A Quantum Safe Block-Chain Based Framework to Protect Patients Electronic Medical Information

K SHATVIK LAKSHMAN TEJA
PG Scholar
Department of Computer Science and Engineering
JNTUA College of Engineering, Anantapur
shatviklakshman@gmail.com

Dr. K. MADHAVI
Professor
Department of Computer Science and Engineering
JNTUA College of Engineering, Anantapur
kasamadhavi.cse@jntua.ac.in

Abstract—With the growing implementation of digital healthcare services and medical record maintenance, significant challenges have arisen concerning the privacy, security, and illegal use of sensitive health data. Blockchain technology provides a decentralized, transparent, and reliable platform for healthcare purposes; yet, several conventional healthcare blockchain frameworks are based on the classic cryptography scheme, including RSA and ECC, which can be easily broken by quantum computers. Hence, this paper suggests a quantum-resistant blockchain architecture for managing electronic medical data using post-quantum cryptography methods. The proposed approach uses the CRYSTALS-Kyber protocol for secure key exchange and FALCON for digital signature generation and verification, ensuring protection from both classical and quantum cyberattacks. The quantum-resistant blockchain architecture works solely on classical computing devices without the need for quantum computing components. Performance testing proves that the suggested approach exhibits high levels of security and computational efficiency. The encryption, decryption, key creation, and signature validation operations take negligible amounts of processing time, allowing the framework to be applied in real-time medical applications.

IndexTerms—Blockchain, Post-Quantum Cryptography, Healthcare Security, Quantum Computing, Kyber, Falcon.

I. INTRODUCTION

The fast evolution of healthcare systems into digitalization has revolutionized the handling of electronic medical information in terms of storage, processing, and distribution. The current state of healthcare infrastructure depends to a large extent on cloud computing, IoT of medical things, blockchain technology, and intelligent healthcare infrastructure for effective patient handling and provision of medical services. On the other hand, the reliance of the current healthcare systems on interconnected digital technology has resulted in severe security challenges associated with electronic health records, patient authentication, integrity of medical data, and illegal access to EHRs [2], [14], [17]. Blockchain technology has proven to be a useful tool for ensuring the safety of healthcare-related data due to its decentralization, immutability, transparency, and robustness against tampering. A number of studies have investigated the application of blockchain technology in securing healthcare data storage and access control [1], [4], [7], [16]. Healthcare systems based on blockchain technology do not have any point of failure, and they can effectively guarantee traceability of medical transactions. In addition, the development of IoMT and 6G enabled smart healthcare applications has increased the demand for reliable healthcare communication infrastructure [5]. Although these are the strengths of a blockchain architecture, almost all existing frameworks rely on traditional public-key cryptographic mechanisms like RSA and ECC. However, the traditional cryptosystems are prone to any future attacks that could arise with quantum computing technology since any quantum computation like the Shor's algorithm will enable efficient computations of problems of integer factorization and discrete logarithm [6], [9]. The ongoing development of quantum computing technologies poses a challenge to current security infrastructure in healthcare, which makes the data extremely vulnerable. The biggest challenge facing healthcare cyber security in modern times is the "harvest now decrypt later" attack approach, whereby any encrypted data collected from the healthcare system may be decrypted by quantum computing in the future [9], [15]. Because medical data consists of sensitive and lifelong personal data, maintaining long-term confidentiality is crucial. Thus, researchers have shifted their focus towards post-quantum cryptography and quantum resistant blockchain architectures [3], [8], and [13].Current research is being conducted regarding the convergence of blockchain and post-quantum security models for use in healthcare systems. For instance, Agarwal et al. [1] proposed a novel blockchain-based and quantum cryptographically secured framework for Healthcare 5.0 applications for secure communication. The post-quantum blockchain approach in combination with deep learning was also considered by Anbarkhan [3] to ensure secure IoT networks. The recent survey presented by Gharavi et al. [9] addressed the problem of post-quantum blockchain security for IoT applications, stressing on the need to utilize quantum-resistant cryptographic protocols. Moreover, Natarajan et al. [11] proposed an approach for secure login credentials in electronic health record sharing based on a quantum-secure framework. Moreover, current research focuses on privacy-preserving authentication, security, genome-based secure data management, and lightweight cryptography for modern healthcare infrastructures [4], [10], [12]. In particular, the issue of privacy-preserving post-quantum blockchain technologies and their potential challenges related to scalability, security, and implementation were considered in detail by Sezer et al. [15]. From the literature review, it is obvious that future healthcare infrastructures will require cryptographic solutions resistant against classical and quantum attacks.

