Toward Quantum-Ready IoT: A Layered Architecture for Lightweight, Post-Quantum and Quantum-Native Security

1. Introduction

With the prominence of quantum technologies, more and more research is being conducted at the intersection of quantum computing and cybersecurity [1]. Some works focus on post-quantum cryptography that can resist attacks from quantum computers [2, 3], while others try to build new types of secure systems by using the unique properties of quantum mechanics [4, 5]. However, building a complete quantum network still faces many challenges, especially in terms of infrastructure [6]. Compatibility is also a problem. For instance, 4G devices cannot leverage the capabilities of 5G networks due to fundamental differences in protocol and hardware. Similarly, most existing IoT devices lack the computational and physical means to accommodate quantum-native security protocols. Without carefully designed adaptation layers, they may become insecure and irreparable once quantum-safe standards are deployed at scale. On the other hand, IoT systems are already limited in their computing power and cannot run heavy cryptographic protocols [7, 8]. This makes them more vulnerable to attacks, and quantum threats will make the situation even worse. Therefore, we need security methods that are lightweight, future-proof, and can still work on existing IoT devices. Ideally, such methods should also be amenable to direct integration with quantum primitives, ensuring seamless alignment with emerging quantum infrastructures.
As quantum threats become increasingly real, the challenge is shifting from designing new cryptographic methods to making them work in practice—on small, outdated, and diverse IoT devices. Despite recent progress, many existing solutions are still too heavy or too specialised to be widely used on real-world devices with limited resources.

2. Related Work

Recent research has explored the possibility of deploying post-quantum cryptography in embedded systems by adapting lattice-based schemes for constrained environments. For instance, Bera et al. proposed a behavioural-biometric authentication system based on post-quantum primitives for healthcare devices [2], while Bagchi et al. developed a lattice-based multi-signature protocol intended for blockchain-integrated IoT networks [3]. These approaches achieve strong cryptographic guarantees, but they typically require relatively high computational resources or dedicated hardware modules, which are often unavailable in ultra-low-power devices. Parameswarath et al. [9] proposed a quantum-safe authentication protocol and demonstrated a computation latency below 1.3 ms. Nevertheless, the paper does not provide detailed quantification of the communication frame size or the memory footprint on embedded devices, so its suitability for bandwidth- and memory-constrained IoT nodes still requires further empirical validation.

Other studies take a different approach by designing authentication protocols that directly leverage quantum properties. In the quantum-native line, Bera et al. integrate BB84-based QKD into Quantum-IoT scenarios—including healthcare—providing information-theoretic keys at the cost of optical transceivers [4], while Khan et al. proposed Soteria, a device attestation scheme based on quantum state challenges [10]. While such protocols offer theoretically strong security, their reliance on quantum channels and quantum optical hardware makes them difficult

to integrate into mobile or low-cost devices. For example, Javed et al. applied quantum-enhanced provenance tracking to secure synchrophasor systems in smart grids [11], but their implementation is tightly coupled with static infrastructure such as fibre optics and cannot generalise to short-range or vehicular scenarios.

In the theoretical domain, a growing number of works have focused on foundational models for quantum authentication and pseudorandomness. The pseudorandom quantum authentication scheme introduced by Haug et al. [5] shows how minimal assumptions, such as pseudorandom unitary transformations, can still achieve semantic security under quantum attack models. Foundational work by Barnum et al. [12] and Curty et al. [13], conducted in the early 2000s, established the first formal frameworks for quantum and classical message authentication. While primarily theoretical and assuming idealised quantum channels, these studies laid the groundwork for modern formulations of quantum-secure authentication and inspired subsequent constructions under more realistic assumptions. Notably, Zhandry's recent work on quantum-secure PRPs [14] and unitary oracles [15] has contributed theoretical tools that are now being used to model the complexity and limits of quantum adversaries. These results offer a rich library of cryptographic primitives, but most are formulated without regard to system-level constraints such as power, memory, or latency.

Taken together, these contributions provide essential insights into both the strengths and limitations of quantum-safe authentication methods. However, a common challenge persists: how to translate theoretical security constructs into protocols that are truly lightweight, hardware-agnostic, and deployable across the vast diversity of modern IoT devices.

3. A Layered Security-Oriented Architecture for Quantum-Integrated IoT

To support quantum-enhanced security in resource-constrained IoT systems, a layered architecture is adopted, integrating physical infrastructure hierarchy with abstract functional planes. As illustrated in Figure 1, the system is organised across four spatial layers—Device, Edge, Fog, and Cloud—complemented by six vertical functional layers, which collectively ensure modularity, extensibility, and quantum readiness under realistic deployment conditions.

