Post-Quantum

Cryptography Conference

Implementing Hybrid TLS with ML-KEM-768 for Post-Quantum Security in Mobile IIoT Deployments

Danny Setyowati
Cyber Defense Graduate Scholar

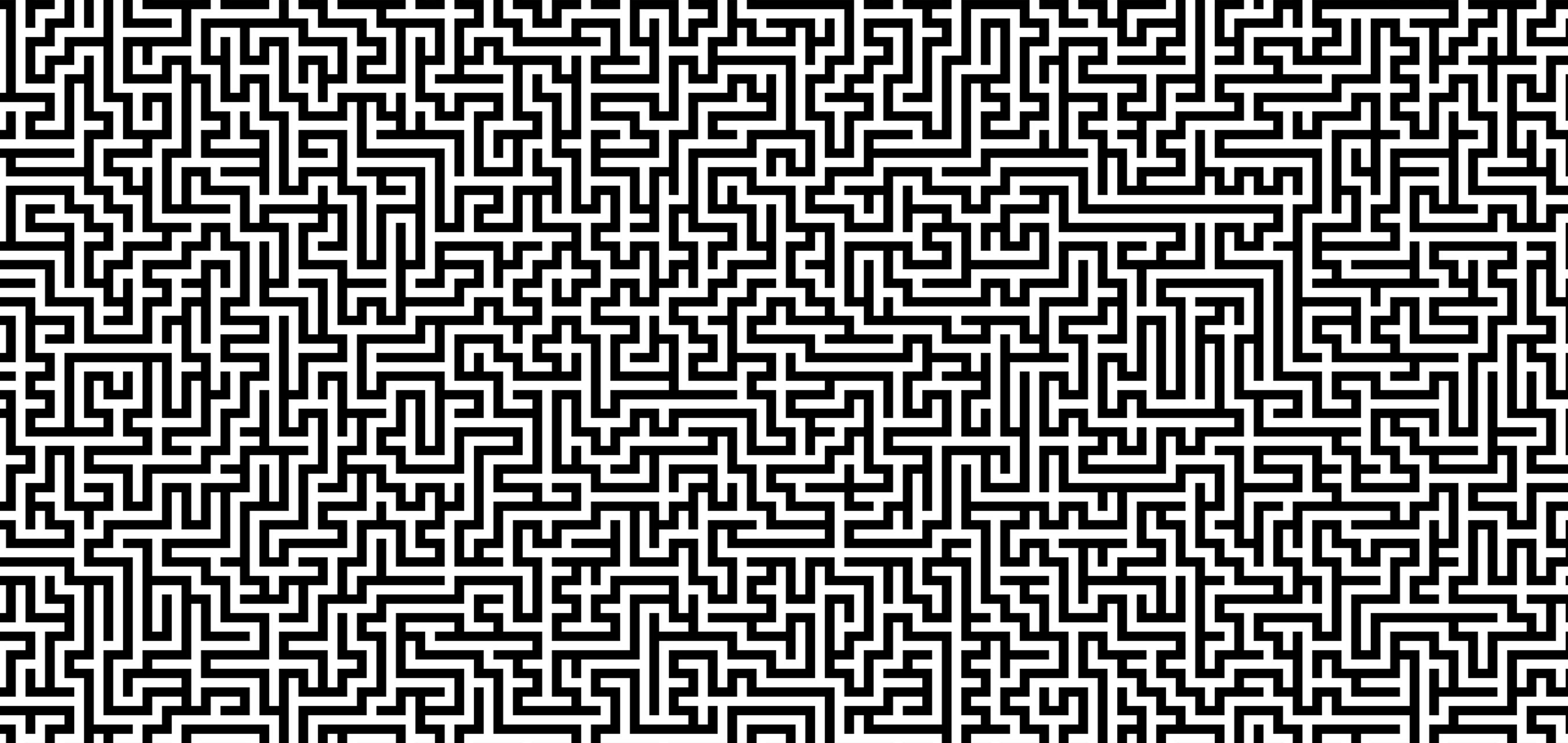
KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