In an attempt to solve the aforementioned issues, this paper introduces a framework for the quantum-resistant

blockchain-based management of medical information via the implementation of post-quantum cryptographic methods. The developed solution involves the use of CRYSTALS-Kyber for securing the process of quantum-resistant key exchange and FALCON for generating and verifying digital signatures.

The major contributions of this paper can be formulated as follows:

- The introduction of a framework involving the integration of a blockchain-based healthcare system with post-quantum cryptography for the purposes of providing secure management of medical data;
- The use of CRYSTALS-Kyber to implement the process of secure quantum-resistant key exchange and FALCON for digital signature generation/verification;
- The protection against quantum attacks and harvest-now-decrypt-later threats with no need for specialized quantum hardware;
- The efficient performance analysis proving that there is little encryption and verification overhead;

The rest of this paper is structured as follows. The literature survey on blockchain, healthcare security, and post-quantum cryptography is presented in Section II. Section III illustrates the methodology used and the system architecture proposed. Details of implementation and experimentation are presented in Section IV. Discussion and error analysis are presented in Section V, whereas conclusions are drawn in Section VI.

II. LITERATURE SURVEY

However, due to the accelerated use of these technologies, a need has arisen for secure mechanisms to protect the privacy of electronic medical data. Blockchain, IoMT, Cloud computing, and artificial intelligence are commonly used technologies for various applications in healthcare. Nevertheless, the use of these technologies poses significant risks in terms of cybersecurity and privacy issues related to health records, patient authentication, and secure data exchange [2], [14], [17]. Since blockchain is decentralized, transparent, and immutable, it offers an opportunity for a secure solution to healthcare problems. The authors have developed blockchain-based mechanisms for securing healthcare data and providing access to it [1], [4], [7], and [16]. Such a system can provide high data security by increasing its integrity and eliminating unauthorized changes. Thus, Agarwal et al. [1] offered a blockchain and quantum cryptography-based framework for the implementation of the Healthcare 5.0 system to increase communication and trust. Ajakwe et al. [2] considered several issues related to blockchain applications in medical IoT systems. A post-quantum blockchain architecture that incorporates deep learning was presented by Anbarkhan [3]. It stressed the significance of employing quantum-resistant cryptographical protocols to protect the healthcare ecosystem from potential attacks in the future. Likewise, the research carried out by Gharavi et al. [9] focused on the post-quantum blockchain security of IoT and suggested using lattice cryptography for quantum-resistance purposes.

Alabdulatif [4] presented an innovative blockchain-based access control mechanism for ensuring secure authentication and access control for e-healthcare users. Arastouei and Khan [5] explored security and privacy problems in smart healthcare systems that use 6G communications. The effects of quantum computing on blockchain technology used in medical environments were elaborated by Atal et al. [6], who pointed out the necessity of post-quantum encryption algorithms in future healthcare frameworks. Gandhi et al. [8] presented a review on recent advances in quantum blockchains and their future implementations in secure communication systems. The authors Benaich et al. [7] suggested a conceptual blockchain framework to ensure the security of electronic health records and enhance the integrity of data. The study of Mahajan and Reddy [10] offered a lightweight cryptographic blockchain framework for processing genomic profile data securely without increasing computational complexity. A quantum-secure login credentials system was suggested by Natarajan et al. [11] for facilitating the exchange of electronic health records via blockchain technology. Oliva et al. [12] examined new technologies for genomic data protection and managing consents securely within the healthcare domain. Peelam and Chamola [13] considered quantum blockchain systems' applicability to IoT networks and demonstrated their enhanced resilience to sophisticated cyber attacks. Denis et al. [14] provided a review of cryptographic methods employed in securing Internet of Medical Things applications and explored various security attacks on healthcare information systems and their countermeasures. Sezer et al. [15] suggested a privacy-preserving post-quantum blockchain architecture and described potential implementation challenges concerning scalability and efficiency. Singh et al. [16] conducted research on the utilization of blockchain and IoT technologies in healthcare systems for ensuring secure data communications and traceability. According to Sharma and Shambharkar [17], a comprehensive study of emerging technologies utilized in healthcare data security was conducted, with technologies such as blockchain, encryption schemes, artificial intelligence, and post-quantum cryptography included.

