

The Rise of Quantum IoT in Smart Healthcare: A Technical Review of Frameworks and Future Directions

¹Poulomi Deb, ²Akshay Reang, ³Prantosh Debbarma, ⁴Kumar Amitabh and ⁵Debadrita Pal

¹National Institute of Electronics and Information Technology
Agartala, Tripura, India
poulomideb.deb7@gmail.com

²National Institute of Electronics and Information Technology
Agartala, Tripura, India
Akshaybusiness01@gmail.com

³National Institute of Electronics and Information Technology
Agartala, Tripura, India
Prantoshdb90@gmail.com

⁴National Institute of Electronics and Information Technology
Agartala, Tripura, India
kumar.amitabh@nielit.gov.in

⁵National Institute of Electronics and Information Technology
Agartala, India
Debadritapal1@gmail.com

(Article history: Selected papers from NIELIT's International Conference on Communication, Electronics and Digital Technologies (NICE-DT'26), 29-30Jan, 2026, Gorakhpur, India)

Abstract. The rapid digitalization of healthcare through Internet-connected medical devices has enabled remote monitoring and data-driven clinical decision-making. However, classical Internet of Things (IoT)-based healthcare systems face significant limitations in terms of computational capability, scalability, and cybersecurity. The Quantum Internet of Things (QIoT) introduces a transformative approach by integrating quantum sensing, quantum communication, quantum computing, and quantum imaging into healthcare ecosystems. This paper presents a comprehensive technical review of QIoT applications in smart healthcare, focusing on architectural frameworks, enabling technologies, and security mechanisms. A unified six-layer QIoT architecture is analyzed, incorporating device, network, edge, cloud, application, and management layers. Recent advancements (2021–2025) in quantum key distribution, quantum machine learning, and post-quantum cryptography are critically examined. Furthermore, practical deployment challenges such as cost, hardware limitations, and integration with existing healthcare systems are discussed. The paper also outlines future research directions toward the realization of Healthcare 5.0.

Keywords: Quantum Internet of Things, Smart Healthcare, Quantum Computing, Quantum Communication, Post-Quantum Cryptography

1 Introduction

Healthcare digitization enables telemedicine, continuous monitoring, and data-driven decisions, but classical IoT suffers from scalability, security, and processing constraints. QIoT augments IoT with quantum capabilities—ultra-sensitive sensing, accelerated computation, and provably secure communication—offering a path toward robust next-generation healthcare systems.

1.1 Comparison Between Classical IoT and Quantum IoT

Table 1.Comparison between Classical IoT and Quantum IoT

Feature	Classical IoT	Quantum IoT
Security	Computational	Information-theoretic
Processing	Classical CPU	Quantum + classical
Scalability	Limited	Hybrid scalable

The comparison indicates that QIoT improves security via quantum protocols (e.g., QKD), enhances processing through hybrid models, and supports better scalability for large, heterogeneous medical systems.

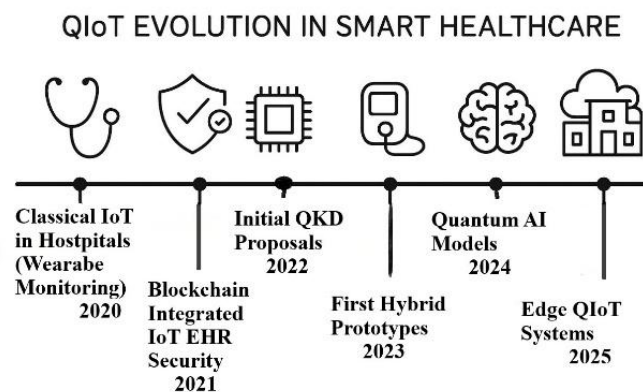


Fig. 1.Evolution timeline of quantum Internet of Things in smart healthcare systems

2 Background and Related Work

Early IoT healthcare focused on wearables and cloud analytics but remained limited by security and compute constraints. Recent work explores QKD for secure transmission and QML for clinical analytics; however, most studies address isolated components with limited real-world validation. A unified, interoperable architecture remains necessary.

Table 2.Key related work on quantum Internet of Things in smart healthcare

Focus	Methodology	Findings and Limitations
Secure medical image transmission	ROI based encryption, quantum block scrambling.	Great confidentiality and integrity of images were attained, and quantum operations were vastly computationally excessively.
Clinical data classification	sqkSVM NISQ quantum classifier qD templated.	Accuracy on datasets was reached of up to 91%; current hardware acts as a noise source, which limits its performance.
Quantum machine learning for healthcare	QML models (VQC, QNN, QRF) systematic review.	There will be substantial future growth opportunities of QML models; the errors in quantum data encoding did not allow scaling.
Quantum security for IoMT [22]	Education Survey of quantum threats and post-quantum cryptography (PQC.)	Determined IoT vulnerability in quantum attacks; highlighted experts in PQC.
QIoT framework design	Combined quantum detectors, communication and computation.	QH-IoT suggested architecture; the benefits were stated, and not implemented.
Hybrid blockchain with quantum signatures	Quantum blind signature and hyperledger.	Better auditability of data, anonymity; blockchain overhead in the network increased the latency.

3 Components of Quantum Internet of Things

QIoT comprises four core components integrated with classical systems.