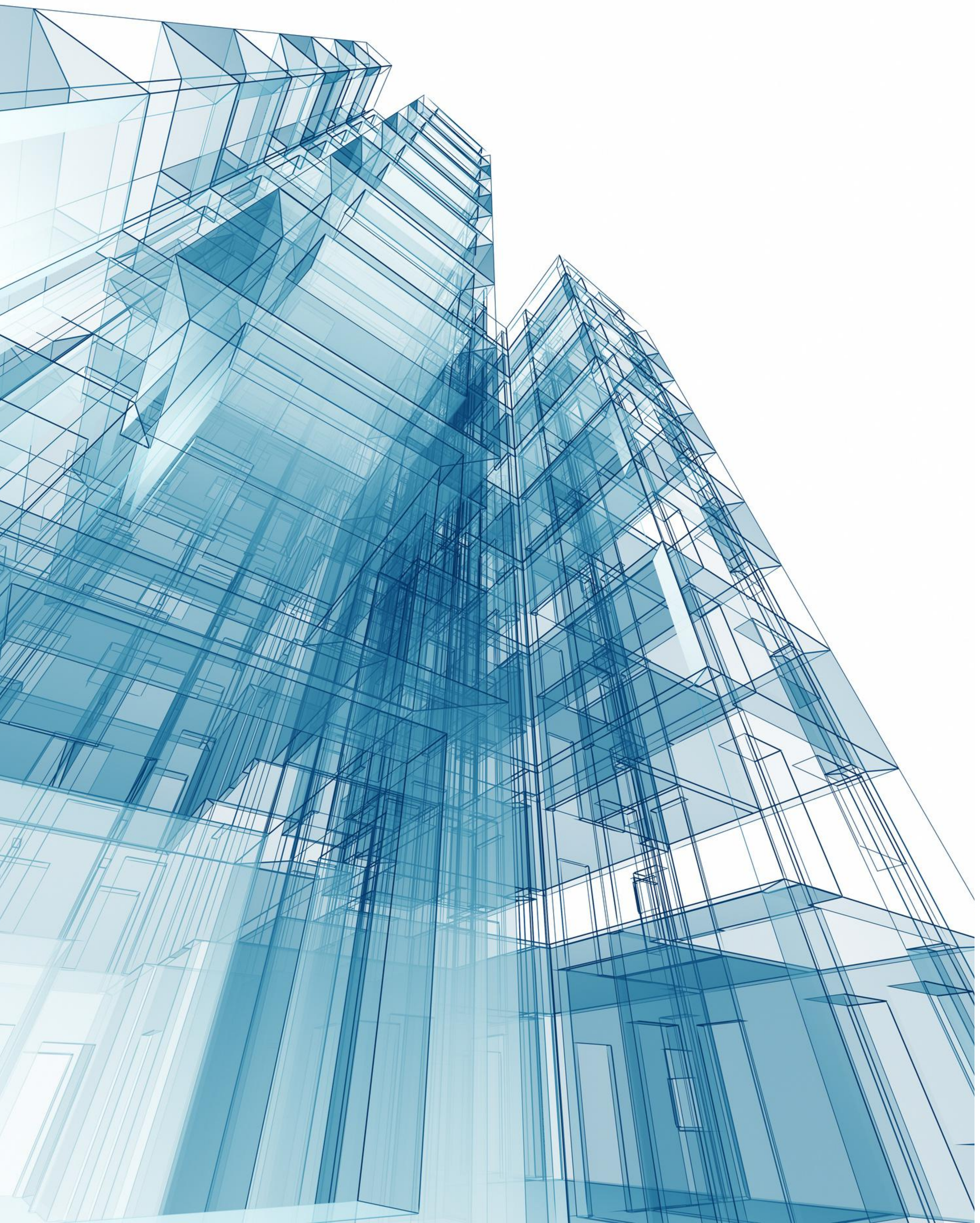
Republic of Indonesia Defense University

Implementing Hybrid TLS with ML-KEM-768 for Post-Quantum Security in Mobile IIoT Deployments