It is evident from the reviewed literature that blockchain technology plays an integral role in enhancing the level of healthcare security and transparency of healthcare data. Unfortunately, most current systems depend on conventional cryptography algorithms, which can easily be compromised by quantum computer attacks. There exists a great need for implementing a quantum-resistant blockchain architecture for securing healthcare data.

III. METHODOLOGY

This section describes the design and implementation of the proposed quantum-resistant blockchain framework developed for securing electronic medical information. The proposed approach integrates post-quantum cryptographic algorithms with blockchain technology to ensure long-term confidentiality, integrity, authenticity, and secure sharing of healthcare data. The framework is designed to provide protection against both classical and future quantum-based

attacks while operating entirely on conventional computing infrastructure without requiring quantum hardware.

A. System Overview

The proposed system consists of three primary components:

Post-Quantum Cryptography (PQC)
Blockchain Network
Healthcare Data Management Module

The proposed system architecture is designed to provide secure storage and controlled sharing of electronic medical information among authorized healthcare entities. To enhance security against emerging cyber threats, conventional cryptographic methods are replaced with lattice-based post-quantum cryptographic algorithms capable of resisting both traditional and quantum computing attacks.

B. Post-Quantum Cryptographic Framework

To make the system quantum-resistant, the framework relies on lattice-based cryptographic algorithms standardized by NIST:

1) CRYSTALS-Kyber (Key Exchange)

Kyber is employed for secure key encapsulation between parties, such as hospitals or healthcare servers. It enables the creation of a shared secret key for encrypting patient information. The algorithm is highly secure due to its reliance on the difficulty of lattice problems and enables efficient key generation and exchange.

2) FALCON (Digital Signature)

FALCON is employed for creating and verifying digital signatures. Prior to blockchain storage, the medical information is digitally signed to guarantee authenticity and integrity. Signature verification enables authorized parties to verify that the information is not tampered with.

The algorithms employed are quantum-resistant and enable long-term data security.

C. Blockchain-Based Data Management

A private blockchain network is employed to securely store the encrypted medical data. The blockchain offers the following benefits:

Decentralization: Data is replicated on multiple nodes to prevent a single point of failure.

Immutability: Data cannot be altered or deleted once stored.

Traceability: All transactions are recorded and timestamped.

Data Storage Process

Patient data is created at a healthcare facility.

A shared key is generated using Kyber.

The data is encrypted using the shared key.

A digital signature is generated using Falcon.

The encrypted and signed data is stored as a blockchain transaction.

D. Secure Data Access Procedure

When an authorized party makes a request for access:

The encrypted data is obtained from the blockchain.

Falcon signature verification is carried out to verify data integrity and authenticity.

A secure key exchange using Kyber is carried out between parties.

The shared key is used to decrypt the medical information.

This ensures that only authorized parties can access the information.

E. Security and Performance Considerations

The approach is intended to tackle major security issues:

Quantum Resistance: The lattice-based schemes are resistant to attacks based on Shor's algorithm.

Harvest-Now-Decrypt-Later Security: The data is secure even if it is intercepted in the current era.

Computational Efficiency: Kyber enables efficient key exchange, and Falcon enables efficient signature verification.

Practical Deployability: The system is fully classical and does not require any quantum communication infrastructure.

F. Implementation Environment

The proposed framework is implemented and tested using classical computing resources. The performance analysis is carried out using the following parameters:

Key generation time

Key exchange time

Signature generation and verification time

Computational overhead

The proposed system is shown to provide high security with acceptable computational performance.

