Received: 2025-08-28
Accepted: 2025-08-31
Published Online: 2025-12-30
DOI: 10.70454/JRIST.2025.10204

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

Post Quantum Cryptography on Healthcare Security: Safeguarding Patient Data in Medical Systems

Shubham Kumar

Sr Associate- Projects, Cognizant Technology Solutions MBP Tech Park, Nagavara, Bengaluru, Karnataka – 560045.

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Quantum computers are capable of solving problems that classical computers cannot, particularly in the realm of cryptographic algorithms such as RSA, DSA, and ECC. Post quantum cryptography refers classical cryptographic algorithm that are designed to secure sensitive data. This research explores the application of post-quantum cryptographic techniques in healthcare systems, with a specific focus on integrating Quantum Key Distribution (QKD) with Genetic Algorithms (GA) for enhanced key optimization. As quantum computing advances, traditional cryptographic systems employed in health care are more and more vulnerable to being broken. Security of sensitive patient information—like electronic health records (EHRs), diagnostic data, and personally identifiable information— requires strong solutions that can handle future quantum attacks. Post-quantum cryptography (PQC) provides a hopeful way forward by employing quantum computer-resistant algorithms. This paper investigates the deployment of PQC methods—e.g., lattice-based, hash-based, and multivariate polynomial cryptography—inside healthcare systems to improve data confidentiality, integrity, and availability. It assesses the weaknesses of present encryption technologies and introduces PQC as a necessary update to protect patient information from sophisticated cyberattacks. The study also addresses the interoperability, computational overhead, and infrastructure readiness challenges of implementing PQC in healthcare. By implementing quantum-resilient cryptographic protocols, healthcare facilities are able to future-proof data protection practices and guarantee the safeguarding of patient data in an era governed by quantum computing.

Keywords: Post Quantum Cryptography, Healthcare Security, Quantum Key Distribution, Genetic Algorithms, Quantum Computing

I. Introduction

This article explains how healthcare systems are shifting towards leveraging quantum technologies and how there is a necessity to enhance security to safeguard sensitive medical information. It analyses recent cryptographic techniques (techniques for encrypting data), such as lattice-based, code-based, hash-based, and multivariate polynomial cryptography, and how these can contribute to safeguarding healthcare information from emerging threats.

This research highlights the potential threat of quantum computers to the encryption techniques currently used, which can render them open to attack. This highlights the need to maintain security strategies within healthcare to avert these novel threats. The article also identifies issues for healthcare organizations when implementing these new security strategies, including compatibility challenges, financial restraints, and the requirement of specialized knowledge and training

Healthcare systems use technology to protect patient information. System authentication, email and Internet protection, and data protection when stored or transmitted (such as in phone calls or messaging) use digital signatures. Encryption (a process of enciphering information to secure it) is utilized by healthcare organizations to protect sensitive information such as patient ID and health information.

Common encryption techniques employed in healthcare include SHA-1, SHA-2, Triple DES, AES, MD-5, and RSA. These are tailored to protect data from being accessed by unauthorized parties. With healthcare systems collecting an increasing amount of data, these conventional techniques are now starting to struggle with keeping up with the growing amount of private data. This is particularly vital in sensitive domains, such as neonatal and mother-infant care, where it is important to protect family health data [1].

With the pace of cyber threats parallel to that of technological advancements, there is a need for quantum cryptography. The health sector is a top priority for hackers in terms of age. In the initial stages of digitization, the health infrastructure was mostly hit by basic malware and viruses, affecting their operations. With electronic health records going viral in the 2000s, data leaks and identity theft became critical issues. The 2010s witnessed a rise in ransomware attacks, with cases such as the Wanna Cry attack bringing healthcare institutions worldwide to their knees in 2017. Advanced threats have surfaced in recent times, such as AI-driven attacks and the hacking of Internet of Medical Things (IoMT) devices. This escalating race for arms between cybercriminals and health care security has put into the limelight the limitations of traditional encryption methods. Thus, safer alternatives have become the need of time, paving the way for quantum cryptography as a security solution to meet future challenges in healthcare.

A. Cryptography

is the art of securing messages such that only the intended recipient can read them, even if someone else tries to intercept them. This comes from the Greek words kryptos (secret) and graphein (to write). The process works by encrypting (or coding) a message into something unreadable (called a cipher), and then the recipient decrypts it back into the original message using a special "key."

There are two main types of cryptographic methods.

- **Private (symmetric) Key Cryptography:** In system, the same key is used to encrypt and decrypt the message. It is similar to having a secret password that both you and the recipient share. If someone tries to intercept a message, they cannot read it without the secret key. An example is XOR encryption, in which the message is mixed with the key, and the recipient uses the same key to reverse the process and obtain the original message.

- **Public Key cryptography:** This system uses two keys. One is public and can be shared freely to encrypt messages, and the other is private and kept confidential to decrypt them. Even if someone knows the public key, they cannot decrypt the message without using the private key. Public key cryptography is more complex and includes methods such as RSA and Diffie Hellman to securely share keys over the internet.

- **Quantum cryptography:** Quantum cryptography is a specialized domain in cryptographic science that leverages the foundational principles of quantum mechanics to establish secure communication channels. In contrast to conventional cryptographic methods that rely on computational complexity for encryption, quantum cryptographic systems exploit the intrinsic properties of quantum states, such as superposition and wave-particle duality, to ensure information security.

Quantum key distribution (QKD) is a fundamental mechanism within quantum cryptography that facilitates the establishment of a shared cryptographic key between communicating entities while guaranteeing the detection of any unauthorized interception attempts. The security paradigm of QKD is inherently grounded in the principles of quantum uncertainty and non clonability, as dictated by Heisenberg's uncertainty relationship and the phenomenon of quantum entanglement. These properties ensure that any perturbation introduced by an eavesdropper alters the quantum state of the transmitted particles, thereby revealing their presence and preserving the integrity of communication.

B. Cryptographic Resilience: Quantum computing provides advanced encryption methods, such as Quantum Key Distribution (QKD), to protect sensitive data (such as Electronic Health Records). These methods secure both current and future data against cyber-attacks. When used effectively, quantum computing strengthens cybersecurity, making systems faster, more accurate, and more prepared for cyber threats. This is expected to be a key part of future cybersecurity strategies [4]. Shor's algorithm shows that traditional cryptography systems can be broken down by quantum computers, creating security risks. To solve this problem, Ajtai introduced lattice-based cryptography in 1996, which is more difficult for quantum computers to crack. Unlike traditional systems, which rely on average-case security, lattice-based systems rely on the most difficult problems, making them more resistant to quantum attacks. Key problems in lattice-based cryptography include the closest vector problem (CVP), shortest integer solution (SIS), shortest vector problem (SVP), and learning with errors (LWE). Based on these tough problems, a lattice-based group authentication (LBA) scheme was developed to provide strong quantum-resistant security for healthcare applications
[5].