At the foundation, the Device Layer consists of distributed physical nodes, such as sensors and embedded microcontrollers, deployed across smart factories, homes, mobility systems, and industrial plants. These devices are typically resource-limited and incapable of executing quantum protocols natively. To accommodate future quantum capabilities, a lightweight classical-to-quantum transformation interface is placed at this level. This module would encode selected classical data features into formats compatible with quantum computation, thereby intended to enable quantum processing without modifying existing hardware.

Immediately above lies the Edge Layer, which serves as a gateway for quantum-aware preprocessing. This layer integrates compact quantum computing and memory modules to support hybrid execution environments, such as quantum virtual machines. Functions like real-time anomaly detection, authentication verification, or privacy-preserving inference could be executed locally, potentially reducing the reliance on cloud-based quantum resources. The edge infrastructure also implements preliminary session setup, data filtering, and encryption key handling, acting as a security buffer for upstream communication.

The Fog Layer bridges the gap between edge devices and cloud services by providing long-range quantum communication capabilities. Equipped with quantum repeaters, modulators, and

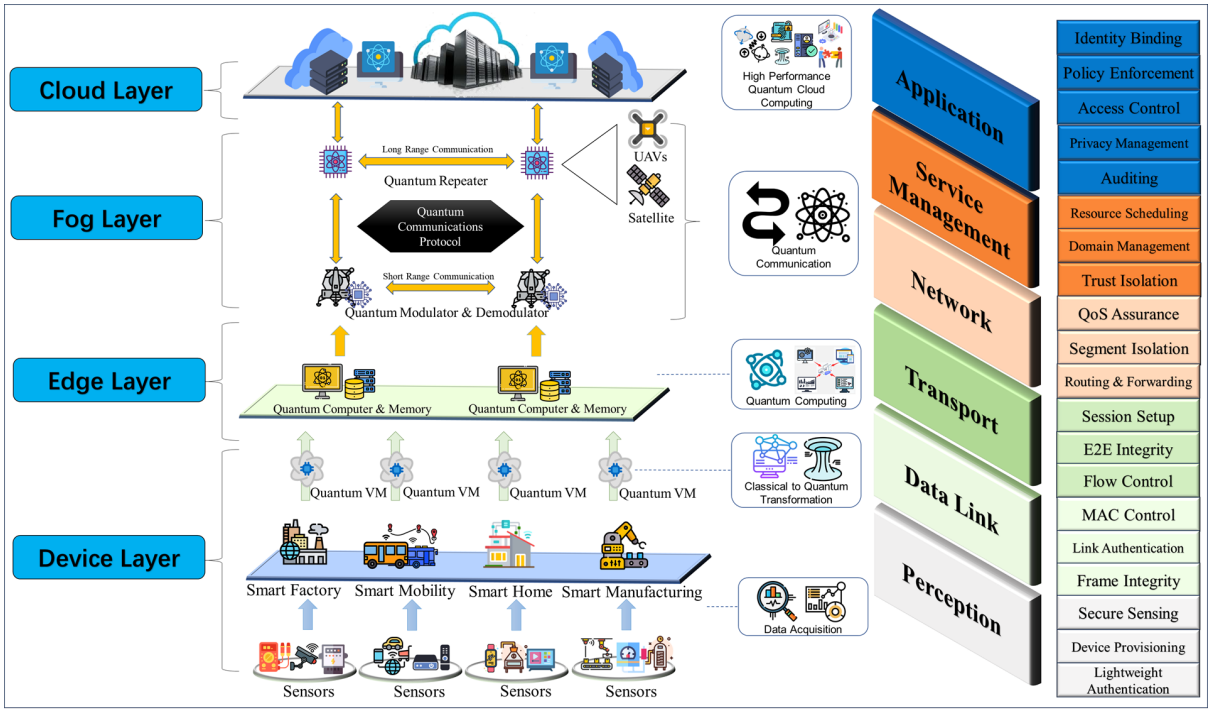

Figure 1: A Layered Security-Oriented Architecture for Quantum-Integrated IoT

demodulators, this layer is designed to facilitate entanglement distribution and protocol relay across wide areas. It also supports protocol adaptation by translating high-assurance credentials and tokens from the cloud into simplified trust representations interpretable by edge and device layers. The fog infrastructure is particularly relevant for mobile, vehicular, or cross-domain IoT scenarios, where direct fibre-based quantum links are infeasible.