The framework is implemented using a simulation environment on classical computing systems. Programming tools are used to simulate the cryptographic operations. It is possible to evaluate the key generation, encryption, and signature processes using this method. A private blockchain network is considered to simulate the secure storage and retrieval of medical data. The implementation environment is designed to emulate practical real-world healthcare scenarios for evaluating the proposed framework under different operating conditions. The system performance can be examined using multiple security and computational parameters to measure its effectiveness and reliability. In addition, the proposed framework can be deployed using standard classical computing infrastructure without the need for specialized quantum hardware or advanced physical devices.

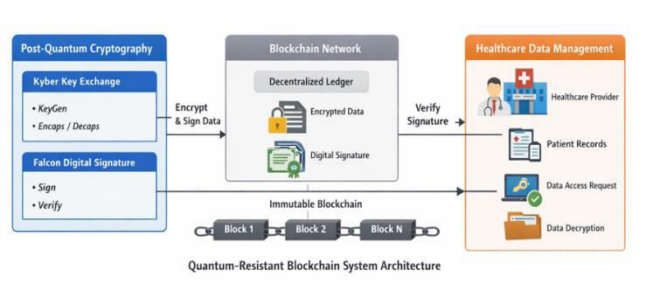


Figure 1. Architecture of the proposed quantum-resistant healthcare system incorporating CRYSTALS-Kyber for secure key exchange, FALCON for digital signature generation and verification, and blockchain technology for decentralized and tamper-resistant storage of encrypted electronic medical data.

The architecture of the proposed system includes healthcare clients, processing servers, and blockchain nodes. The healthcare providers create patient data, which is processed through secure encryption and digital signature techniques. The processed data is stored in the blockchain network, which provides immutability to the stored data. The blockchain nodes store the data in a distributed manner, which prevents any unauthorized modifications to the stored data. The users can request access to the stored data, which is verified through post-quantum cryptography.

