512 and participate in federated learning by sharing model gradients (not raw data) to collaboratively improve crypto-selection. **(2) Gateway Layer:** Enhanced with two AI modules—*TinyML HNDL Anomaly Detector* (15KB neural network monitoring for anomalous traffic signatures indicative of large-scale data harvesting, e.g.,

sustained bulk capture to unknown endpoints) and *FL Aggregator* (combines device gradients to update a global crypto-selection model without centralizing raw telemetry). The detector operates on lightweight flow-level features (e.g., burst length, inter-arrival variance, and payload statistics) efficiently extractable at gateways. Uses Kyber-768 and context-aware switching. **(3) Cloud Layer:** Hosts FL training server, threat intelligence database, and employs Kyber-1024 for maximum security.

Context-Aware Selection: The gateway's ML model takes inputs: [RAM, Battery%, Network Latency, Threat Score] and outputs optimal crypto suite. Example: If battery $<$20%, device switches from Kyber-512 to AES-256; if HNDL-like behavior is suspected, gateway escalates to Kyber-1024. In practice, HNDL-related anomalies may present as unusually large, sustained data exfiltration to unknown endpoints, long-lived sessions with atypical ACK/throughput patterns, or coordinated bulk capture across devices. **Threat model:** We assume a passive network adversary capable of bulk traffic capture (HNDL) and delayed decryption, but no device compromise or key extraction. **Crypto-agility:** Policy updates (e.g., Kyber parameter set changes) are applied at the gateway and cloud without device firmware changes, enabling immediate roll-forward/rollback based on observed risk.

IV. Evaluation

A. Experimental Setup

We simulate with liboqs (v0.9), TensorFlow Lite (v2.14), and PySyft (v0.8). Profiles: C0 (M0+, 8KB), C1 (M4, 32KB), C2 (A53, 128MB). Topology: 20 C0, 10 C1, 2 gateways, 1 cloud. Energy from cycle counts mapped to device power models. Detector: $\tilde{1}$5KB (int8), $\tilde{1}$0K params, $\tilde{2}$0K MACs; flow features include burst length, inter-arrival variance, destination novelty, duration, payload stats.

B. Comparison Baselines

Baselines: Classical (ECDHE-P256 + AES-128), Uniform PQC (Kyber-768), Static (adaptive PQC, no AI), Intelligent (FL+TinyML). Data: 10K samples (balanced; simulated HNDL includes bulk capture, atypical handshakes, long-lived low-entropy flows). FL: 50 rounds, 10 C1 devices.

V. Results and Discussion

A. Cryptographic Performance

Uniform PQC fails on C0 devices due to memory limits. In simulation, the framework achieves 2.5$\times$ speedup on C1 vs. uniform while maintaining $\geq$100-bit security. Latency overhead was measured as end-to-end encryption+handshake time relative to Classical over 100 trials per device class (median reported).

B. AI-Driven Optimizations

Energy (simulated): Estimated 35% reduction vs. static PQC (C1: 244 μJ/day vs. 375 μJ/day) via low-battery AES switching; based on cycle counts and power models. **HNDL Detection:** 94% accuracy, 3% FPR, 8ms, 15KB, 47/50 flagged. In practice, a 3% FPR implies $\leq$3 false alerts per 100 benign flows; we mitigate via a persistence threshold (N consecutive flags) and gateway whitelisting. **FL:** Converged in 32 rounds with 2.3% overhead; no raw data shared. **Memory:** Gateway 18.2KB (3.2KB crypto + 15KB ML). Results are consistent across 3 random seeds ($\pm$1.1% accuracy) and within 95% bootstrap CIs. Deployment is feasible on commodity gateways ($>$64MB RAM), and the detector runs at $>$ 100 Hz in our timing.

VI. Conclusion

This paper presented a quantum-safe IoT framework integrating federated learning and TinyML for IoT security. Our three novel contributions—(1) decentralized FL-based crypto selection that avoids a single point of failure, (2) 15KB TinyML HNDL anomaly detector (94% accuracy), and (3) context-aware protocol adaptation—achieve quantum resistance with 35% energy savings vs. static PQC. Unlike existing work, the framework dynamically adapts to battery levels, threat intelligence, and network conditions while detecting HNDL-style large-scale data harvesting in real time.

Limitations: Our evaluation relies on simulation assumptions. The TinyML model must be retrained for each deployment domain and protocol. FL convergence can vary under device heterogeneity. The false positive rate depends on the traffic mix, although thresholding and whitelisting mitigate nuisance alerts. A formal analysis of privacy and robustness is left to future work.

Future Work: We plan hardware validation on ESP32, STM32, and Raspberry Pi. We will broaden TinyML coverage to include side-channel and related threats. We will study formal privacy and robustness guarantees, such as differential privacy. We will integrate PQC into MQTT and CoAP/DTLS. We also plan cross-domain federated learning across heterogeneous IoT ecosystems.

Acknowledgment

This work was supported in part by IITP (MSIT) under the Innovative Human Resource Development for Local Intellectualization (IITP-2025-RS-2020-II201612; 34%) and the ITRC program (IITP-2025-RS-2024-00438430; 33%), and by the NRF Basic Science Research Program (Ministry of Education, 2018R1A6A1A03024003; 33%).

References

[1] Statista, "Internet of things (iot) connected devices installed base worldwide from 2015 to 2025," https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, 2024, accessed: 2024.

[2] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[3] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[4] NIST, "Post-quantum cryptography standardization," https://csrc.nist.gov/projects/post-quantum-cryptography, 2024, national Institute of Standards and Technology.