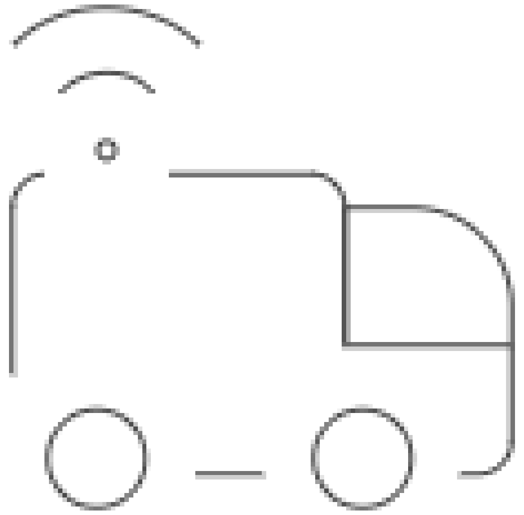


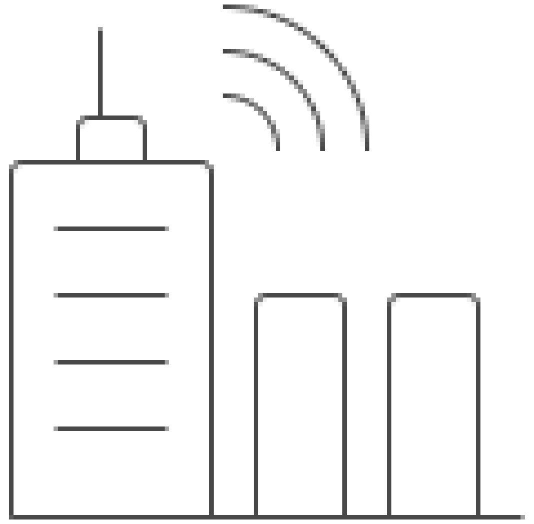
- Quantum computing threatens the foundations of digital trust.
- Industrial IoT (IIoT) systems, like mobile manufacturing trucks are especially vulnerable.
- These trucks rely on real-time secure communication with a central SOC.
- But traditional TLS (RSA, ECDHE) isn’t quantum-safe.

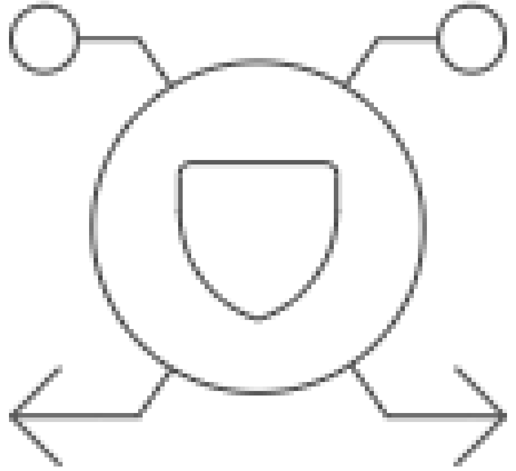
- Integrate ML-KEM-768 (NIST FIPS 203 standard) into TLS as a hybrid handshake.
- Test its performance and security in a simulated mobile IIoT environment.
- Verify compliance with IEC 62443 security standards.



System Components







Mobile Manufacturing Truck

Node-RED generates sensor data for the system.

Security Operations Center

Mosquitto MQTT broker with Python subscriber for data.