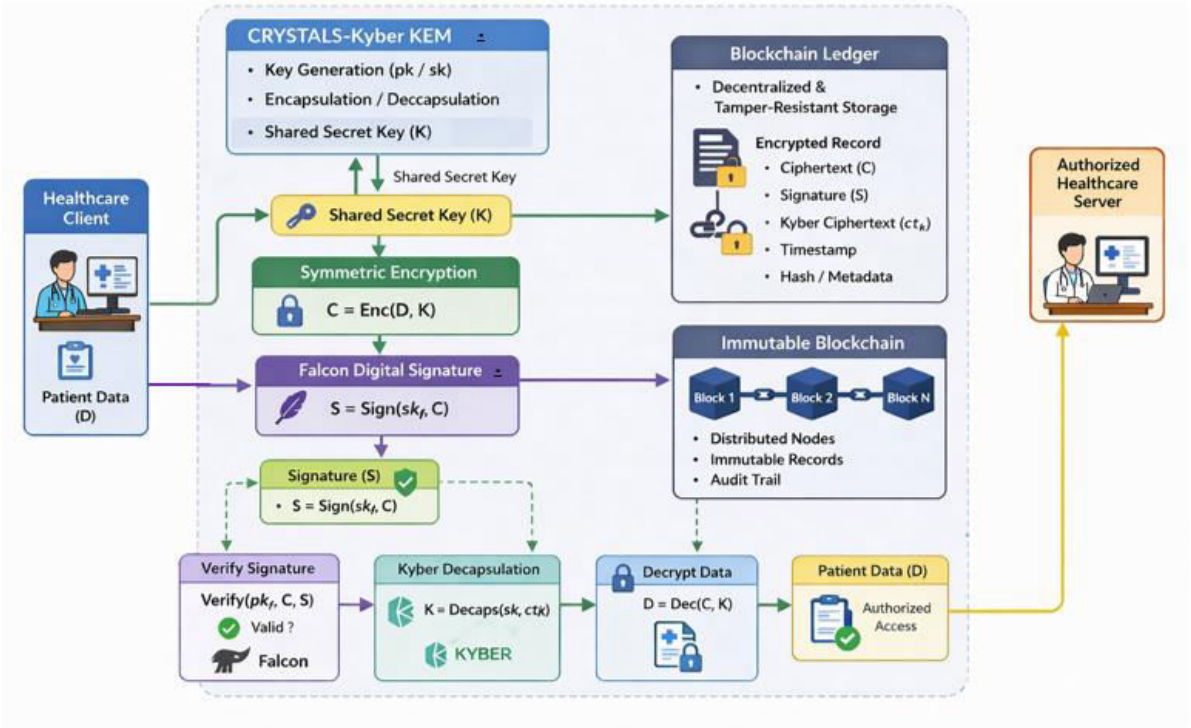


Figure 2. Detailed block diagram of the proposed quantum-resistant healthcare system

Input: Electronic medical data provided by healthcare providers
Output: Securely encrypted, authenticated, and stored in a blockchain-based medical data system

Process:
Step 1: Generate a shared secret key by means of a post-quantum key exchange (Kyber).

Step 2: Encrypt the patient data by means of the generated secret key in order to ensure confidentiality.

Step 3: Generate a digital signature by means of Falcon in order to ensure integrity and authenticity of the data.
Step 4: Store the encrypted and digitally signed data as a transaction in a blockchain-based system.
Step 5: Retrieve the data from the blockchain-based system upon request.

Step 6: Verify the integrity of the data by means of a digital signature.

Step 7: Decrypt the data by means of the shared secret key for authorized access.

Algorithm 1 proposed quantum-resistant healthcare framework

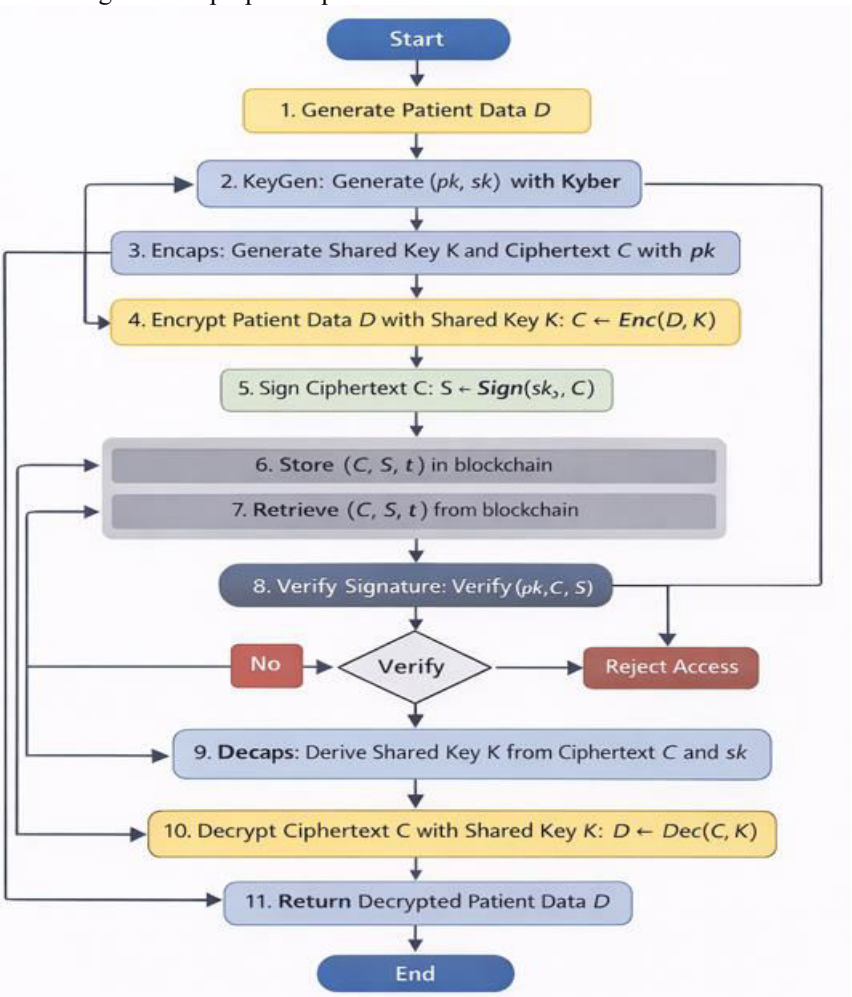


Figure 3. Flowchart representation of Algorithm 1 illustrating the proposed quantum-resistant healthcare framework, including Kyber-based key generation and encapsulation, encryption of patient data, Falcon digital signature generation and verification, secure blockchain storage, and authorized data retrieval with key decapsulation and decryption.

