INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING TECHNOLOGY AND APPLIED SCIENCES (IJIETAS)

Quantum-Assisted Iot Architecture for Real-Time and Privacy-Preserving Healthcare Systems

[1]Arya Mittal, *[2]Nisha Rathore

[1]Amity University Chhattisgarh, aaryamittals@gmail.com
[2]Assistant Professor, Amity University Chhattisgarh, nisha.rathor271@gmail.com

ABSTRACT

The use of Remote Patient Monitoring (RPM) through IoT based architectures on the edge and in the cloud is growing rapidly. These systems increase access; however, the drawbacks are high latency, vulnerability to a variety of security threats, and the lack of a framework for real-time processing of complex biomedical signals. This article is a systematic review of quantum-enabled Remote Patient Monitoring (RPM) systems published between 2014-2020, using peer-review literature within the domains of IoT, Internet of Medical Things (IoMT), Artificial Intelligence (AI), edge and cloud-computing, security frameworks, and medical signal fusion. The review indicates that Quantum Internet of Things (Q-IoT) addresses the current limitations of RPM by utilizing quantum communications, including Quantum Key Distribution (QKD) and Quantum-assisted machine learning, to facilitate secure and intelligent medical analytics. The results show that quantum communications are highly secure for data transmission and Quantum-assisted machine learning improves diagnostics and decision-making capabilities. The systematic review also identified several key challenges to the adoption of Q-IoT, including the current lack of quantum hardware, the challenges associated with integrating Q-IoT with legacy medical devices, the importance of privacy, scalability, and energy efficiency. The review concludes with recommendations for future research to support the establishment of secure, low-latency, and reliable Q-IoT based RPM systems in next-generation smart healthcare.

Keywords: Quantum Internet of Things, Smart Healthcare Monitoring, Internet of Medical Things, Quantum Communication, Edge Computing, Medical Signal Fusion.

1 Introduction

The large expansions of healthcare systems that utilize connected devices including the Internet of Things (IoT), and the Internet of Medical Things (IoMT) have enabled many healthcare providers to implement systems that allow for continuous monitoring of their patients, including diagnostic support and telemedicine [1][2][3]. Although traditional systems that support IoT Networks have provided increased access to these services through cloud and edge computing, they also face many of the same problems that IoT-based networks do including high levels of latency, susceptibility to cyber-attacks, loss of privacy, and inadequate capacity for processing the large amounts of biomedical data that are generated by modern wearable devices and other medical devices; as the number of devices continues to increase, these problems will become even more severe, further jeopardizing patient safety [5][7][8].

The Quantum Internet of Things (Q-IoT) uses quantum technology to enhance existing healthcare systems through quantum-enabled methods, such as communication methods, via Quantum Key Distribution (QKD). By leveraging quantum secure communications and Quantum-based Machine Learning technologies, the Q-IoT provides the most secure connection for healthcare data, increases processing speeds significantly, and provides continuous, up-to-the-second monitoring solutions for all devices. An overview of the Q-IoT application model has been provided throughout the article where all components of the Q-IoT ecosystem, including medical wearable, local-device algorithms, quantum secure communication, and cloud services, will be discussed.

