WAS Science Nature
WASSN

ISSN: 2766 - 7715
WAS PRESS

Minireview

Quantum Cryptography for Securing Information Systems Survey

Maryam Naji Marir Ali-habsi[1,*], Anma Mohammed Al-yaaqoubi[1] and Shama Salim Al-zidi[1,] Rabie A. Ramadan[1]

[1] Department of Information Systems, College of Economics, Management, and Information Systems, University of Nizwa, Nizwa, Sultanate of Oman. 21356517@uofn.edu.om; 15618256@uofn.edu.om ; 15515848@uofn.edu.om; Rabie@rabieramadan.org

* Correspondence: Maryam Naji Marir Ali-habsi; 21356517@uofn.edu.om

Received: 03-01-2025; Accepted: 04-15-2025; Published: 05-09-2025

Abstract: Healthcare institutions' growing reliance on digital technology for patient information management raises concerns regarding the security and privacy of sensitive health data. Quantum cryptography presents a viable way to improve health data security. Transmission guarantees secrecy and confidentiality. To protect the transmission of health data, this study investigates the quantum of quantum cryptography and how it is used in healthcare systems. It examines the benefits of quantum key distribution (QKD) over traditional encryption techniques and its function in supplying secure communication routes. The study also addresses quantum cryptography's difficulties and possible applications in healthcare systems, emphasizing how it might completely transform data security in this sector.

Keywords: Quantum Cryptography; Quantum Key Distribution (QKD); Security; Healthcare systems

1. Introduction

Traditional encryption techniques are vulnerable to online attacks due to the increase in processing power, but quantum cryptography offers new protection for health data transfer. This study examines the fundamentals of quantum cryptography and how it may be used to transmit health data securely in healthcare systems. It starts by reviewing the significance of data security and the growing usage of digital technology in healthcare. After that, it summarizes quantum cryptography, contrasts it with traditional cryptography techniques, and emphasizes how quantum key distribution (QKD) offers safe communication channels. The study explores quantum cryptography in healthcare to enhance privacy, security, and compliance with legal mandates, overcoming challenges in transmitting health data.

Finally, the paper discusses the technical, cost, and scalability challenges of implementing quantum cryptography in healthcare systems while highlighting quantum technology's emerging relevance to healthcare. Overall, this paper explores the use of quantum cryptography in healthcare systems, focusing on its role in ensuring privacy and confidentiality in health data transmission.

1.1. Quantum Cryptography: Principles and Concepts

It is one of the branches of quantum information science, and this branch uses the principles of quantum mechanics to secure communication channels, unlike some that rely on the mathematical complexity of encryption, such as classical encryption [1].

Quantum key distribution (QKD) is one of the basic principles of quantum cryptography, which is used to generate and distribute encryption keys. This distribution is based on the principle of quantum entanglement (two particles are linked and entangled so that the state of one of the two bodies is directly linked to the state of the second particle), regardless of the distance between them.

Quantum uncertainty is another principle used by quantum cryptography to detect eavesdropping. According to the Heisenberg uncertainty principle, specific pairs of properties of a quantum system are challenging to measure with arbitrary precision. Any attempt to eavesdrop or measure a quantum system will disturb it in a way that can be detected.

One of the advantages of quantum cryptography is unconditional security (the laws of quantum mechanics guarantee the security of encryption keys). Another advantage is its ability to detect eavesdropping, which ensures and provides secure communication.

In our increasingly sophisticated world, quantum encryption represents a major advance in secure communication technology and is revolutionizing data security in various industries, such as healthcare. When applied there, it ensures the protection of confidential, sensitive, and health information from electronic threats, theft, and unauthorized access.

1.2. Application of Quantum Encryption in Healthcare Systems

Medical records, treatment plans, personal identifiers, and others contain vast amounts of sensitive patient information that healthcare systems must deal with. Securing patient information and privacy is an important matter and a significant challenge for these systems. On the other hand, there is a powerful solution to secure this information by using quantum encryption, which ensures that unauthorized access and electronic threats to this information or attempts to steal it are not allowed [2].

Quantum encryption is applied to secure electronic health records in healthcare systems. These records contain patients' medical history, diagnoses, treatments, medications, etc. Encrypting this information ensures that healthcare providers cannot obtain or access it, thus protecting patient privacy. Another application of quantum encryption is to secure communication between healthcare providers and patients. For example, quantum cryptography can encrypt telemedicine sessions, ensuring that communication between the healthcare provider and the patient remains confidential and private.