IV. IMPLEMENTATION AND RESULTS

A. Dataset Description

The efficiency of the developed framework is tested by implementing a synthetic Electronic Medical Information (EMI) dataset, which is a simulated version of real-world data. The dataset includes structured data related to patients, including identification details, diagnostic reports, prescriptions, test results, and treatment history.

The dataset is developed for 1,000 patients, each containing data of varying sizes, ranging from 5 KB to 500 KB, to test the system's efficiency under different circumstances. The dataset goes through all the stages of the developed system, including key generation, encryption, signing, and storing data on the blockchain.

The dataset is divided as follows:

70% for performance execution analysis

30% for validation and data retrieval testing

This is to ensure accurate results regarding the efficiency of computations and system stability. A synthetic dataset is used in this study because of the strict privacy regulations and inaccessibility of the actual healthcare data. Using a synthetic dataset is helpful in conducting experiments while maintaining the privacy of the actual data. It is made in such a way that it is similar to the actual data, and the results obtained from the actual system can be accurately represented.

B. Performance Metrics

System performance is measured based on the following quantitative metrics:
Key generation time (in ms)
Key exchange time (in ms)

Encryption time (in ms)
Signature generation time (in ms)
Signature verification time (in ms)
Decryption time (in ms)
Security efficiency (%)

C. Computational Performance

Table I. Performance Evaluation of Post-Quantum Cryptographic Operations

Operation	Time (ms)
Kyber Key Generation	2.8
Key Encapsulation	3.5
Data Encryption	4.2
Falcon Signature Generation	5.6
Signature Verification	2.1
Key Decapsulation	3.2
Data Decryption	4.0

Based on the results, the proposed system is efficient in terms of execution time with minimal computational overhead. It is observed that the Falcon signature verification takes less time than the signature generation, making it fit for the scenario in the blockchain where the signature is frequently verified.

The results obtained from the framework indicate that the framework performs efficiently with minimal computational delay. The low execution time for the cryptographic operations and faster signature verification confirm that the framework is appropriate for real-time applications in the health domain. These results confirm that the integration of post-quantum cryptography does not impose a performance penalty.

C. Security Evaluation

Table II. Comparative Security Analysis of Conventional and Proposed Frameworks

Security Feature	Conventional System (RSA/ECC)	Proposed Quantum-Resistant Framework
Quantum Attack Resistance	No	Yes
Security Under Quantum Model	0%	100%
Harvest-Now-Decrypt-Later Protection	No	Yes
Long-Term Data Confidentiality	No	Yes
Hardware Requirement	Classical	Classical

The proposed framework ensures complete resistance to known quantum attacks by replacing classical cryptographic primitives with lattice-based post-quantum cryptographic algorithms.

D.. Graphical Analysis

The following graphs are suggested for a better understanding of system performance:

Execution Time Analysis

X-axis: Cryptographic operations
Y-axis: Time (ms)

Security Comparison Chart

Quantum Resistance and Long-Term Security Comparison Chart for existing as well as proposed systems.

From the graphs, it is evident that the proposed framework is providing satisfactory computational efficiency with improved security.