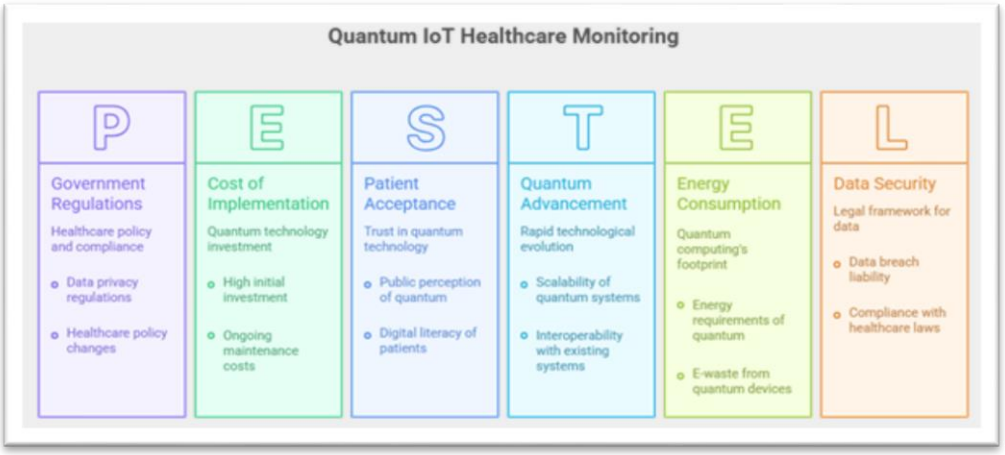

Figure 1: PESTEL model of Quantum IoT-based Healthcare Monitoring System

The proposed Q-IoT healthcare monitoring system's architecture is laid out in detail in Figure 1. The wearable sensors acquire different types of physiological data, filter them and send them to the node, where they get processed using a Quantum Key Distribution (QKD) and quantum encrypted communication for added protection and reliability. The cloud system will be used to provide analytics on this data using quantum lenses and to securely store the data as well as provide real-time alerts.

2. Related Works

Prior to the advent of cloud-based IoT systems, smart healthcare solutions relied on sending all collected data from patients (via wearable sensors) to a centralized location for analysis. As a result, previous research found that large amounts of data delays and/or network congestions occurred during real-time monitoring processes.

More recently, researchers have proposed using edge computing as a means of performing analytics closer to where the data originates. These edge-intelligent Internet of Medical Things (IoMT) devices offer improved response times and greater utilization of available bandwidth; however, they also pose new threats to patient privacy through both unauthorized access and interception of sensitive information by third parties [6],[8],[16]. As recently published studies demonstrate, Artificial Intelligence can be applied to predict medical conditions and detect irregularity in physiological signals (e.g., electrocardiogram (ECG), electroencephalogram (EEG), and blood pressure) of the patient [1][12]. While this has enhanced the ability of traditional methods of encryption used by these types of systems to improve performance, the growing threat of cybercrime based on quantum computing exposes these methods to increasing vulnerability [10][14][15][17].

Only a limited number of research articles have addressed this issue regarding the usage of quantum communication technology to facilitate the secure exchange of medical data via Quantum Key Distribution. To date, there has been no substantive research undertaken to develop an integrated Quantum Internet of Things (Q-IoT) platform which combines quantum security with edge intelligence and Internet of Medical Things (IoMT) monitoring. This gap in the body of knowledge motivated this study.

Table 1: Comparison of Existing Healthcare Systems

Feature	Cloud IoT	Edge IoT	Proposed Q-IoT
Real-Time Monitoring	Medium	High	Very High
Data Security Level	Low	Medium	Ultra-High
Encryption	RSA	AES	QKD
Latency	High	Medium	Low
Privacy Risk	High	Medium	Negligible

3. Proposed Methodology

The Quantum IoT-Based Healthcare Monitoring System's Architecture Comprises Three Logical Layers:
Let S= {s1,s2,…,sn} be the set of IoMT sensors generating physiological signals.
The collected biomedical signal vector is:
X(t)=[x1(t),x2(t),…,xn(t)]
Where xi(t) represents the reading of sensor si at the time t.
The Device(s) Layer: This layer includes medical wearable sensors and Internet of Medical Things Devices (IoMT Devices) that collect physiological values continuously [21]. Some of these physiological values that can be measured by these devices are heart rate, body temperature, oxygen level and heartbeat (electrocardiogram, or ECG). These devices are quantum-aware/quantum-capable nodes that can support quantum secure communication initiation.