II. Related Work:

In year 2025, Postquantum cryptography (PQC) is crucial for protecting telemedicine data against forthcoming quantum attacks. This study identifies weaknesses in present-day encryption by employing U.S. HHS breach data and finds that enhanced encryption alone cannot cut it—ISSUE like insider threats and phishing also underpin breaches. Weak negative correlation (r = -0.087) implies that encryption saves the day but is not enough defense alone. The research compares four NIST-endorsed PQC algorithms—Kyber, Dilithium, Falcon, and SPHINCS+—on the basis of performance indicators like speed and storage. Through ANOVA, Falcon is the most efficient one, with high processing speeds and low storage space usage, best suited for real-time healthcare. HIMSS Cybersecurity Survey institutional readiness scores identify infrastructure and skill as the major drivers of PQC uptake. Guided by findings, the research suggests using Falcon for telemedicine encryption. It also focuses on enhancing key management and resolving system misconfigurations to minimize breach threats. These strategies together improve telehealth resilience[1]. This research is regarding the development of a safe system for handling patients' login information while using electronic health records (EHRS). system employs a system known as blockchain, where the patient's data and how it is connected with other data pieces (such as other records or information) is stored. Each data piece (referred to as a block) is attached to other data pieces, creating a network whereby the patients control their data, sharing and storing it safely. Patients will receive their own login credentials to access their medical history. This is to make sure that only authorized people are able to view the records. In order to protect the data, the system employs encryption (a method of converting data so that it is not readable unless with the proper key). It employs two methods of encryption:

Symmetric encryption: This is where the same key is employed to lock and unlock the data. Asymmetric encryption: It employs two different keys—one for encrypting the data and the other for decrypting it. Hospital and Patient Roles: Some information is stored on the hospital server, while patients manage their information. This makes the information safe to exchange among them [2]. In this research, the use of quantum nanosensors to track mental health conditions such as stress, anxiety, depression, and postpartum depression with great accuracy is suggested. The sensors offer continuous and real-time tracking that helps in early diagnosis and interventions at the right time. They respond to the immense need for mental health services in the U.S. by providing individualized and precise treatment. Robust encryption mechanisms help maintain patient information safely. The technology transforms mental health care by enhancing diagnosis, treatment, and data security for smart hospitals [3]. This article discusses the increasing issue of cyberattacks against patient information, i.e., Electronic Health Records (EHR), which results in severe complications such as data breaches and ransomware attacks. It proposes incorporating cutting-edge technologies such as quantum computing and machine learning to build a more secure cybersecurity framework for EHRs. Quantum algorithms such as Quantum Support Vector Machines (QSVM) and Grover's Search can be employed to identify, prevent, and forecast cyberattacks. The paper also examines how this new system functions in practical situations, how it compares with the old models, and presents pragmatic solutions to improve security [4]. The "quantum crisis" might render existing healthcare security systems obsolete, compromising patient safety and confidentiality. Quantum computing might shatter conventional encryption, enabling cyberattacks on hospital networks and medical devices. To solve this, a new lattice-based post-quantum group authentication protocol is presented for healthcare with enhanced security. The protocol is secure against general attacks such as replay and man-in-the-middle. It also needs less computational power and communication, thus being more efficient and secure compared to existing techniques [5]. The healthcare digitization has produced a sudden boost in electronic health records (EHRs) and medical information systems, enhancing healthcare services while also subjecting institutions to even more sophisticated cyber threats. Modern security systems have a hard time keeping pace with contemporary cyberattacks, as perpetrators of cybercrime take advantage of vulnerabilities in the existing encryption process. Quantum computing offers a compelling solution to the above issues. As compared to normal computers that employ binary information (0s and 1s), quantum computers employ quantum bits (qubits) which can have many states simultaneously, allowing them to process faster and solve problems faster. Quantum computing is best suited for designing superior encryption techniques, enhancing data protection, and securing healthcare systems from cyberattacks [6]. Quantum machine learning (QML) is an application of combining machine learning with quantum computing in order to better process large-scale healthcare data. This technology has the potential to enhance patient treatments through more precise examination of large sets of medical information. There are, however, issues with utilizing QML for healthcare, such as privacy issues and ethical questions. The article discusses recent advancements in QML, such as quantum neural networks and quantum generative models, and their likely applications. The article also considers how QML can augment machine learning, concentrating on the VQC algorithm. In total, QML can revolutionize healthcare by enhancing data processing and clinical applications [8]. Quantum computing is going to revolutionize the medical world entirely, rendering classical computing obsolete. Pattern recognition and predictive analysis are just two kinds of work that quantum computing might accelerate substantially. By contrast,

Received: 2025-08-28
Accepted: 2025-08-31
Published Online: 2025-12-30
DOI: 10.70454/JRIST.2025.10204

classical computing, driven by artificial intelligence approaches like machine and deep learning, mainly relies on large datasets to supply these types of operations. This innovation is expected to allow true-time visualization of intricate medical records, ensuing quicker and more precise diagnostics through genetics and imaging data. With the use of mathematical strength of quantum computing, health practitioners can look forward to serious progress in customized medicine, optimization of therapy, and overall patient care, that will enhance standards for medical services delivery. Essentially new and innovative partnerships exist between Quantum Computing and the medical sector. It was therefore only a matter of decades when the medical field was dramatically altered by quantum computing. The emergence of quantum technology is to usher in a whole new era of computation. Although a scientific topic per se, the rules of quantum mechanics and technologies hold the ability to revolutionize all manner of industries, including healthcare. Quantum convergence offers tremendous possibilities across the entire medical field. In addition, technologies as a whole and AI specifically have brought significant enhancements to the healthcare field. These technologies are being applied and revolutionizing the healthcare sector to deliver better care, aid, and diagnosis. Similarly, quantum computing is expected to change the way it is utilized in the healthcare sector. Today, individualized medicine based on pharmaceutical kinetics human physiology and genomics is the norm. Thus quantum computing is a perfect means of doing this [9]. The healthcare sector requires robust encryption techniques to secure sensitive information from misuse. Various cryptography methods, such as lattice cryptography, identity-based cryptography, and visual cryptography, secure data. Quantum cryptography provides unparalleled security, whereas identity-based cryptography provides data access based on users' roles. Visual cryptography secures visual information by transforming it into another form, which can be decrypted back to its original state. Even with these developments, there are still weaknesses in healthcare systems. This chapter contrasts these cryptography techniques, noting their strengths and weaknesses, and proposes enhancements for improved data security in healthcare [10].