PQC-Dev Oracle

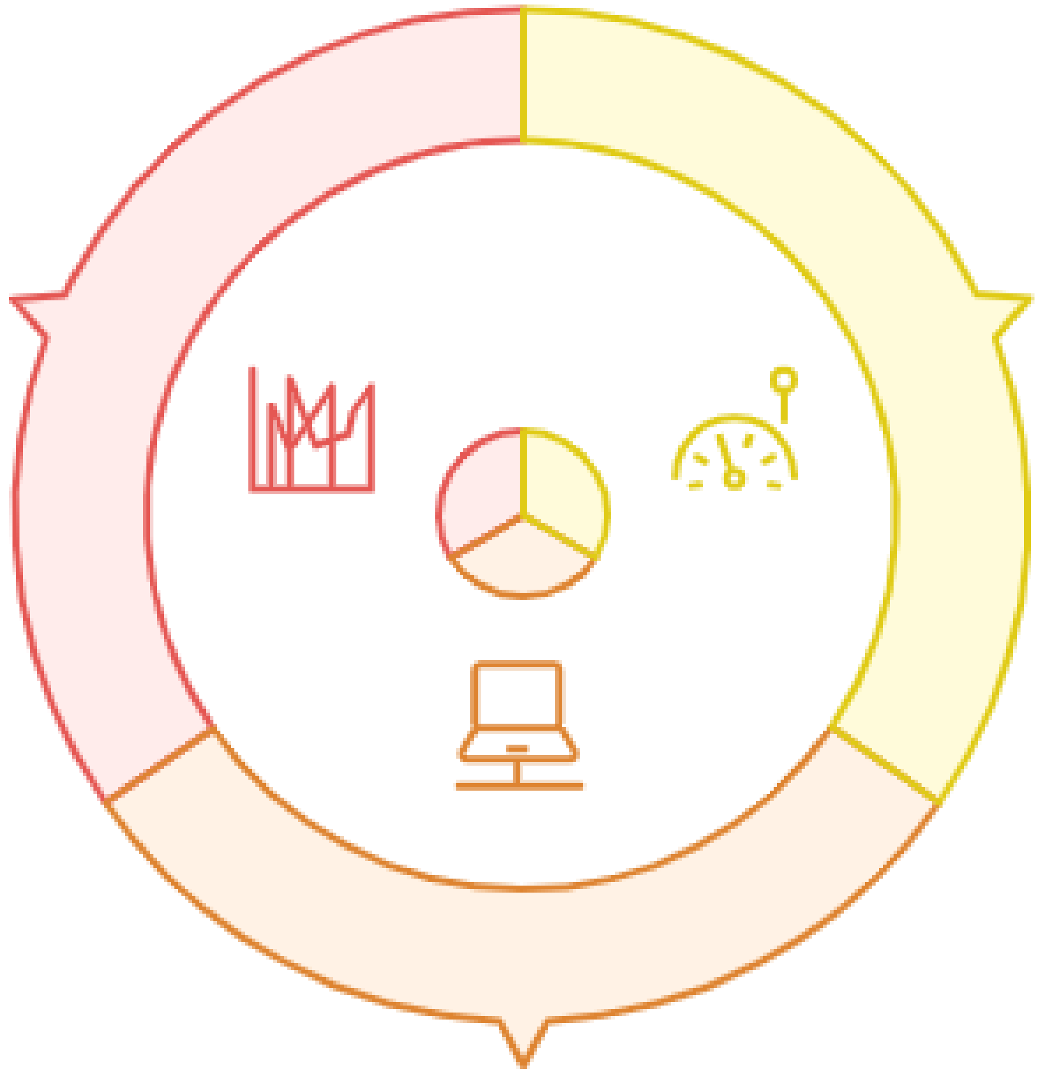
Lightweight C-based service running ML-KEM-768 encryption.

- Virtual testbed with 3 VMs.
- End-to-end latency measured from data generation to decapsulation.
- CPU load monitored across devices.
- Simulated attacks: MITM and DoS to test resilience.

System Performance Metrics

Outlier Latency

Occasional outliers around 400 ms represent realistic mobile network jitter. The system maintains stability despite these fluctuations.