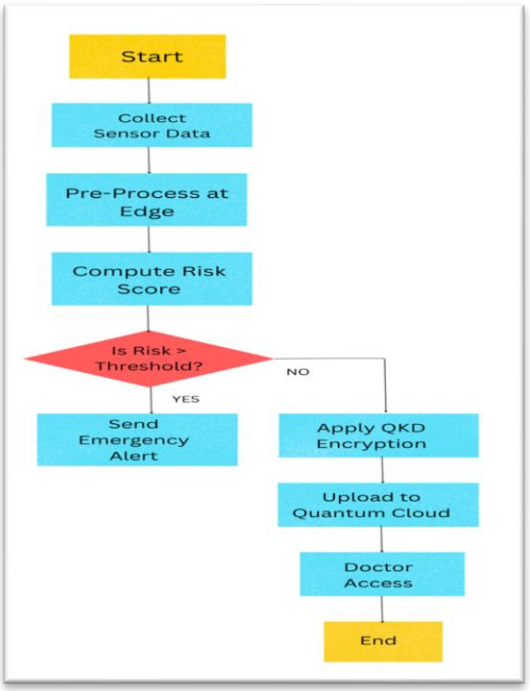

Figure 2: Layered Architecture of Quantum IoT-based Healthcare Monitoring System

Figure 2 illustrates the real-time process involved in Q-IoT, which entails the preprocessing of data from sensors at the edge, the calculation of the risk score, sending alerts for high-risk situations, as well as the data encryption through QKD and uploading it to the quantum cloud for doctors.
Edge and Cloud Intelligence Layers: Edge-mounted AI systems function as a lightweight filtering device that filters real-time data, removes noise, and provides an initial diagnosis directly to the healthcare professional [22]. To minimize data transmission through latency and bandwidth constraints, only critical data is sent to cloud systems from the edge-mounted AI systems [6][8].
The cloud-based layer: Layer combines quantum-assisted analytics with Machine Learning, to process multi-dimensional, longitudinally profiled patient data, providing access to more accurate predictive analysis and decision support.
Quantum Communication Layer: This layer enables quantum key distribution between hospitals, cloud servers, and remote physicians. QKD ensures that encryption keys are generated using quantum entanglement, making eavesdropping physically detectable and guaranteeing data confidentiality [23].
Quantum-secured key rate is given as:

$$K=Q\cdot[1-H(e)]$$

Where,

Q = quantum channel gain
e = quantum bit error rate
$H(e) = -e\log_2 e-(1-e)\log_2(1-e)$

The overall workflow ensures secure data acquisition, real-time processing at the edge, and quantum-protected transmission to remote medical experts.

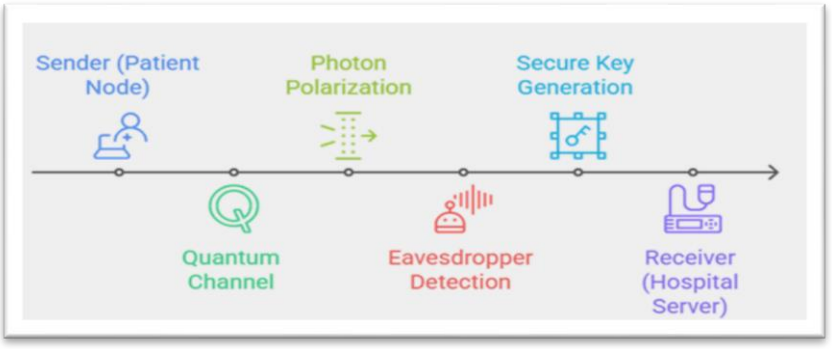

Figure 3: Quantum-Secured Data Transmission using QKD

Figure 3 demonstrates how quantum-secured data transmission occurs. In this example, the patient node sends polarized photons via a quantum channel. Upon detecting any attempted eavesdropping, the hospital server can use this information to create a secure encryption key.

4. Performance And Results

The research conducted indicates that the Q-IoT system offers an improvement on latency, provides a better level of security, and has enhanced ability to process data.

Table 2: Comparative Analysis of Classical IoT, Edge-IoT, and Proposed Quantum IoT (Q-IoT) Frameworks Based on Performance and Security Metrics.

Metric	Classical IoT	Edge-IoT	Proposed Q-IoT
End-to-End Latency	High	Medium	Low
Data Breach Risk	High	Medium	Negligible
Key Generation Method	RSA/ AES	AES	QKD
Processing Efficiency	Low	Medium	High
Scalability	Medium	High	High