In year 2024, This paper talks about the need to improve cybersecurity in healthcare as technology advances, especially with the rise of quantum computing. Quantum computers have the potential to break current encryption methods used to protect sensitive medical data. The paper discusses different types of advanced encryption methods that can withstand quantum attacks, such as lattice-based and code-based cryptography. It also highlights the challenges healthcare systems face in adopting these new methods, like compatibility issues, high costs, and the need for specialized training. The paper stresses the importance of adopting these new security measures soon to protect healthcare data from future risks [11]. This article discusses how smart healthcare systems (SHS) use IoT to collect and analyze health data for better treatment. It highlights the security challenges, as quantum computers can break traditional encryption methods like discrete logarithms. To address this, the article proposes a blockchain based solution with a secure key exchange protocol using lattice-based cryptography. Blockchain helps detect errors in medical data and improves security, transparency, and efficiency. The protocol’s security is proven in theory and against common attacks. It also performs better than previous methods in terms of cost and efficiency [12]. This paper explores how blockchain technology, combined with post-quantum cryptography (PQC), can improve the security and privacy of patient data in healthcare. By using a permissioned blockchain, sensitive data is securely stored. The paper uses discrete event simulation (DES) to evaluate blockchain transactions, patient data requests, and data encryption. The simulation shows how the combination of PQC and blockchain can address key issues related to the integrity and confidentiality of shared patient data, enhancing the overall management of healthcare information [13]. The Internet of Things (IoT) has transformed healthcare, facilitating remote patient monitoring, enhanced medication adherence, and chronic disease management. However, this interconnected ecosystem faces significant vulnerabilities with the advent of quantum computing, which threatens to break existing encryption standards protecting sensitive patient data in IoT-enabled medical devices. This chapter examines the quantum threat to healthcare IoT security, highlighting the potential impacts of compromised encryption, including privacy breaches, device failures, and manipulated medical records. It introduces post-quantum cryptography (PQC) and quantum-resistant techniques like quantum key distribution (QKD), addressing their application in resource-constrained healthcare IoT devices such as pacemakers, monitoring tools, and telemedicine systems. The chapter further explores the challenges of integrating these solutions and reviews global efforts in mitigating quantum risks, offering insights into suitable PQC primitives for various healthcare use cases [14]. This study proposes a new security protocol for intelligent healthcare systems to protect patient data from quantum computing threats. The protocol uses attribute-based authentication without certificates, ensuring secure communication and access control. It aims to replace traditional cryptographic systems that are vulnerable to quantum attacks. The approach improves the efficiency and security of medical data exchanges. Overall, it provides a more reliable solution for secure communication in healthcare [15]. This paper discusses the growing need to strengthen cybersecurity in healthcare as quantum technologies emerge. It explores post quantum cryptographic methods like lattice-based, code-based, hash-based, and multivariate polynomial encryption to secure sensitive medical data. The paper highlights the challenges healthcare systems face in adopting these new methods, such as compatibility issues, cost, and the need for specialized training. It also addresses the risks posed by quantum computing and the vulnerabilities in current encryption methods [16]. This paper focuses on securing smart healthcare systems that use IoT devices and wearables. It points out that traditional encryption methods are vulnerable to quantum attacks and suggests using lattice-based cryptography (LBC) as a safer alternative. The paper proposes a secure communication system for healthcare, including a key exchange protocol for internal communication and a post-quantum blockchain for external communication. The new blockchain system uses a lattice-based signature instead of the current ECDSA method. Overall, the goal is to ensure trust, security, and privacy in smart healthcare data [17]. This paper addresses security concerns in the healthcare sector as it adopts the Internet of Medical Things (IoMT). While IoMT improves productivity, current authentication methods are weak and vulnerable to data breaches, especially with simple passwords. The paper proposes a new authentication protocol that ensures the confidentiality and integrity of medical data. This protocol strengthens security by validating both user and device identities, using post-quantum cryptography to prepare for future quantum computing threats. The goal is to improve protection for sensitive medical data in the evolving digital healthcare environment [18]. Recent advancements in AI and quantum computing have significantly influenced quantum cryptography. AI-driven techniques enhance cryptographic efficiency and robustness, offering innovative security solutions. However, the rise of quantum computers poses a major challenge to traditional encryption methods, known as the ‘quantum threat.’ To counter this, researchers explore neural network-based AI to develop more secure cryptographic models. AI can optimize key distribution, detect vulnerabilities, and improve quantum-resistant algorithms. Despite challenges, integrating AI in cryptography holds promise for future digital security paradigms. This interdisciplinary research area continues to evolve, shaping the future of secure communication [19].