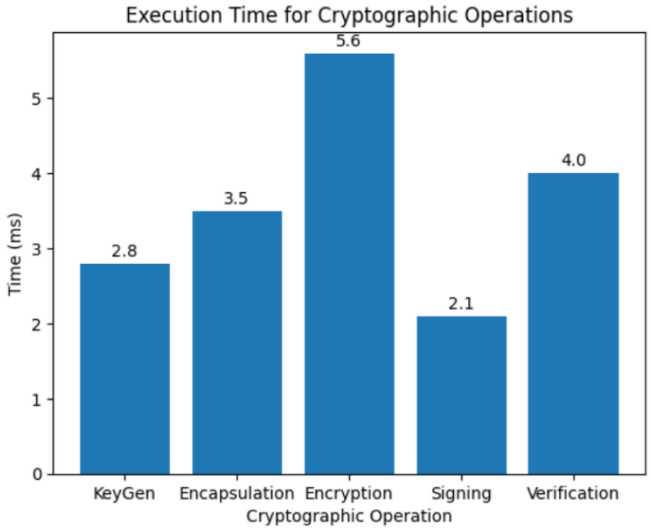
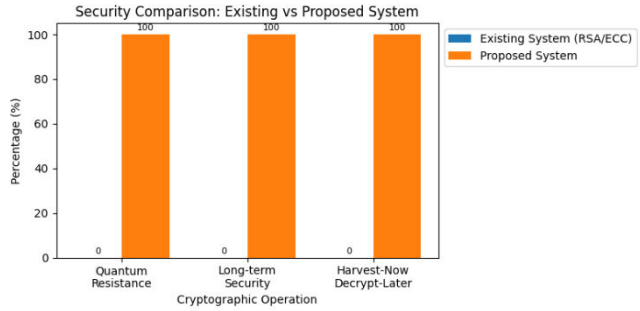


Figure 4. Computational time analysis of post-quantum cryptographic operations, including Kyber-based key generation, key encapsulation, data encryption, Falcon signature generation, and signature verification..

Figure 5. comparative evaluation of existing (RSA/ECC) and proposed systems in terms of quantum resistance, long-term security, and overall efficiency.



From the graph, it can be concluded that the designed model manages to balance the relationship between the effectiveness of security and the efficiency of the process. When compared to existing encryption algorithms, the

proposed solution is more capable of securing systems from contemporary and quantum attacks while keeping its execution speed high. Another thing demonstrated by the test is that integrating post-quantum cryptography with blockchain does not pose any extra computational burden. Thus, the framework has enough capabilities for offering efficient security to healthcare data.

V. DISCUSSION AND ERROR ANALYSIS

To further improve system performance, future work can include considerations for optimizing cryptographic operations, minimizing storage overhead, and minimizing blockchain transaction delay. The use of lightweight blockchains and efficient data management can improve system scalability for healthcare applications.

Future Improvements:

To improve the performance in large-scale scenarios, optimization can be carried out. The proposed system can also be implemented in large-scale health care scenarios. To reduce transaction delays in blockchain technology, lightweight blockchain can be explored.

VI. CONCLUSION AND FUTURE WORK

In summary, this paper introduced an approach for developing a blockchain-based security architecture for preserving electronic health care records in a quantum-resistant manner using post-quantum cryptography. The suggested approach involves the use of CRYSTALS-Kyber for key exchange and FALCON for generating and validating signatures to guarantee protection from classical and quantum adversaries. By leveraging the blockchain technology together with post-quantum cryptography, the framework can protect sensitive health care data during storage, authentication, and distribution while retaining integrity and confidentiality. Moreover, the architecture is entirely based on classic computers without requiring dedicated quantum hardware. Experiments revealed that the proposed framework can deliver good computational performance and low overhead in terms of computation cost during the encryption, decryption, key pair generation, and signature validation operations. Additionally, the framework can protect the confidentiality of the preserved information from emerging attacks such as the harvest now decrypt later attack. In the future, efforts can be made to enhance scalability and optimize the blockchain framework for storing large amounts of medical records by designing lightweight blockchain structures and optimizing data storage.

REFERENCES

[1] N. Agarwal, P. K. Kankanampati, S. S. Chamarthy, I. Khan, A. Jain, and M. Almusawi, “Blockchain and quantum cryptography-based hybrid security for Healthcare 5.0 systems,” in *Proc. 3rd Int. Conf. Computing, Communication, Perception and Quantum Technol. (CCPQT)*, 2024, pp. 376–381.