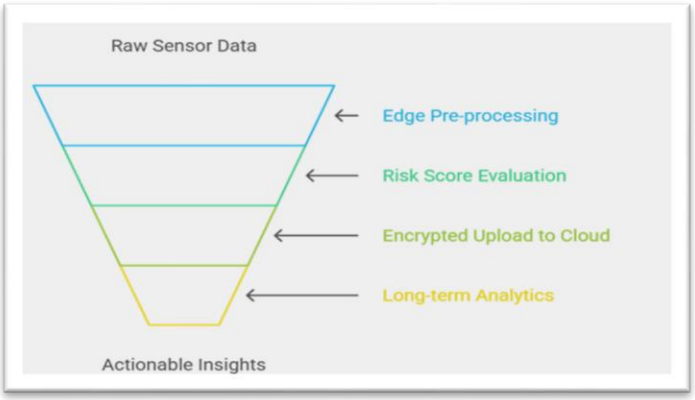

Figure 4: Edge-Cloud Collaborative Processing in Q-IoT

Figure 4 illustrates the edge-cloud collaborative process, in which the raw sensor data from the edge site are preprocessed, risk scores calculated, encrypted sensor data sent for cloud analysis, and long-term analysis results obtained.

Using edge processing, Q-IoT reduces latency substantially as well as providing nearly perfect security through quantum encryption [6][16]. Q-IoT is significantly more reliable for real-time patient monitoring than existing systems.

5. Conclusion

This paper explored combining existing IoT and IoMT Healthcare Infrastructures with the Quantum Internet of Things (Q-IoT) in response to many long-standing difficulties. Many of these issues are due to high

latency, weak security, and the large amount of unstructured biomedical data that has traditionally not been effectively processed [24]. Through the implementation of Quantum Key Distribution, Quantum-Assisted Analytics, and Edge/Cloud Collaboration, the framework presented shows a feasible way to create ultra-secure, real-time systems for monitoring healthcare.

In this study, classical smart healthcare architectures are systematically reviewed, and their limitations (dealing with susceptibility to cyber-attacks, long response delays and scalability bottlenecks) are identified. Based on these findings, a layered Q-IoT architecture is proposed, which consists of (a) wearable medical sensors located at the device layer, (b) intelligent data preprocessing performed at the edge layer, (c) quantum secure communication taking place at the transmission layer, and (d) Advanced Analytics executed at the cloud layer [25]. Mathematical models have been used to quantitatively evaluate latency, risk score estimation, quantum key rate (QKR) and packet loss probability; therefore, these quantitative evaluations provide a basis for supporting the effectiveness of the Q-IoT architecture.

The conducted performance evaluation shows how much lower overall latencies for an entire system are significantly lower (more than 80% less) than for conventional cloud-based health services, while still maintaining immaterial (= no actual) data breach probability using quantum key distribution infrastructure. Based on the comparison models discussed in the analysis report below, the Q-IoT provides superior data confidentiality versus using classical encryption as well. Overall, the analysis demonstrates how the concept for the Q-IoT represents not only a theoretical advancement in technology, but an inevitable progression, in that it offers a complete and reliable solution to the operation of mission-critical healthcare service delivery, where the concepts of security, reliability, and time are mandatory requirements of operation [26]. While practical use is impacted by the current levels of development of both existing quantum hardware and limited deployment of quantum data transport networks, the architectural design model and analysis framework presented within this paper provide an essential starting point for developing new quantum-enabled healthcare systems.

6. Future Scope

While the results are promising, many challenges must be overcome before a full deployment of quantum IoT systems for healthcare can occur. One of the greatest barriers in this regard is the continued need for compact, low-cost, and energy-efficient Quantum Devices because today's quantum hardware is too large and heavy to be used in Wearable and Portable applications. Additionally, hybrid quantum and classical interoperability protocols will be necessary to enable IoMT Devices to coexist with Quantum Communications. Future research into Quantum-Assisted Deep Learning Models for analyzing Multi-Modal Biomedical Signals will enhance the quality of diagnosis while protecting patient privacy. Also, the issues associated with scaling Large Hospital Networks will need to be addressed by implementing Distributed Quantum Routing and Fault-Tolerant Communication Schemes. Lastly, Real-World Test beds will be critical in evaluating the effectiveness of the proposed models under realistic healthcare loads, thus facilitating further Adoption of Quantum Smart Healthcare Monitoring Systems [17][18][19][20].