In year 2023, This study addresses security challenges in Internet of Things (IoT)-based healthcare systems, where medical devices handle sensitive patient data. Existing authentication methods, based on integer factorization and discrete logarithm problems, are vulnerable to quantum computing. The researchers analyzed a proposed lattice-based authentication scheme by Gupta et al. and found several vulnerabilities, such as impersonation, de-synchronization, and smart card attacks. To improve security, they propose a new authentication and access control scheme using Saber, a lattice-based cryptographic algorithm resistant to quantum attacks. The new scheme is simpler, more efficient, and tailored for e health systems. It provides better protection against the vulnerabilities identified in Gupta et al.'s scheme. The proposed system was implemented in the Vivado 2018.3 environment for Zynq UltraScale FPGAs. Performance comparisons with existing protocols showed that it offers enhanced security and efficiency. Overall, this solution strengthens the privacy and security of medical IoT systems [20]. This study presents a secure method for transmitting medical data in IoT healthcare systems by combining hybrid encryption, post-quantum cryptography, and deep learning techniques. The medical data is first transformed into binary form and categorized. Hybrid encryption using RSA and Twofish secures odd positions, while NTRU Encrypt is applied to even positions. A deep learning model, combining Bi-LSTM and CNN, is used for key selection. The ciphertexts from RSA-Twofish and NTRU Encrypt are merged with secure multiparty computation. Non-interest regions are extracted using an optimized U-Net model with the Self-Improved Butterfly Optimization Algorithm. Lattice based coding and hyperelliptic curve cryptography further secure the data. Watermarking is applied to medical images to ensure confidentiality and integrity. Image compression using HEVC reduces storage needs while maintaining quality. Secure cloud storage and blockchain integration ensure data integrity and access control. The process is reversed at the receiving end to securely retrieve and decrypt the data [21]. Traditional digital signatures face challenges on low-end IoT devices due to resource constraints, while quantum computing threats demand post-quantum cryptographic (PQC) alternatives. However, PQC signatures typically incur high costs, making them impractical for IoT applications like wearables and smart sensors. LightQSign (LightQS) addresses this by introducing a lightweight PQ signature scheme with minimal hash operations per signing process. It enables one-time public key derivation without external verifiers, reducing security risks and cryptographic overhead. LightQS achieves 20x faster signing with smaller keys compared to NIST PQC standards. Security proofs in the random oracle model validate its robustness. Experiments on 8-bit microcontrollers confirm its efficiency, making it ideal for resource-constrained IoT environments [22]. Cryptography plays a vital role in ensuring confidentiality, integrity, authentication, and non-repudiation in daily life. However, the rise of quantum computing threatens traditional encryption, leading to the exploration of quantum-resistant methods. Quantum key distribution (QKD) leverages quantum mechanics for secure key exchange, while post-quantum encryption (PQC) relies on mathematical problems that quantum computers cannot efficiently solve. This study reviews PQC from the perspective of traditional cryptography, examining its development and significance. It specifically focuses on Kyber, a leading PQC algorithm, analyzing its security and performance. Additionally, the study highlights the challenges and advancements in this field. Finally, future trends and predictions for PQC development are discussed [23]. Medical cyber-physical systems (MCPSs) enhance smart healthcare by enabling seamless patient system interaction, requiring a secure authentication mechanism to protect sensitive medical data. This research proposes an efficient authentication and encryption system (EAES) to enhance security in MCPSs. A modified elliptic-curve Diffie–Hellman (ECDH) encryption is applied to secure patient data stored in the cloud, ensuring controlled access for medical analysis. Quantum key distribution (QKD) manages encryption keys to strengthen data protection. Additionally, blockchain technology is integrated for mutual authentication of users within MCPSs. The proposed system is implemented and evaluated using performance metrics. Finally, its effectiveness is compared with conventional security techniques [24]. Security and privacy are critical in healthcare, requiring secure access to sensitive patient data. This research implements an improved Quaternion-based neural network with blockchain to enhance data protection. Quaternion neural network cryptography is used to encrypt shared health data before storing it in the cloud, while blockchain securely stores encryption keys in blocks, utilizing the SHA algorithm for key event identification. A modified genetic algorithm generates encryption and decryption keys, ensuring secure access. Authorized patients and physicians can decrypt and download medical data using the stored key. The proposed system is evaluated for encryption time and cost, demonstrating improved efficiency. Results show reduced encryption time, decryption time, and transaction costs compared to existing methods [25]. The rise of large quantum computers poses a significant threat to cryptography, making most symmetric and asymmetric algorithms vulnerable. Grover's algorithm accelerates key searching in symmetric schemes like AES and 3DES, while Shor's algorithm efficiently breaks asymmetric cryptosystems such as RSA, Diffie-Hellman, and ECC by solving prime factorization and discrete logarithm problems in polynomial time. This paper examines the vulnerabilities of classical cryptosystems in the quantum era and explores various post quantum cryptographic (PQC) families. It also reviews the ongoing NIST PQC standardization process and compares the performance of PQC algorithms across different platforms. Finally, the paper highlights key future research directions in post-quantum cryptography [26]. Future quantum computers will compromise common cryptographic algorithms, posing a significant threat to network security. Therefore, researching quantum-safe cryptography and assessing the security of traditional cryptographic methods have become urgent. This paper explores quantum-safe cryptographic approaches, surveying various quantum key distribution (QKD) protocols, simulation tools, and commercial applications. Additionally, it compares the first four post-quantum cryptographic (PQC) algorithms recently announced by the National Institute of Standards and Technology (NIST). The study also discusses challenges in quantum safe cryptography, highlighting key research directions for the future development of secure cryptographic solutions [27]. This paper discusses the role of quantum computing in healthcare data security and management. It highlights the growing reliance on cryptographic systems to protect patient information and the increasing challenge of handling large healthcare data efficiently. As traditional computational systems may become inadequate, quantum computing is explored as a potential solution for data storage, retrieval, and security. The study reviews current challenges, available options, and future possibilities for using quantum algorithms in large-scale healthcare systems, based on clinical studies and literature reviews [28].

In year 2021, Kalaivani, V. addresses the critical security threat of secure key distribution in wireless body sensor networks (WBSNs). Traditional methods like email or phone risk key interception, leading to potential medical data breaches and severe consequences. To counter this, an enhanced BB84 Quantum Cryptography Protocol (EBB84QCP) is proposed, integrating quantum theory with a bitwise operator for secure key sharing. This approach eliminates direct key transmission, making hacking nearly impossible. The method is designed to be efficient, considering the resource constraints of body sensors. Experimental results confirm its effectiveness in securely distributing secret keys for sensitive medical data transmission [29]. Malina, L., Dzurenda, etc. all focuses on privacy protection in Intelligent Infrastructure (II) services within the Internet of Things (IoT), with a strong emphasis on post quantum cryptography (PQC). It surveys security threats, Privacy-Enhancing Technologies (PETs), and their effectiveness against future quantum computing attacks. The paper maps recent PET schemes based on post-quantum cryptographic primitives and explores their deployment in real-world IoT/II applications. A case study on the Internet of Vehicles (IoV) demonstrates PETs in action. It also examines regulatory challenges, including GDPR, and highlights the rising risks from data collection. Finally, the paper discusses the limitations of current PETs and suggests future research directions for post-quantum security solutions [30].

Cena,J., Oluwaseyi etc. all explores the role of post-quantum cryptography (PQC) and quantum encryption in securing microsphere-based drug delivery systems. It highlights the growing cyber threats to pharmaceutical research, manufacturing, and intellectual property. Quantum Key Distribution (QKD) ensures secure communication by detecting interception attempts, while PQC safeguards data against future quantum cyberattacks. The paper examines emerging trends, ethical considerations, and real-world applications of quantum encryption in drug development and personalized medicine. By integrating these technologies, pharmaceutical security can be strengthened, ensuring regulatory compliance and data integrity [31].