At the top, the Cloud Layer provides high-performance quantum computing services and global policy enforcement. It is capable of executing large-scale quantum cryptographic operations such as key distribution, federated authentication orchestration, and encrypted analytics. This layer manages identity resolution, inter-domain auditing, and trust model propagation, forming the semantic and cryptographic backbone of the entire architecture.

In parallel to the spatial decomposition, the architecture defines six functional planes that operate across all physical layers:

- **Perception Layer**: responsible for device provisioning, secure sensing, and lightweight authentication. It ensures that raw data entering the system originates from trusted sources.
- **Data Link Layer**: handles low-level communication integrity through MAC control, frame authentication, and link-layer encryption.
- **Transport Layer**: ensures reliable message exchange through end-to-end session setup, flow control, and data integrity verification.
- **Network Layer**: oversees logical segmentation, routing, quality-of-service enforcement, and domain-based trust separation.
- **Service Management Layer**: handles resource scheduling, domain isolation, and trust policy orchestration across edge, fog, and cloud components.

- **Application Layer**: defines access control, identity binding, policy compliance, and privacy enforcement. These operations govern how users and devices interact with the system, both locally and globally.

Each functional plane is expressed in a technology-agnostic manner, allowing the underlying cryptographic or computational mechanism to be replaced with quantum-safe or quantum-native alternatives as standards evolve. For example, session setup in the transport layer can be instantiated using post-quantum key encapsulation mechanisms (KEMs), while identity binding in the application layer may be realised using quantum-enhanced zero-knowledge proofs.

This architecture is expected to provide a smooth integration path from current IoT infrastructure toward quantum-augmented systems. By harmonising spatial deployment constraints with functional separation of duties, it provides a systematic foundation for secure, scalable, and forward-compatible IoT deployments in the quantum era.

4. Expected Contributions

This research aims to contribute a comprehensive design and analysis of a lightweight, quantum-compatible security architecture for heterogeneous IoT systems. The expected contributions are as follows:

- **Layered Architectural Framework.** A structured architecture that integrates spatial hierarchy with functional planes, providing a clear path for embedding quantum technologies into existing IoT infrastructures.
- **Quantum-Compatible Edge Design.** A blueprint for edge-level components that can support limited quantum functionality without relying on full quantum capabilities, including transformation modules and hybrid verification routines.
- **Trust Propagation via Fog Infrastructure.** A relay mechanism for translating complex quantum-level credentials into simplified tokens that can be validated by constrained devices, with specific focus on fog-mediated trust delegation.
- **Modular Security Functions.** A functional decomposition that decouples security responsibilities across perception, transport, and application layers, which is intended to enable flexible adoption of quantum-safe primitives at each layer.
- **Feasibility Analysis.** A resource-oriented evaluation showing that the proposed methods can be deployed under realistic constraints, including processing power, communication latency, and memory limitations.

5. Conclusion

As quantum computing technologies mature, the security foundations of modern IoT systems must be revisited. Existing solutions either assume ideal quantum infrastructure or neglect the practical constraints of real-world deployments. This research proposes a layered architecture that addresses both challenges: it introduces spatial and functional decomposition to bridge the gap between resource-limited IoT devices and powerful quantum services.

The proposed system is intended to enable partial integration of quantum methods—such as authentication, secure sensing, and credential propagation—without requiring a full replacement of current hardware. Through modular interfaces, hierarchical communication models,

and abstraction of cryptographic functions, the architecture provides a scalable and forward-compatible framework for quantum-secure IoT systems. The outcome is expected to support future deployments where classical and quantum devices coexist, without introducing additional risk or complexity to the end users.

References

[1] Prateek Singh et al. "A Survey on Available Tools and Technologies Enabling Quantum Computing". In: *IEEE Access* 12 (2024). Open Access; Published: 12 April 2024, pp. 57974–57991. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2024.3388005. URL: https://doi.org/10.1109/ACCESS.2024.3388005.

[2] Basudeb Bera et al. "Healthcare Security: Post-Quantum Continuous Authentication With Behavioral Biometrics Using Vector Similarity Search". In: *IEEE Transactions on Information Forensics and Security* 20 (2025). Published: 17 January 2025, pp. 1597–1612. DOI: 10.1109/TIFS.2025.3531197. URL: https://doi.org/10.1109/TIFS.2025.3531197.

[3] Prithwi Bagchi et al. "Quantum Safe Lattice-Based Single Round Online Collaborative Multi-Signature Scheme for Blockchain-Enabled IoT Applications". In: *ACM Transactions on Sensor Networks* 21.2 (2025). Published: 22 March 2025, pp. 1–33. DOI: 10.1145/3715696. URL: https://doi.org/10.1145/3715696.