It is also used to secure medical devices and sensors used in healthcare. These devices often contain patient information such as vital signs and physiological measurements, which must be secured and protected so that unauthorized people cannot access them. Quantum cryptography encrypts the data transmitted by these devices, thus ensuring the protection and confidentiality of the data [3].

In general, there are significant benefits to applying quantum cryptography in healthcare systems, such as securing and protecting data and ensuring that unauthorized people cannot access it.

2. Advantages of Quantum Cryptography in Healthcare

Quantum cryptography offers many advantages over traditional encryption methods, making it suitable for securing data transmission in healthcare systems [4].

1. Unconditional security: The laws of quantum mechanics guarantee the security of encryption keys. This provides a high level of protection compared to those that rely on computational complexity, such as classical encryption methods.
2. Key distribution: It allows the secure distribution of encryption keys, compared to classical key distribution methods, which are vulnerable to eavesdropping.
3. Compliance with regulatory requirements: Healthcare systems are subject to strict regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), which requires systems to protect sensitive patient health information. Quantum encryption ensures the security and privacy of data transmission, helping healthcare providers comply with these regulations.

4. Eavesdropping detection: Eavesdropping detection is important, meaning that any attempt to intercept or measure quantum information leads to a disturbance in the quantum state. It is detected by alerting the communicating parties.
5. Protection from quantum attacks: Quantum encryption is resistant to attacks from quantum computers. These devices can break traditional encryption methods, but unlike quantum encryption, they provide a secure alternative that is not vulnerable to quantum attacks.
6. Enhanced privacy and confidentiality: Healthcare providers can enhance the confidentiality and privacy of sensitive information by using quantum encryption, ensuring that information remains safe and unauthorized people cannot access it.

It is important to use quantum encryption to secure the transmission of health data in healthcare systems. It represents a secure and effective solution. Due to its ability to provide unconditional security, protection from quantum attacks, and detection of eavesdropping, it is an ideal choice for securing sensitive information.

3. Challenges And Limitations

While quantum cryptography provides notable advantages for securing health data transmission, several challenges and limitations need to be addressed [5]:

1. Technical Challenges [6]

- Implementing quantum cryptography requires very specialized components and expertise, including quantum key distribution (QKD) devices. These technologies rely on advanced quantum mechanics rules, like photon-based communication, which demand precise handling and calibration.
- Infrastructure Compatibility: Its existing healthcare systems, built on classical computing and cryptography, could not be readily compatible with quantum systems, leading to huge technical hurdles in integration.
- Limited Expertise: Quantum cryptography is highly specialized, and healthcare organizations may find it challenging to find or train personnel with the necessary expertise.

2. Cost Considerations

   Quantum cryptography nowadays is a high-cost technology, posing challenges for many healthcare providers. The following are some of those challenges:

   - Specialized Equipment: Devices like QKD units, single-photon detectors, and advanced fiber-optic communication systems are expensive to purchase and maintain.
   - Ongoing Costs: In addition to the initial investment, there are additional costs for regular maintenance, upgrades, and employee training to ensure the system works effectively.
   - Budget Constraints: Underfunded healthcare providers may find it difficult to allocate resources for quantum cryptographic solutions, especially when compared to other immediate healthcare priorities.

3. Scalability Issues

   Deploying quantum cryptography in large healthcare systems shows challenges related to scalability.

   - Increasing Complexity: As the number of users, devices, and facilities grows, managing quantum encryption systems becomes more complicated.
   - Key Management Overhead: Quantum cryptographic systems often require unique keys for each channel. In a large-scale system with thousands of users, the generation, distribution, and secure storage of these keys becomes a logistical burden.
   - Performance Bottlenecks: Expanding quantum cryptographic networks to accommodate a larger scale could lead to poor performance.

4. Key Management

   Quantum cryptography depends heavily on securing encryption keys, which ensures the system's overall security.

- Key Distribution: Quantum systems use QKD to exchange keys securely, but the process requires dedicated infrastructure, such as optical fibers or satellite-based links.
- Key Storage: Healthcare organizations must ensure that encryption keys are stored securely to prevent unauthorized access, requiring robust security protocols and hardware.