In year 2020, Post-Quantum Cryptography (PQC) protects healthcare data from quantum threats by ensuring secure encryption and key exchange. Crystals-Kyber is used for secure communication in hospital networks, while Classic McEliece provides long-term security for patient records. SIKE was once considered for medical IoT security but has been broken. PQC enhances encryption for electronic health records, telemedicine, and remote patient monitoring systems. It also strengthens the security of medical IoT devices like pacemakers and wearables. By implementing PQC, healthcare systems can safeguard sensitive data and critical infrastructure from future quantum cyber risks [32]. Post-quantum cryptography (PQC) is crucial for protecting telemedicine data against forthcoming quantum attacks. This study identifies weaknesses in present-day encryption by employing U.S. HHS breach data and finds that enhanced encryption alone cannot cut it—ISSUE like insider threats and phishing also underpin breaches. Weak negative correlation (r = -0.087) implies that encryption saves the day but is not enough defense alone. The research compares four NIST-endorsed PQC algorithms- Kyber, Dilithium, Falcon, and SPHINCS+—on the basis of performance indicators like speed and storage. Through ANOVA, Falcon is the most efficient one, with high processing speeds and low storage space usage, best suited for real-time healthcare. HIMSS Cybersecurity Survey institutional readiness scores identify infrastructure and skill as the major drivers of PQC uptake. Guided by findings, the research suggests using Falcon for telemedicine encryption. It also focuses on enhancing key management and resolving system misconfigurations to minimize breach threats. These strategies together improve telehealth resilience[32]. With quantum computation advancing, legacy encryption algorithms such as RSA, ElGamal, and Paillier get exposed further and further. For this reason, the work presents a lattice-based homomorphic encryption scheme resistant to quantum attacks. This post-quantum encryption facilitates computations over encrypted information, making it secure for applications sensitive to privacy. The research has mathematical confirmations, practical demonstration, and security analysis in depth. While not explicitly healthcare-oriented, the scheme is highly compatible with healthcare requirements, particularly in federated learning scenarios. The systems are employed to process medical information without invading patient privacy. The solution suggested improves security while preserving functionality. It provides a future-proof alternative for secure collaborative data processing in sensitive areas[33] The Internet of Things (IoT) has revolutionized healthcare through remote patient monitoring, improved medication adherence, and the management of chronic diseases. Still, the networked ecosystem of IoT confronts tremendous weaknesses with the emergence of quantum computing, which risks crumbling current encryption protocols safeguarding sensitive patient information in IoT connected medical devices. This chapter discusses the quantum threat to healthcare IoT security, emphasizing the possible effects of broken encryption, such as privacy invasions, device malfunctions, and doctored medical records. It presents post-quantum cryptography (PQC) and quantum-resistant methods such as quantum key distribution (QKD), discussing their use in resource-limited healthcare IoT devices such as pacemakers, monitoring devices, and telemedicine devices. The chapter also discusses the challenges of implementing these solutions and surveys worldwide initiatives in countering quantum threats, providing insights into appropriate PQC primitives for different healthcare applications[34]. Quantum computing poses a serious threat to traditional encryption algorithms such as RSA and ECC, which depend on mathematical issues quantum algorithms have an efficient way of solving. Shor's algorithm, among others, directly undermines the roots of these systems' security. Post-quantum cryptography (PQC) has arisen, therefore, with the aim of creating algorithms resilient to such an attack. This research delves into how quantum computing threatens

Received: 2025-08-28
Accepted: 2025-08-31
Published Online: 2025-12-30
DOI: 10.70454/JRIST.2025.10204

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

classical cryptography and provides essential PQC methods, such as lattice-based, code-based, hash-based, and multivariate polynomial cryptography. It highlights PQC's imperative importance in maintaining data confidentiality and integrity. As quantum threats increase, PQC provides secure digital communication. Its implementation is imperative for future cybersecurity resilience [35].

III. Background Work

A. Post-Quantum cryptography

Quantum cryptography is an advanced technology in network security that facilitates secure communication between a sender and receiver based on the principles of quantum physics. Stephen Wiesner first introduced the concept in the 1970s. Subsequently, Charles H. Bennett of IBM and Gilles Brassard of the University of Montreal collaborated with Wiesner to expand upon the Quantum Key Distribution (QKD) technique, which resulted in the establishment of the BB84 protocol in 1984. Of all the quantum cryptography techniques, the BB84 protocol is the foundational method that takes advantage of the distinctive nature of quantum light to provide total security and confidentiality for classical information. Quantum communication commonly uses free space transmission, and for satellite-based communication, any attack can be detected by classical channel monitoring methods. Furthermore, the use of simplified protocols and hardware for quantum communication can improve the rate of key generation.

The QKD protocol involves Rahul sending a series of single qubits, and each is prepared in accordance with independently selected quantum states { |↑>,|→>,| >,| > }. Shivam, the receiver, measures every qubit based on an independently chosen basis. Rahul and Shivam then communicate with one another for every encoded qubit to determine if their choices were similar. According to a subset of their data, they determine if their choices were identical. If the results fall within a certain range, the transmission is secure; otherwise, it shows that there is an intruder attempting to intercept the communication

Quantum computing has the ability to create strings of maximally entangled states such as

$(|00\rangle + |11\rangle) / \sqrt{2}$. Rahul and Shivam both measure the entangled qubits in randomly chosen bases, a crucial step in arriving at a common secure key.

Quantum Key Distribution employs the polarization properties of quantum states to ensure secure data exchange between Rahul and Shivam. The process generally takes the following steps:

- Rahul generates a random bit sequence and maps them into quantum states (photons), which are transmitted to Shivam.

- Shivam gets the photons and randomly selects a basis to decrypt each bit.

- The two parties then exchange information through a classical channel to match on which bits were each measured with the same basis.

- If their comparison error rate is below a certain threshold, the experiment is said to have succeeded and shows a secure key exchange.

Received: 2025-08-28
Accepted: 2025-08-31
Published Online: 2025-12-30
DOI: 10.70454/JRIST.2025.10204

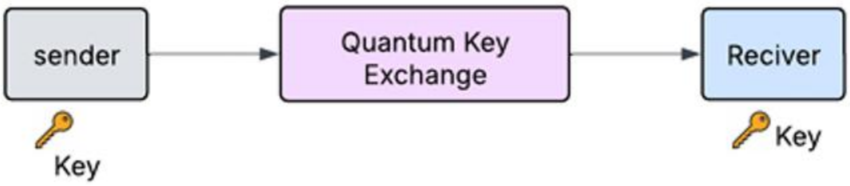


Fig 1: Quantum key exchange flow diagram with keys.

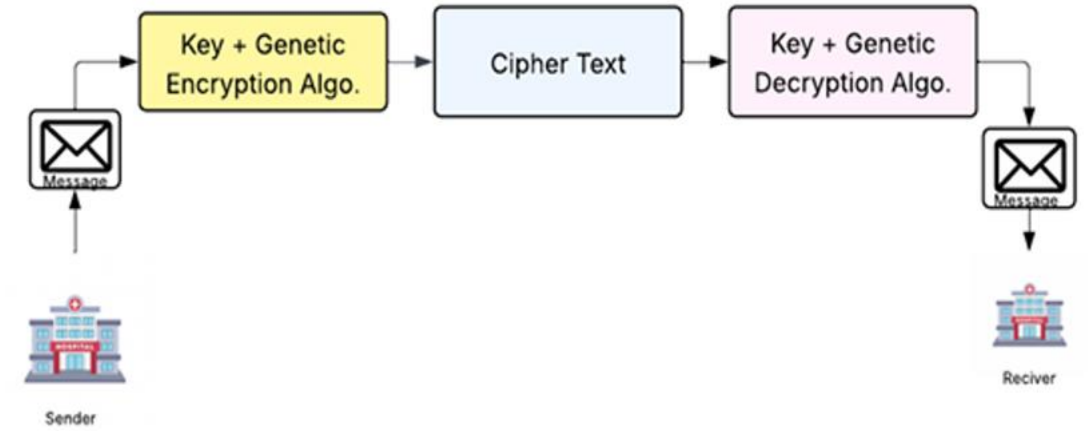

Key + Genetic Encryption Algo.
Cipher Text
Key + Genetic Decryption Algo.
Message
Message
Sender
Reciver