[4] Basudeb Bera, Ashok Kumar Das, and Biplab Sikdar. "Securing Next-Generation Quantum IoT Applications using Quantum Key Distribution". In: *IEEE Internet of Things Magazine* 8.1 (Jan. 2025). Published: 24 December 2024, pp. 50–56. DOI: 10.1109/IOTM.001.2400059. URL: https://doi.org/10.1109/IOTM.001.2400059.

[5] Tobias Haug et al. "Pseudorandom Quantum Authentication". In: *CoRR* abs/2501.00951 (2025). Introduces PQAS scheme. arXiv: 2501.00951. URL: https://arxiv.org/abs/2501.00951.

[6] Mansoor Ali Khan, Muhammad Naveed Aman, and Biplab Sikdar. "Architecting the Quantum Future: Key Devices and Layers in Quantum Network Design". In: *2024 IEEE Physical Assurance and Inspection of Electronics (PAINE)*. Conference Date: 12–14 November 2024; Added to IEEE Xplore: 16 December 2024. Huntsville, AL, USA: IEEE, 2024. DOI: 10.1109/PAINE62042.2024.10792827. URL: https://doi.org/10.1109/PAINE62042.2024.10792827.

[7] Rohini Poolat Parameswarath and Biplab Sikdar. "Quantum-Safe Authentication Protocol Using Post-Quantum Key Encapsulation Mechanism for Transportation Systems". In: *2024 IEEE 4th International Conference on Sustainable Energy and Future Electric Transportation (SEFET)*. Conference Date: 31 July – 03 August 2024; Added to IEEE Xplore: 24 October 2024. Hyderabad, India: IEEE, 2024. DOI: 10.1109/SEFET61574.2024.10717975. URL: https://doi.org/10.1109/SEFET61574.2024.10717975.

[8] Mansoor Ali Khan, Muhammad Naveed Aman, and Biplab Sikdar. "Quantum Guard: Pioneering Quantum-Based Malware Defense for IoT Devices". In: *2024 IEEE Conference on Dependable and Secure Computing (DSC)*. Conference Date: 06–08 November 2024; Added to IEEE Xplore: 29 November 2024. Tokyo, Japan: IEEE, 2024. DOI: 10.1109/DSC63325.2024.00032. URL: https://doi.org/10.1109/DSC63325.2024.00032.

[9] Rohini Poolat Parameswarath, Nalam Venkata Abhishek, and Biplab Sikdar. "A Quantum Safe Authentication Protocol for Remote Keyless Entry Systems in Cars". In: *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*. Conference Date: 10–13

October 2023; Added to IEEE Xplore: 11 December 2023. Hong Kong, Hong Kong: IEEE, 2023. DOI: 10.1109/VTC2023-Fall60731.2023.10333825. URL: https://doi.org/10.1109/VTC2023-Fall60731.2023.10333825.

[10] Mansoor Ali Khan, Muhammad Naveed Aman, and Biplab Sikdar. "Soteria: A Quantum-Based Device Attestation Technique for Internet of Things". In: *IEEE Internet of Things Journal* 11.9 (May 2024). Published: 25 December 2023, pp. 15320–15333. DOI: 10.1109/JIOT.2023.3346397. URL: https://doi.org/10.1109/JIOT.2023.3346397.

[11] Kashif Javed et al. "Securing Synchrophasors Using Data Provenance in the Quantum Era". In: *IEEE Open Journal of the Communications Society* 5 (2024). Open Access; Published: 01 March 2024, pp. 1594–1608. ISSN: 2644-125X. DOI: 10.1109/OJCOMS.2024.3372524. URL: https://doi.org/10.1109/OJCOMS.2024.3372524.

[12] Howard Barnum et al. "Authentication of Quantum Messages". In: *Proceedings of FOCS '02* (2002). arXiv: quant-ph/0205128. URL: https://arxiv.org/pdf/quant-ph/0205128.

[13] Marcos Curty and David J. Santos. "Quantum authentication of classical messages". In: *Phys. Rev. A* 64.062309 (2001). DOI: 10.1103/PhysRevA.64.062309. arXiv: quant-ph/0103122. URL: https://arxiv.org/pdf/quant-ph/0103122.

[14] Mark Zhandry. "A Note on Quantum-Secure PRPs". In: *CoRR* abs/1611.05564 (2016). arXiv: 1611.05564. URL: https://arxiv.org/abs/1611.05564.

[15] Mark Zhandry. *How to Model Unitary Oracles*. IACR Cryptology ePrint Archive, Paper 2025/1072. 2025. IACR: 2025/1072. URL: https://eprint.iacr.org/2025/1072.