5. Interoperability

   Healthcare systems mainly rely on a mix of classical cryptographic systems (RSA, AES) and emerging quantum cryptographic solutions. Ensuring these systems work together seamlessly is a significant challenge for them [7].

   - Compatibility Issues: Integrating quantum cryptography into existing systems requires reconfiguring or upgrading older infrastructure, which is costly and time-consuming.
   - Protocol Differences: Classical and quantum cryptographic methods operate differently, forcing the development of new protocols to bridge the gap and ensure secure communication.
   - System Downtime: Transitioning to quantum-enabled systems while maintaining compatibility with existing systems can lead to temporary service disruptions, which will impact critical healthcare operations.

6. Quantum Network Infrastructure

   Establishing quantum communication networks to support quantum cryptography is complex and requires significant investment from healthcare providers.

7. Quantum Key Distribution Range

   Systems have limited range due to signal loss during transmission, potentially necessitating the need to ensure coverage over larger distances.

8. Quantum cryptography

   The systems are complex and require regulation and ethical decision-making at the individual level. For example, doctors and administrators using quantum-secured systems must be ethically aware of how technology handles patient data, including preventing misuse or mishandling. So, it's helpful to provide training programs to raise ethical awareness among healthcare professionals using quantum systems and develop a culture of responsible innovation to encourage transparency and trust [9].

9. Balancing Innovation and Risk Management

   Adopting quantum technologies requires balancing their transformative potential with associated risks (data misuse, unethical applications, and unintended failures). Quantum cryptography must be implemented alongside risk assessments to mitigate vulnerabilities in data security.

5. Prospects and Implications

Despite current challenges and difficulties, quantum cryptography offers exciting potential for revolutionizing healthcare data security [8]:

1. Advancements in Quantum Technologies:

   Ongoing research will improve efficiency, reduce costs, and enhance quantum cryptographic systems' range, speed, and reliability, making them more effective for healthcare.

2. Integration with IoT:

   Quantum cryptography can secure communications between healthcare IoT devices, protect sensitive patient data, and improve the safety of interconnected systems.

3. Enhanced Security and Privacy:

   By leveraging quantum principles, healthcare providers will ensure secure and confidential transmission of sensitive information, boosting trust and reliability.

4. Regulatory Compliance:

   Quantum cryptography helps comply with privacy laws by ensuring the security of patient data and fostering confidence between patients and providers.

5. Global Collaboration:
   Secure quantum networks will enable healthcare providers worldwide to share research, collaborate on treatments, and improve patient care across borders.
6. Quantum-Safe Cryptography:
   Because quantum computers evolve, traditional encryption methods will be vulnerable. Quantum cryptography has a foundation for quantum-safe systems, ensuring long-term data protection.
7. AI Integration
   Quantum cryptography can be combined with AI to enhance threat detection and prevention. AI-driven algorithms could monitor encrypted communications for unusual or suspicious activities to proactively secure healthcare systems.
8. Decentralized Healthcare Security
   Quantum cryptography could enable more secure decentralized healthcare models, such as blockchain-based health record systems, ensuring data integrity and confidentiality in these environments.
9. Accessibility and Affordability
   As quantum technologies mature, their affordability may improve, making advanced cryptographic solutions accessible even to smaller healthcare organizations, reducing the gap in data security.
10. Secure Telemedicine
    Quantum cryptography could provide enhanced security for video consultations, patient portals, and remote diagnostic tools, ensuring patient trust in virtual care [9].
11. Cross-Sector Collaboration
    Quantum cryptography will foster collaboration between the healthcare industry and quantum technology developers.
12. Preparedness for Future Threats
    By adopting quantum cryptography early, healthcare systems can future-proof their data security against the rise of quantum computers, ensuring long-term resilience against evolving cyber threats.

The future of quantum cryptography in healthcare is promising. Innovations are expected to transform data security, ultimately creating safer and more efficient healthcare systems.

4. Quantum Technologies Requirements

Quantum cryptography in healthcare requires clear ethical guidelines to address privacy concerns, responsibility gaps, and the societal impact of data misuse. Ethical considerations ensure that quantum systems protect patient data responsibly, avoiding unintended harm such as biased algorithms or privacy breaches.

Also, as quantum cryptography systems automate sensitive processes like data encryption, responsibility gaps may arise where it’s unclear who is accountable for failures or breaches. If quantum-secured systems fail to transmit patient data properly, determining accountability between technology providers, healthcare professionals, or system managers becomes complex. The solution for that is to establish shared accountability frameworks for stakeholders involved in quantum systems (for example, technology vendors, healthcare providers).