Fig 2: Data Communication flow diagram between sender and receiver

Table 1. Key Exchange Using Quantum Channel

Rahul String	1	1		0	1	0	0	1	0	1	1	1	1	0	0
Rahul basis	+	+		+	X	X	+	X	X	X	X	+	+	+	+
Rahul send	-	-		|	\	/	|	\	/	\	\	-	-	|	|
Shivam's Basis	+	X		+	+	X	+	X	+	X	X	+	+	+	+
Shivam's String	1	0		0	1	0	0	1	1	1	1	1	1	0	0
Same Basis?	Y	N		Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Bits To Keep	1			0		1	0	1		1	1	1	1	1	1
Test	Y			N		N	Y	N		N	N	N	Y	Y	N
Key				0		1		1		1	1	1			0

This method ensures that any attempt at eavesdropping can be detected, maintaining the integrity and confidentiality of the communication.

Algorithm

```
Key_Generation(){
    Step 1:
        Rahul generates  a random binary sequence For each bit in a
        • Rb[i] = Random_basis(a[i])
        • P1[i] = Polarized_photons(Rb[i])
        Rahul sends the polarized photons P1 to Shivam through a quantum channel.

    Step 2:
        Shivam receives the polarized photons P1 from a. Rahul. For each photon in P1:
        • Rb[j] = Random_basis(P1)
        • P2 = Polarized_photons(Rb[j])
}
```

Afterward, both Rahul and Shivam compare their polarized photon data over a classical communication channel. They identify the common elements in P1 and P2, noted as P1 ∩ P2 = x, where x becomes the shared key used for encryption and decryption.

B. Genetic Algorithm

A genetic algorithm is a search procedure based on the concept of natural selection and genetics. the theory behind genetic algorithms is borrowed from Charles Darwin's theory of evolution. It follows the thought process that only those are optimally fit for survival and transfer their traits to the next generation under the system of natural selection. As explained by Tomassini, the general principle here is that a population of beings must behave to evolve and undergo change over a period of time in the manner natural systems adapt.

A genetic algorithm typically starts off with a population of people who are generated at random. After the initial population has been set up, the algorithm proceeds into a loop that is repeated. In each loop, referred to as a generation, a new population of people is created based on applying a sequence of random (stochastic) operations to the current population. This process is repeated through numerous generations.

Steps Involved in Genetic Algorithm:

- **Step I:** The process starts by using a random generator to create an initial population made up of P chromosomes. Within this population, chromosomes with beneficial traits are encouraged to survive and reproduce, while those with ineffective characteristics are gradually removed.
- **Step II:** The population changes with time by using the random operators repeatedly, commonly involving mutation, crossover, and selection, to generate new offspring from the current individuals.
- **Step III:** Selection is based on a fitness function, which measures and assigns a fitness value— typically in the form of a real number—to each chromosome based on its performance or fit towards the desired objective.

IV. Proposed work

Pseudocode of Proposed Algorithm

Step 1: Quantum Key Distribution (QKD) - QOST Protocol

1. Initialize Parameters

• Set n = 10 (number of qubits for QKD).

2. Rahul Generates Key and States

• Generate rahul_bits: Random sequence of n bits (0 or 1).

• Convert bits into rahul_states:

▪ 0 → $|0\rangle$ (Z-basis)

▪ 1 → $|+\rangle$ (X-basis)

3. Prepare Quantum Circuit for Rahul

• Create quantum circuit qc with n qubits.

• Encode Rahul's states:

▪ If rahul_states[i] is +, apply Hadamard (H gate) on qubit i.

4. Shivam Selects Measurement Basis

• Generate shivam_measurements as a random choice of Z-basis ($|0\rangle/|1\rangle$) or X-basis ($|+\rangle/|-\rangle$).

5. Shivam Measures in Chosen Basis

• If shivam_measurements[i] is X, apply Hadamard (H gate) before measurement.

6. Simulate Quantum Circuit Execution

• Use AerSimulator to execute qc.

• Retrieve measurement results as shivam_results.

7. Derive Shared Key

• Retain bits where Rahul and Shivam used the same basis:

▪ Rahul's 0 with Shivam's Z

▪ Rahul's + with Shivam's X

• Store the result as shared_key.

Step 2: Genetic Algorithm for Key Optimization

1. Define Target Message

• Set target_message = "HELLO".

• Convert each character to ASCII (target_bits).

2. Genetic Algorithm Setup

- Define fitness function:
- Encrypt target_bits using a candidate key (via XOR).
- Calculate score as the negative sum of absolute differences between encrypted and target_bits.
- Register GA components:
- Population: 50 individuals (random bit sequences of shared_key length)
- Selection: Tournament selection (size = 3).
- Crossover: One-point crossover.
- Mutation: Flip bit with probability 0.1.

3. Run Genetic Algorithm

- Initialize population.
- Execute GA for 20 generations with:
- Crossover probability = 0.7
- Mutation probability = 0.2

4. Retrieve Best Optimized Key

• Select best individual from the final population.

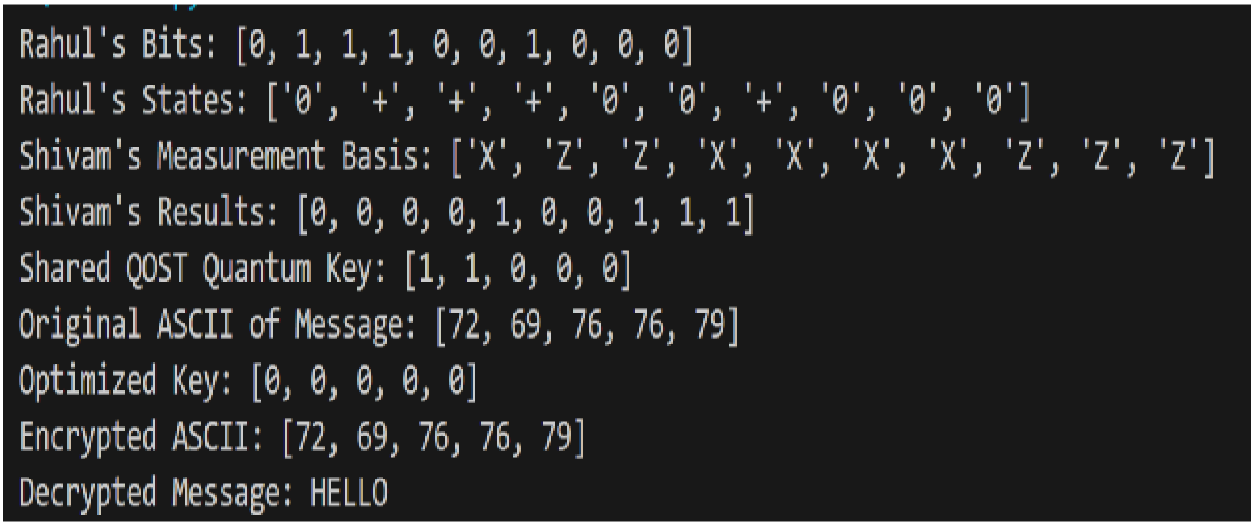
5. Encrypt & Decrypt Message Using Optimized Key