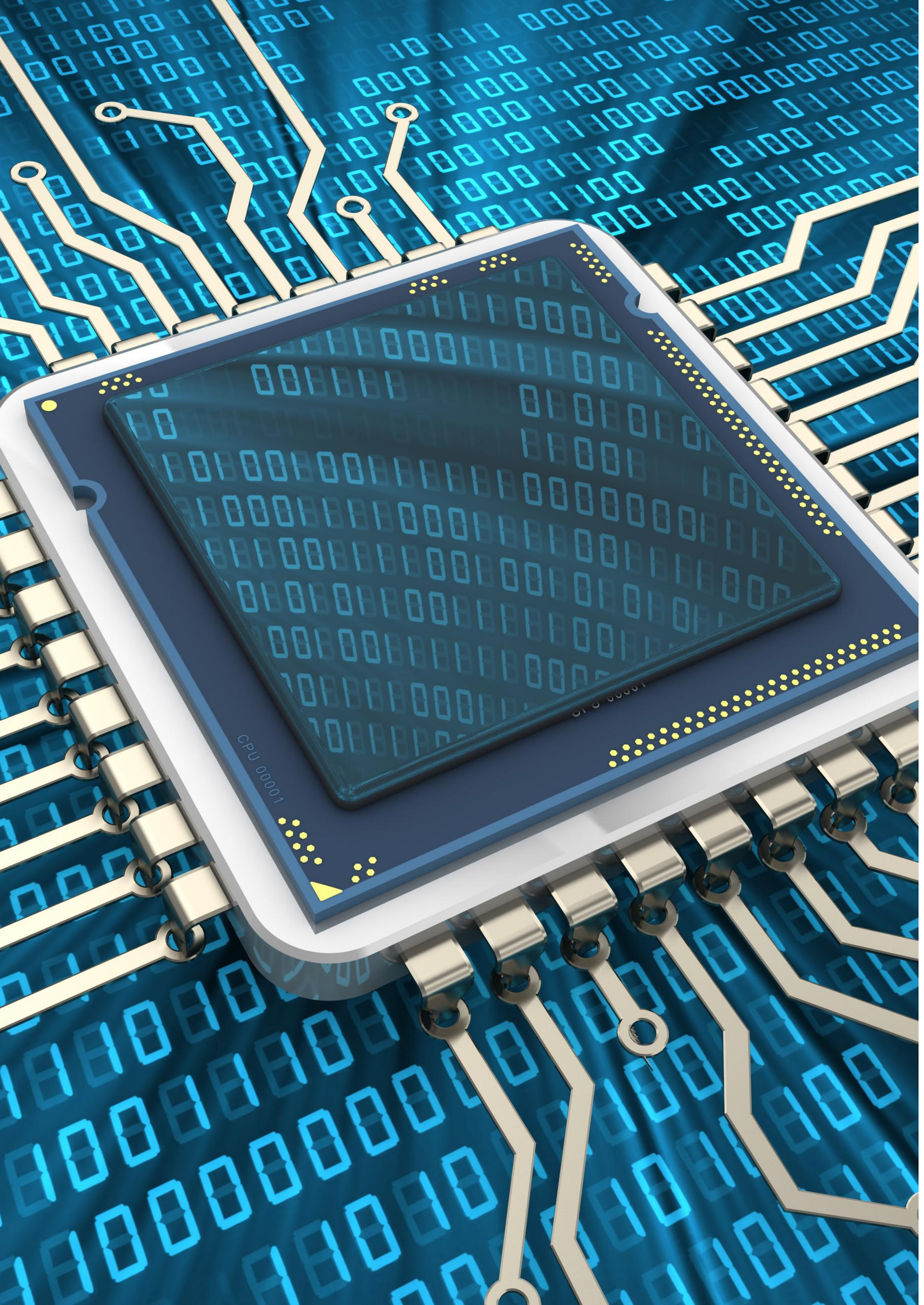
Latency Threshold

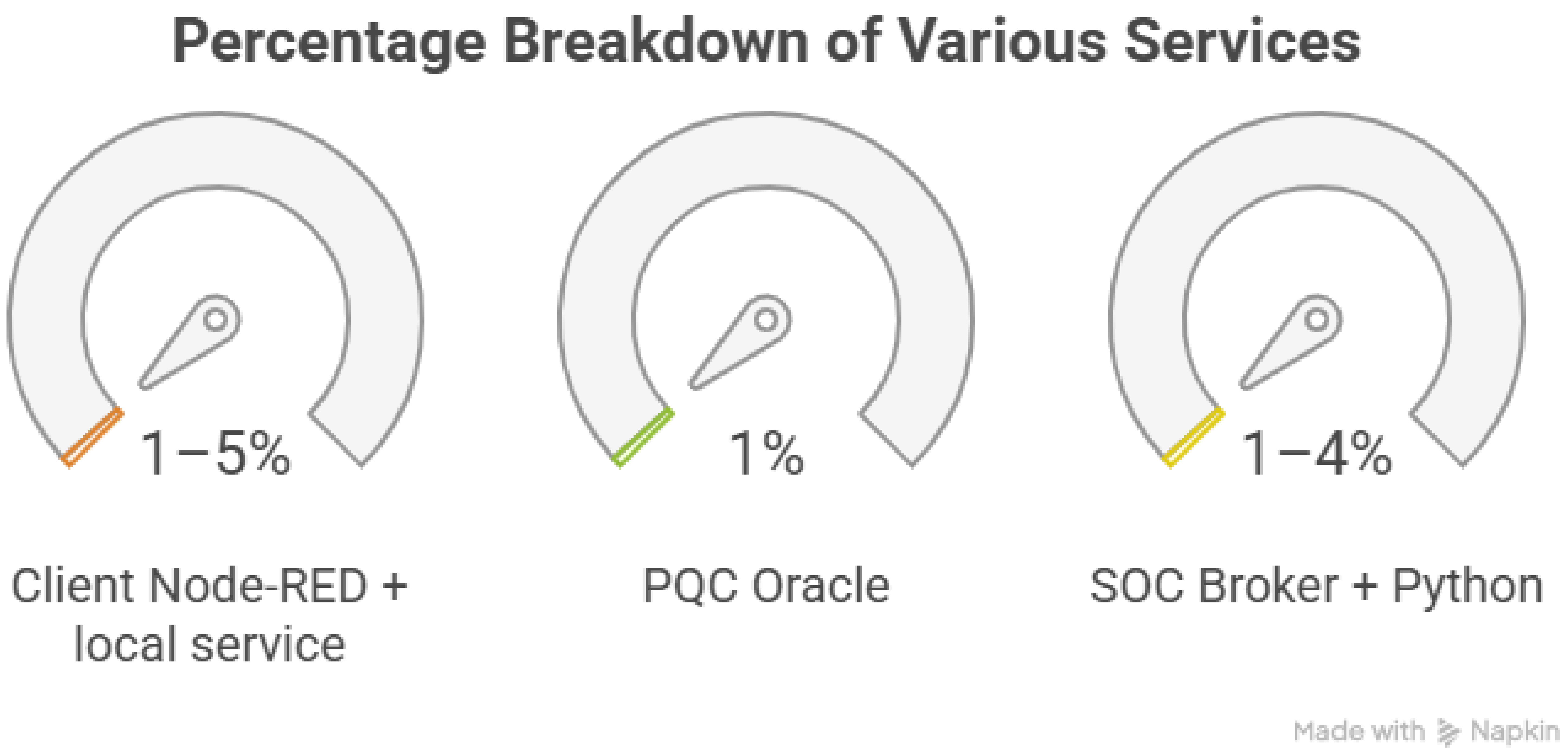
The system maintains latency well below the 300 ms threshold. This is crucial for real-time industrial applications.

Packet Latency

Ninety percent of data packets experience latency under 150 ms. This indicates efficient and reliable performance.

Mean end-to-end latency: 108.8 ms




Percentage Breakdown of Various Services
1–5%
Client Node-RED + local service
1%
PQC Oracle
1–4%
SOC Broker + Python
Made with Napkin

- MITM attack simulation → channel integrity preserved.
- DoS simulation → system failed gracefully, auto-recovering with state restoration.
- PQC-hybrid design prevents unauthorized data decryption even under duress.

- PQC integration is feasible in real-time mobile IIoT.
- Hybrid TLS ensures backward compatibility while resisting future quantum threats.
- Aligns with IEC 62443 defense-in-depth strategies.
- Provides a practical blueprint for quantum-safe industrial deployments.

- Validate on physical embedded devices (ARM SBCs, gateways).
- Add PQC digital signatures (e.g., ML-DSA) for authentication.
- Integrate with AI-driven anomaly detection at the SOC.

“Innovation means preparing not just for today’s attacks, but tomorrow’s quantum threats”