Quantum Adversarial AI in Secure IoT Networks

Background & Motivation

QPA Research Group

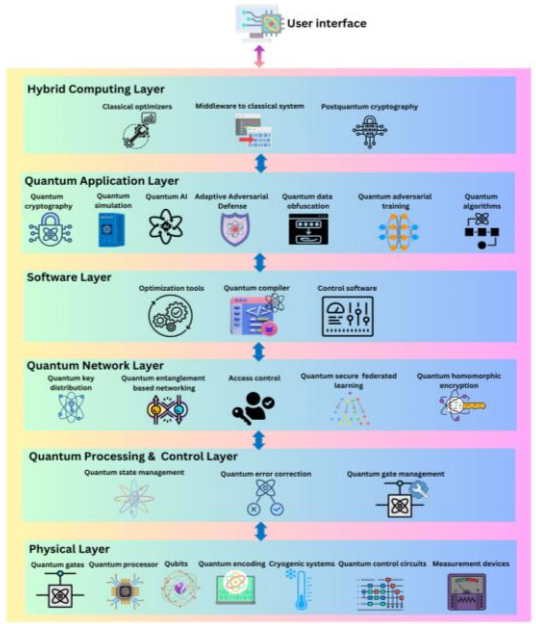
- AI-enabled IoT expands the attack surface across heterogeneous devices, communications, and security models; quantum computing may amplify adversarial attacks.
- Attacks manipulate training data, quantum states, models, decision boundaries, or outputs through causative, exploratory, and inference techniques.
- Resilient IoT requires coordinated quantum, post-quantum, and adversarial-AI defenses across the full computing stack.

Şafak, I., Frantti, T., Alagöz, F., Mikkonen, T., & Haghparast, M. (2026). Quantum adversarial artificial intelligence in secure internet of things networks. In *Adversarial Example Detection and Mitigation Using Machine Learning* (pp. 125-136). Cham: Springer Nature Switzerland.

https://doi.org/10.1007/978-3-031-99447-0_9

Attack-Defense Landscape and Reference Architecture

Reference quantum computing architecture



- **Attack surface:** Poisoning, backdoors, extraction, state perturbation, decision-boundary and inference attacks
- **Access levels:** white-box, gray-box, and black-box
- **Core defenses:** Adversarial training, quantum error correction, differential privacy, and randomized encodings
- **Secure communications:** Post-quantum cryptography, QKD, access control, and secure federated learning
- Six coordinated layers improve fault tolerance, performance, and security

Source: Safak et al., 2026, Fig. 9.2

GOAL: Resilient quantum-enabled IoT through coordinated attack detection, mitigation, and layered security