• XOR target_bits with optimized_key to generate encrypted_message.
• Decrypt by applying XOR again, converting ASCII back to characters (decrypted_message).

6. Output Results

• Print Optimized Key, Encrypted ASCII, and Decrypted Message.

V. Result and Discussion

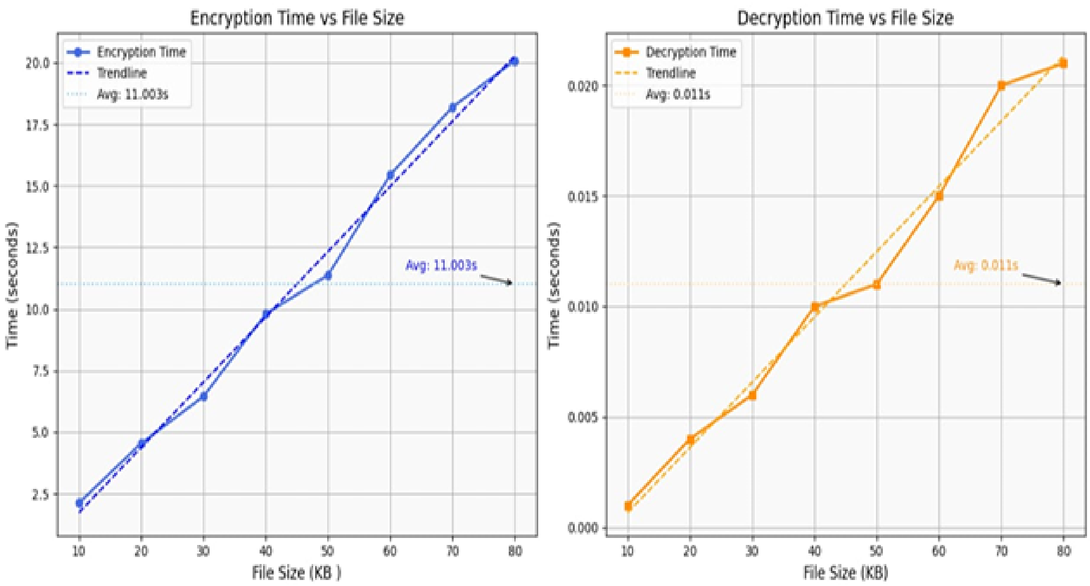


```
Rahul's Bits: [0, 1, 1, 1, 0, 0, 1, 0, 0, 0]
Rahul's States: ['0', '+', '+', '+', '0', '0', '+', '0', '0', '0']
Shivam's Measurement Basis: ['X', 'Z', 'Z', 'X', 'X', 'X', 'X', 'Z', 'Z', 'Z']
Shivam's Results: [0, 0, 0, 0, 1, 0, 0, 1, 1, 1]
Shared QOST Quantum Key: [1, 1, 0, 0, 0]
Original ASCII of Message: [72, 69, 76, 76, 79]
Optimized Key: [0, 0, 0, 0, 0]
Encrypted ASCII: [72, 69, 76, 76, 79]
Decrypted Message: HELLO
```

Fig 3: Output of Proposed Algorithm

Explanation of output

• Rahul sends qubits encoded with random bases and bits.
• Shivam measures with random bases.
• They compare which bases match and derive a shared secret key.
• Rahul encrypts the message using the key (XOR).
• Shivam uses the same key to decrypt i



This image contains two line graphs comparing encryption and decryption time versus file size. Here's a breakdown of each graph:

Left Graph: Encryption Time vs File Size

- X-axis (horizontal): File size in kilobytes (KB), ranging from 10 KB to 80 KB.
- Y-axis (vertical): Time in seconds taken for encryption.
- Blue solid line: Represents actual encryption times for different file sizes.
- Blue dashed line: A trendline showing the general pattern of the encryption time increase.
- Average Time: Labeled as Avg: 11.003s, shown as a horizontal dotted line.

Observation:

- Encryption time increases linearly with file size
- The trendline closely follows the actual data, indicating consistent performance scaling.
- The average encryption time is about 11 seconds.

Right Graph: Decryption Time vs File Size

- X-axis: Same file sizes (10 KB to 80 KB).
- Y-axis: Decryption time in seconds, but note the much smaller scale compared to encryption (in milliseconds range).
- Orange solid line: Actual decryption times.
- Orange dashed line: Trendline.
- Average Time: Labeled as Avg: 0.011s.

Observation:

- Decryption is extremely fast compared to encryption.
- Time also increases with file size but remains under 0.022 seconds even for 80 KB files.
- The average decryption time is just 0.011 seconds.

Conclusion

The rapid advancement of quantum computing poses a significant threat to conventional cryptographic mechanisms widely used in healthcare systems. This study highlights the urgent need to transition from traditional encryption schemes to post-quantum cryptographic (PQC) solutions to ensure long-term security of sensitive healthcare data. By examining quantum-resistant approaches such as lattice-based, hash-based, and multivariate polynomial cryptography, the research demonstrates how PQC can effectively address vulnerabilities in existing cryptographic infrastructures.

Furthermore, the integration of Quantum Key Distribution (QKD) with Genetic Algorithms (GA) presents a promising framework for secure and optimized key management, enhancing both robustness and adaptability against quantum-enabled attacks. Although challenges related to interoperability, computational overhead, and infrastructure readiness remain, the findings suggest that these obstacles can be mitigated through careful system design and phased implementation strategies.

Overall, adopting quantum-resilient cryptographic protocols is not merely a preventive measure but a necessary evolution in healthcare cybersecurity. Implementing PQC enables healthcare organizations to future-proof their data protection mechanisms, ensuring confidentiality, integrity, and availability of patient information in the emerging quantum era.