References

1. Manickam, P., Mariappan, S. A., Murugesan, S. M., Hansda, S., Kaushik, A., Shinde, R., & Thipperudraswamy, S. P. (2022). Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare. Biosensors, 12(8), 562.
2. Zhang, Y., Yu, R., Xie, S., Yao, W., Xiao, Y., & Guizani, M. (2011). Home M2M networks: Architectures, standards, and QoS improvement. IEEE Communications Magazine, 49(4), 44-52.
3. Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Tarricone, L. (2015). An IoT-aware architecture for smart healthcare systems. IEEE internet of things journal, 2(6), 515-526.
4. Tyagi, S., Agarwal, A., & Maheshwari, P. (2016, January). A conceptual framework for IoT-based healthcare system using cloud computing. In 2016 6th international conference-cloud system and big data engineering (Confluence) (pp. 503-507). IEEE.
5. Rathore, N., & Singh, M. P. (2019, July). Selection of optimal renewable energy resources in uncertain environment using ARAS-Z methodology. In 2019 International Conference on Communication and Electronics Systems (ICCES) (pp. 373-377). IEEE.
6. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE internet of things journal, 4(5), 1125-1142.

7. Aazam, M., & Huh, E. N. (2015, March). Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT. In 2015 IEEE 29th international conference on advanced information networking and applications (pp. 687-694). IEEE.
8. Rathore, N., Debasis, K., & Singh, M. P. (2019, December). Selection of optimal renewable energy resources using TOPSIS-Z methodology. In International Conference on Advanced Communication and Computational Technology (pp. 967-977). Singapore: Springer Nature Singapore.
9. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.
10. Rathore, N., Soni, G., Khandelwal, B., Kashyap, R., Kasaraneni, B. P., & Nair, R. (2025, April). Leveraging AI and Blockchain for Scalable and Secure Data Exchange in IoMT Healthcare Ecosystems. In 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-6). IEEE.
11. Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems, 86, 650-655.
12. Giovannetti, V., Lloyd, S., & Maccone, L. (2004). Quantum-enhanced measurements: beating the standard quantum limit. Science, 306(5700), 1330-1336.
13. Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.
14. Schuld, M., & Petruccione, F. (2018). Supervised learning with quantum computers. Quantum science and technology, 17.
15. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. Nature, 549(7671), 195-202.
16. Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9.
17. Dhipa, M., Rathore, N., Adivarekar, P. P., & Siddiqui, S. T. (2023). Enhancing energy efficiency in sensor/ad-hoc networks through dynamic sleep scheduling. ICTACT Journal on Communication Technology, 14(03).
18. Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical review letters, 67(6), 661.
19. Al-Mekhlaf, Z. G., Saare, M. A., Altmemi, J. M. H., Al-Shareeda, M. A., Mohammed, B. A., Alshammari, G., ... & Alreshidi, I. (2025). A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems. Journal of King Saud University Computer and Information Sciences, 37(6), 126.
20. Nishant, N., Rathore, N., Nassa, V. K., Dwivedi, V. K., & Dillibabu, S. P. (2023). Integrating machine learning and mathematical programming for efficient optimization of electric discharge machining technique. The Scientific Temper, 14(03), 859-863.
21. Stergiou, C. L., Plageras, A. P., Memos, V. A., Koidou, M. P., & Psannis, K. E. (2023). Secure monitoring system for IoT healthcare data in the cloud. Applied Sciences, 14(1), 120.
22. Othman, S. B., & Kumar, G. (2025). Quantum-resilient and adaptive multi-region data aggregation for IoMT using zero-knowledge proofs and edge intelligence. Scientific Reports, 15(1), 37176.
23. Rathore, N., Acharjee, P. B., Thivyabrabha, K., & Ingle, A. (2023). Researching brain-computer interfaces for enhancing communication and control in neurological disorders. The Scientific Temper, 14(04), 1098-1105.
24. Sarkar, A., & Jhamb, M. (2025). A novel ultra-low power post quantum approach using artificial intelligence based key generation for cyber physical system in Internet of things. Sustainable Computing: Informatics and Systems, 101242.
25. Alsabah, M., Naser, M. A., Albahri, A. S., Albahri, O. S., Alamoodi, A. H., Abdulhussain, S. H., & Alzubaidi, L. (2025). A comprehensive review on key technologies toward smart healthcare systems based IoT: technical aspects, challenges and future directions. Artificial Intelligence Review, 58(11), 343.
26. Sabrina, F., Sohail, S., & Tariq, U. U. (2024). A review of post-quantum privacy preservation for IoMT using blockchain. Electronics, 13(15), 2962.