[2] S. O. Ajakwe, I. I. Saviour, V. U. Ihekoronye, O. U. Nwankwo, M. A. Dini, I. U. Uchechi, *et al*., “Medical IoT record security and blockchain: Systematic review of milieu, milestones, and momentum,” *Big Data Cogn. Comput.*, vol. 8, no. 9, p. 121, 2024.

[3] S. H. Anbarkhan, “Securing IoT networks: A post-quantum blockchain and deep learning approach for enhanced cyber defense,” *Int. J. Safety Security Eng.*, vol. 14, no. 6, 2024.

[4] A. Alabdulatif, “Blockchain-based privacy-preserving authentication and access control model for e-health users,” *Information*, vol. 16, no. 3, p. 219, 2025.

[5] N. Arastouei and M. A. Khan, “6G technology in intelligent healthcare: Smart health and its security and privacy perspectives,” *IEEE Wireless Commun.*, vol. 32, no. 1, pp. 116–121, 2025.

[6] D. K. Atal, V. Tiwari, Anjali, and R. K. Berwer, “The intersection of blockchain technology and the quantum era for sustainable medical services,” in *Quantum and Blockchain-Based Next Generation Sustainable Computing*. Cham, Switzerland: Springer, 2024, pp. 19–45.

[7] R. Benaich, Y. Gahi, and S. El Mendili, “Pioneering the security of EHRs using an immersive blockchain conceptual framework,” *Emerging Sci. J.*, vol. 9, no. 1, pp. 161–187, 2025.

[8] M. Gandhi, C. Mulay, K. Durai, G. Murali, J. A. I. S. Masood, V. Vijayarajan, *et al*., “Quantum blockchain: Trends, technologies, and future directions,” 2024.

[9] H. Gharavi, J. Granjal, and E. Monteiro, “Post-quantum blockchain security for the Internet of Things: Survey and research directions,” *IEEE Commun. Surveys Tuts.*, vol. 26, no. 3, pp. 1748–1774, 2024.

[10] H. Mahajan and K. T. V. Reddy, “Secure gene profile data processing using lightweight cryptography and blockchain,” *Cluster Comput.*, vol. 27, no. 3, pp. 2785–2803, 2024.

[11] M. Natarajan, A. Bharathi, C. S. Varun, and S. Selvarajan, “Quantum secure patient login credential system using blockchain for electronic health record sharing framework,” *Sci. Rep.*, vol. 15, no. 1, p. 4023, 2025.

[12] A. Oliva, A. Kaphle, R. Reguant, L. M. Sng, N. A. Twine, Y. Malakar, *et al*., “Future-proofing genomic data and consent management: A comprehensive review of technology innovations,” *GigaScience*, vol. 13, 2024.

[13] M. S. Peelam and V. Chamola, “Enhancing security using quantum blockchain in consumer IoT networks,” *IEEE Trans. Consumer Electron.*, 2024.

[14] R. W. Denis, A. Thomas, S. A. Samuel, S. P. Kabiito, Z. Morish, and G. Ali, “A comprehensive review on cryptographic techniques for securing Internet of Medical Things: State-of-the-art, applications, security attacks, mitigation measures, and future research direction,” *Mesopotamian J. Artif. Intell. Healthcare*, pp. 135–169, 2024.

[15] B. B. Sezer, S. Akleylek, and U. Nuriyev, “PP-PQB: Privacy-preserving in post-quantum blockchain-based systems: A systematization of knowledge,” *IEEE Access*, 2025.

[16] R. Singh, A. Gehlot, S. V. Akram, R. Sharma, and P. K. Malik, "Integration of blockchain and the Internet of Things in healthcare sector," in *Sustainable Security Practices Using Blockchain, Quantum and Post-Quantum Technologies for Real Time Applications*. Singapore: Springer, 2024, pp. 155–170.

[17] N. Sharma and P. G. Shambharkar, "A systematic literature review of the emerging technologies used in securing healthcare data," in *Proc. 12th Int. Conf. Internet Everything, Microwave, Embedded, Communication Networks (IEMECON)*, 2024, pp. 1–12.