References

[1] Balogun, A. Y. Post-Quantum Cryptography and Encryption Standards: Safeguarding Patient Data against Emerging Cyber Threats in Telemedicine.(2025)

[2] Natarajan, M., Bharathi, A., Varun, C. S., & Selvarajan, S. (2025). Quantum secure patient login credential system using blockchain for electronic health record sharing framework. Scientific Reports, 15(1), 4023.

[3] Meikandan, P. V., Upama, P. B., Rabbani, M., Ahamad, M. M., & Ahamed, S. I. (2025). Quantum computing for smart healthcare. In Sensor Networks for Smart Hospitals (pp. 525 534). Elsevier.

[4] Ovabor, K., Owolabi, O. O., Atkison, T., Iledare, A., & Ijeoma, C. (2025). Quantum-driven predictive cybersecurity framework for safeguarding Electronic Health Records (EHR) and enhancing patient data privacy in healthcare systems.

[5] Prajapat, S., Thakur, G., Kumar, P., Das, A. K., Jamal, S. S., & Susilo, W. (2025). Designing lattice-enabled group authentication scheme based on post-quantum computing in healthcare applications. Computers and Electrical Engineering, 123, 110028.

[6] Jhessim, E., & Anku, V. (2025). Quantum computing for cybersecurity in healthcare systems: A multi-modal approach.

[7] Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post quantum cryptography for authentication and user privacy in IoT devices. Cluster Computing, 28(2), 93.

[8] Sonavane, A., Jaiswar, S., Mistry, M., Aylani, A., & Hajoary, D. (2025). Quantum machine learning models in healthcare: future trends and challenges in healthcare. Quantum Computing for Healthcare Data, 167-187.

[9] Singla, S., & Sodhi, N. S. (2025). Cryptography in practice. In Next Generation Mechanisms for Data Encryption (pp. 164-183). CRC Press.

[10] SaberiKamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. Heliyon, 10(10).

[11] Soni, L., Chandra, H., & Gupta, D. S. (2024). Post-quantum attack resilience blockchain assisted data authentication protocol for smart healthcare system. Software: Practice and Experience, 54(11), 2170-2190.

[12] Zhukabayeva, T., Ur Rehman, A., Tariq, N., & Benkhelifa, E. (2024). Hyperledger Fabric Based Post Quantum Cryptography Healthcare Application Using Discrete Event Simulation. IEEE Access.

[13] Alif, A., Hasan, K. F., Laeuchli, J., & Chowdhury, M. J. M. (2024). Quantum Threat in Healthcare IoT: Challenges and Mitigation Strategies. arXiv preprint arXiv:2412.05904.

[14] Ni, L., Gu, B., Liu, X., & Zhou, H. (2024, July). Post-Quantum Attribute-Based Authenticated Key Agreement Protocol for Smart Healthcare. In Proceedings of the 2024 6th International Conference on Big Data Engineering (pp. 33-38).

[15] SaberiKamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. Heliyon, 10(10).

[16] Boujelben, M., & Abid, M. (2024). Post-quantum security design for hierarchical healthcare systems based on lattices. The Journal of Supercomputing, 80(12), 17292-17313.

[17] Lo, C. K. M., Tan, S. F., & Chung, G. C. (2024, August). Enhanced Authentication Protocol for Securing Internet of Medical Things with Lightweight Post-Quantum Cryptography. In 2024 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET) (pp. 625-630). IEEE.

[18] Radanliev, P. (2024). Artificial intelligence and quantum cryptography. Journal of Analytical Science and Technology, 15(1), 4.

[19] Adeli, M., Bagheri, N., Maimani, H. R., Kumari, S., & Rodrigues, J. J. (2023). A post quantum compliant authentication scheme for IoT healthcare systems. IEEE Internet of Things Journal, 11(4), 6111-6118.

[20] Karthikeyan, D. (2023, December). Secure Medical Data Transmission In Iot Healthcare: Hybrid Encryption, Post-Quantum Cryptography, And Deep Learning-Enhanced Approach. In 2023 Global Conference on Information Technologies and Communications (GCITC) (pp. 1-12). IEEE.

[21] Yavuz, A. A., Darzi, S., & Nouma, S. E. (2023). Lightweight and Scalable Post-Quantum Authentication for Medical Internet of Things. arXiv preprint arXiv:2311.18674.

[22] Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., ... & Xiong, N. (2023). Post-quantum security: Opportunities and challenges. Sensors, 23(21), 8744.

[23] Gawali, P. P., Mahalle, P. N., Shinde, G. R., Sable, N. P., Takale, D. G., & Barot, J. (2023, August). Quantum Key Distribution and Blockchain Based Secure Authentication in Medical Cyber-Physical Systems. In International Conference on ICT for Sustainable Development (pp. 607-622). Singapore: Springer Nature Singapore.

[24] Suganthi, P., & Kavitha, R. (2023). Secure and privacy in healthcare data using quaternion based neural network cryptography with the blockchain mechanism. IETE Journal of Research, 69(10), 6997-7014.

[25] Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023, January). Post quantum cryptography: a review of techniques, challenges and standardizations. In 2023 International Conference on Information Networking (ICOIN) (pp. 146-151). IEEE.

Received: 2025-08-28
Accepted: 2025-08-31
Published Online: 2025-12-30
DOI: 10.70454/JRIST.2025.10204

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926, P- 3117-535X

[26] Xu, G., Mao, J., Sakk, E., & Wang, S. P. (2023, March). An overview of quantum-safe approaches: quantum key distribution and post-quantum cryptography. In 2023 57th Annual Conference on Information Sciences and Systems (CISS) (pp. 1-6). IEEE.

[27] Mantry, H., & Maheshwari, A. (2022). Quantum cryptography for securing personal health information in hospitals.

[28] Kalaivani, V. (2021). Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. Personal and ubiquitous computing, 27(3), 875.

[29] Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevičius, R., ... & Tang, Q. (2021). Post-quantum era privacy protection for intelligent infrastructures. IEEE Access, 9, 36038-36077.

[30] Cena, J., Oluwaseyi, J., & Emmanuel, O. K. (2021). Quantum-Enhanced Data Encryption for Protecting Microsphere-Based Drug Delivery Innovations.

[31] Kumar, M., & Pattnaik, P. (2020, September). Post quantum cryptography (pqc)-an overview. In 2020 IEEE High Performance Extreme Computing Conference (HPEC) (pp. 1-9). IEEE.

[32] Chen, A. C. (2024). Homomorphic Encryption Based on Lattice Post-Quantum Cryptography. arXiv preprint arXiv:2501.03249.

[33] Alif, A., Hasan, K. F., Laeuchli, J., & Chowdhury, M. J. M. (2024). Quantum Threat in Healthcare IoT: Challenges and Mitigation Strategies. arXiv preprint arXiv:2412.05904.

[34] Mamatha, G. S., Dimri, N., & Sinha, R. (2024). Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era. arXiv preprint arXiv:2403.11741.