3.1 Quantum sensing

Enables ultra-precise detection of biological signals (e.g., NV centers, magnetometers).

Trade-off: high sensitivity vs. calibration complexity and cost.

3.2 Quantum Computing

Supports drug discovery, genomics, and optimization using VQE/QAOA and QML.

Trade-off: NISQ limitations (noise, qubits) → hybrid execution preferred.

3.3 Quantum Communication

QKD (e.g., BB84) provides information-theoretic security for medical data.

Trade-off: infrastructure cost and distance constraints → hybrid PQC integration.

3.4 Quantum Imaging

Improves resolution with lower radiation exposure for diagnostics.

Trade-off: complex optics and limited commercialization.

4 QIoT Architecture for Smart Healthcare

A hybrid six-layer architecture enables incremental adoption.

4.1 Device Layer

Quantum-enhanced sensors for precise data acquisition.

4.2 Network Layer

Secure communication via QKD and PQC.

4.3 Edge Layer

Low-latency hybrid processing and anomaly detection.

4.4 Cloud Layer

Scalable quantum resources for intensive analytics.

4.5 Application Layer

Clinical decision support and visualization.

4.6 Management Layer

Security, compliance, and resource orchestration.

5 Practical Deployment Challenges

High hardware cost, integration with legacy systems, energy demands, and limited expertise constrain deployment. Near-term adoption favors hybrid architectures and targeted use cases (secure transmission, specialized diagnostics).

6 Future Research Directions

Focus areas include scalable hardware, error mitigation, hybrid quantum–classical models, standardized protocols, and regulatory frameworks for clinical validation.

Conclusion

QIoT can significantly enhance healthcare security, precision, and analytics. With hybrid deployment and continued advances, it provides a practical pathway toward Healthcare 5.0.

References

1. R.V. Sutradhar; P.V. Karmakar: A review on smart healthcare employing quantum internet of things. *IEEE Engineering Management Review* 51(3), 170–189 (2024)
2. L. Zhang: QUMA: Quantum unified medical architecture using blockchain. *Informatics in Medicine Unlocked* 11(2) (2024)
3. A. Kumar: A logical IoT architecture for a spatially distributed quantum sensor system. *IEEE Internet of Things Journal* (2024)
4. M. Chen: Sensing at the nanoscale using nitrogen-vacancy centers in diamond: A model for a quantum pressure sensor. *Nanomaterials* 14(8), 675 (2024)
5. L. Wang: A framework for processing large-scale health data using quantum computing in smart healthcare. *Frontiers in Digital Health* 6, 1502745 (2024)
6. K. Wang: Utilizing multifrequency resonances of electron spins in diamond nitrogen-vacancy centers for quantum sensing. *Journal of Applied Physics* 136(16), 164401 (2024)
7. S. Lee: IoT revolutionizing healthcare: A survey of smart healthcare system architectures. *IEEE Transactions on Network Science and Engineering* (2023)
8. K. Zhang; H. Li; Y. Wang: Physical layer architecture for spatially distributed quantum IoT sensors in telecom networks. *IEEE Internet of Things Journal* (2024)
9. L. Wang: Context-aware architecture using IoT and generative adversarial networks for healthcare systems. *Journal of Artificial Intelligence Technology* 4(3), 187–203 (2024)
10. R. Patel: An efficient and secure framework for smart healthcare using IoT and machine learning. *IEEE Access* 12, 167834–167851 (2024)
11. D. Martinez: Quantum-assisted supervised learning for healthcare intrusion detection systems. *IEEE Transactions on Neural Networks and Learning Systems* (2024)
12. M. Chen: Improvement of an edge-IoT architecture driven by artificial intelligence for chronic disease management. *Sensors* 24(24), 7965 (2024)
13. A. Brown: Leveraging IoT-aware technologies and AI techniques for real-time critical healthcare applications. *Sensors* 22(19), 7675 (2024)
14. D. Kim: Hybrid and fusion approaches for fault-tolerant quantum computing. *Journal of the Korean Physical Society* 85(8), 623–635 (2022)
15. S. Kumar: Practical application-specific advantage through hybrid quantum computing. *Nature Physics* 18(8), 234–245 (2022)
16. I. Davis: Strengthening authentication mechanisms using post-quantum cryptography. *Journal of Internet Technology* 9(4), 1245–1267 (2024)
17. S. Pirandola; U.L. Andersen; L. Banchi; et al.: Advances in quantum cryptography. *Advances in Optics and Photonics* 12(4), 1012–1236 (2020)
18. L. Gyongyosi; S. Imre: A survey on quantum computing technology. *Computer Science Review* 31, 51–71 (2019)
19. G. Sorelli; N. Treps; F. Grosshans: Quantum imaging: principles and recent developments. *Laser & Photonics Reviews* 14(2), 1900104 (2020)
20. I. Ahmed; G. Jeon: Quantum machine learning for healthcare: a review. *IEEE Access* 9, 110453–110472 (2021)
21. N. Kumar; S. Zeadally: Quantum-enabled Internet of Things: vision, challenges, and future directions. *IEEE Network* 36(1), 62–69 (2022)
22. C. Alcaraz; J. Lopez: Post-quantum cryptography in healthcare IoT. *Future Generation Computer Systems* 137, 123–138 (2023)