Quantum algorithms have been used to fill gaps in electronic health records (EHRs), improving the accuracy of clinical data for decision-making. In addition, QSVC and QNN algorithms have successfully classified patient data to predict medication adherence and persistence.

5. Conclusions

Quantum cryptography marks a transformative leap in secure communication, offering unmatched protection for healthcare systems. By having the power of quantum mechanics, it will ensure the confidentiality and integrity of sensitive health data, also safeguarding it against cyber threats and unauthorized access. Though challenges remain, the future is bright. With ongoing innovation, techniques, and research, quantum cryptography is set to overcome these barriers and become a practical, efficient, and cost-effective solution. As it evolves, it promises to redefine data security in healthcare, fostering a safer and more trusted environment for patients and providers alike. Continuous advancements in quantum technologies are steadily addressing these barriers, paving the way for more accessible and cost-effective solutions.

As quantum cryptography matures, it will enhance data security, enable global collaboration, protect healthcare IoT systems, and ensure compliance with stringent regulatory requirements. This innovation will empower healthcare providers to share confidently, store confidently, and transmit sensitive information, creating a foundation for a more secure and efficient healthcare system. Ultimately, quantum cryptography represents more than a technological breakthrough—it is a vital step toward a future where patient privacy and data security are uncompromised, fostering trust and resilience in healthcare systems worldwide.

Supplementary Materials: There are no supplementary materials.

Author Contributions: Conceptualization, M.N.M.A. and R.A.R.; methodology, M.N.M.A. and A.M.A.; software, S.S.A.; validation, M.N.M.A., A.M.A., and R.A.R.; formal analysis, M.N.M.A.; investigation, A.M.A.; resources, R.A.R.; data curation, S.S.A.; writing—original draft preparation, M.N.M.A. and S.S.A.; writing—review and editing, R.A.R.; visualization, A.M.A.; supervision, R.A.R.; project administration, R.A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the University of Nizwa, Nizwa, Sultanate of Oman.

Acknowledgments: The authors thank the University of Nizwa for their support in publishing this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Raparthi, M. Quantum Cryptography and Secure Health Data Transmission: Emphasizing Quantum Cryptography's Role in Ensuring Privacy and Confidentiality in Healthcare Systems. Blockchain Technology and Distributed Systems 2022, 2(2), 1–10.
2. Hoffmann, C.H.; Flöther, F.F. Why Business Adoption of Quantum and AI Technology Must Be Ethical. Research Directions: Quantum Technologies 2024, 2, e4. https://doi.org/10.1017/qut.2024.5
3. Flöther, F.F. The State of Quantum Computing Applications in Health and Medicine. Research Directions: Quantum Technologies 2023, 1, e10. https://doi.org/10.1017/qut.2023.4
4. Raparthi, M. Quantum-Inspired Neural Networks for Advanced AI Applications—A Scholarly Review of Quantum Computing Techniques in Neural Network Design. Journal of Computational Intelligence and Robotics 2022, 2(2), 1–8.
5. Raparthi, M. Privacy-Preserving IoT Data Management with Blockchain and AI—A Scholarly Examination of Decentralized Data Ownership and Access Control Mechanisms. Internet of Things and Edge Computing Journal 2021, 1(2), 1–10.
6. Raparthi, M. Real-Time AI Decision Making in IoT with Quantum Computing: Investigating & Exploring the Development and Implementation of Quantum-Supported AI Inference Systems for IoT Applications. Internet of Things and Edge Computing Journal 2021, 1(1), 18–27.
7. Shiwlani, A.; et al. Synergies of AI and Smart Technology: Revolutionizing Cancer Medicine, Vaccine Development, and Patient Care. International Journal of Social, Humanities and Life Sciences 2023, 1(1), 10–18.
8. Paul, A.L. Quantum Cryptography: The Future of Secure Data Transmission. ResearchGate 2024. https://www.researchgate.net/publication/380720723_Quantum_Cryptography_The_Future_of_Secure_Data_Transmission
9. Paul, A.L. Impact of Quantum Computing on Data Encryption. ResearchGate 2024. https://www.researchgate.net/publication/380972947_Impact_of_Quantum_Computing_on_Data_Encryption