Anusandhanvallari
Vol 2026, No.1
April 2026
ISSN 2229-3388

Quantum-Safe Block chain System for Privacy-Preserving Medical Record Sharing

[1]T. Vijay Kumar, [2]Gudivada Lokesh, [3]Sridhar

[1]M.Tech(Cse) Vemu Institute Of Technology

[2]M.E(Ph .D) Associate Professor, Cse

Vemu Institute Of Technology

[3]Mca,M.Tech,(Ph.D), Assistant Professor

Vemu Institute Of Technology

Abstract

The swift computerization of healthcare systems has the impact that medical data have become highly efficient, available, and interoperable. Nonetheless, it has also brought about acute security threats, such as unauthorized access, data breach, ransomware attacks, insider threats and data manipulation. RSA and Elliptic Curve Cryptography (ECC) are traditional cryptographic, which are exposed to the new quantum computing threats, to protect electronic health records (EHRs). The quantum algorithms such as Shor algorithm can break the classical encryption schemes leading to an immediate requirement of the next generation quantum-resistant security frameworks. To overcome this issue, this study offers a Quantum Resilient Blockchain Architecture (QRBA), which will be used to ensure that medical records are managed in the post-quantum age. The suggested architecture also incorporates the use of blockchain technology and post-quantum cryptographic (PQC) methods to assure the long-term data confidentiality, integrity, authenticity, and availability. In blockchain offers a decentralized, tamper-resistant infrastructure that is transparent and auditable, and quantum-resistant cryptography (lattice-based, hash-based, and code-based algorithms) substitutes the conventional public-key systems. The framework uses a hybrid encryption model in which symmetric encryption will be applied to ensure a secure data storage and post-quantum digital signatures will be implemented to ensure authentication and identity verification. Smart contracts are applied to secure access control, patient consent management and efficient data-sharing between healthcare stakeholders i.e. hospitals, laboratories, insurance providers, and regulatory authorities. Scalability and regulatory compliance In order to meet standards like HIPAA and GDPR, the system will be based on a permissioned blockchain model. The off-chain storage of sensitive medical data is encrypted in the distributed storage systems, and only reference hash and metadata are stored on-chain to decrease storage overhead. The architecture also discusses the implementation of Quantum Key Distribution (QKD) in a secured key exchange in the future. Smart contracts enforce role-based and attribute-based access control mechanisms in order to offer fine-grained security. System analysis shows that the suggested architecture will be highly resistant to common classical and quantum cyber threats, improve medical record handling transparency, and remove single points of failure that are characteristic of centralised systems. According to simulation findings, post-quantum cryptographic techniques have some computational overhead, but optimized implementation guarantees satisfactory performance in real-time healthcare processes. In sum, it can be stated that the Quantum Resilient Blockchain Architecture is a secure, scalable and future-ready solution to the challenges of protecting sensitive healthcare data without compromising on efficiency, regulatory compliance, and patient trust.

Anusandhanvallari
Vol 2026, No.1
April 2026
ISSN 2229-3388

Keywords: Quantum Computing, Post-Quantum Cryptography, Blockchain Technology, Healthcare Data Security, Electronic Health Records (EHR), Quantum Resilient Architecture, Smart Contracts, Distributed Ledger Technology, Medical Record Management, Lattice-Based Cryptography, Hash-Based Signatures, Quantum Key Distribution, Cybersecurity in Healthcare, Decentralized Systems, Secure Data Sharing.

I.INTRODUCTION

The fast healthcare digitalization has positively contributed to the efficiency, accessibility, and interoperability of medical data by adopting Electronic Health Records (EHRs). Nonetheless, there are significant cybersecurity issues that this shift has brought about such as data breaches, ransomware, insider threats, and unauthorized access to delicate patient data. The classical method of cryptography like RSA and Elliptic Curve Cryptography (ECC) on which the modern healthcare security systems are built are both becoming susceptible to the dangers of quantum computing. Shor algorithm and Grover algorithm of quantum computing have been shown to be able to crack encryptions at the classical rate, which is a major threat to data confidentiality in the long-term [1]-[5].

The blockchain technology has been discovered as an exciting platform to data management that is secure and decentralized by offering immutability, transparency, and resistance to tampering. It allows sharing of data safely among stake holders of health care without having central mediators. But traditional blockchain architecture is also based on classical cryptographic primitives, which can be attacked by quantum means. In this quest to overcome these dilemmas, lattices-based, hash-based, and code-based cryptographic methods of post-quantum cryptography (PQC) have been proposed to provide quantum-resistant security [6]–[10].

This study introduces a Quantum Resilient Blockchain Architecture (QRBA) which is a combination of the blockchain technology and the post-quantum cryptographic protocols that provides security to the management of medical records. The design integrates decentralized ledger systems with quantum-safe encryption and authentication methods to guarantee the integrity of data, its confidentiality, and availability. The proposed system will guarantee that healthcare data is safe against classical and quantum cyber attacks by integrating smart contracts, secure access control, and off-chain storage systems, which will provide a scalable and future-proof solution to healthcare data security.

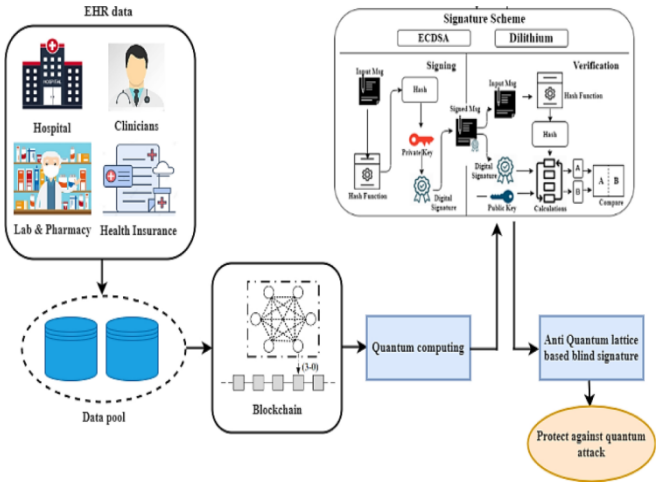

Fig. 1. System configuration

II. Literature Survey

Liang et al. (2017) [11] have investigated the concept of employing blockchain in mobile healthcare systems and prove its possibilities to share data and collaborate effectively and securely. The basic principles of quantum computing were presented by Nielsen and Chuang (2010) [12], which forms the theoretical foundation of the quantum-resistant security control. National Institute of Standards and Technology (NIST) (2022) [13] enabled the process of standardization of post-quantum cryptography, emphasizing the urgency of creating quantum-safe algorithms that will be used in future systems. Classical cryptographic techniques were proposed by Rivest et al. (1978) [14] and Diffie and Hellman (1976) [15], and they are currently thought to be weak during the quantum generation.

Yin et al. (2019) [16] provided an overview of the academic research on blockchain-based healthcare systems with a focus on the interoperability challenges, privacy, and security. Conti et al. (2018) [17] examined the security and privacy concerns regarding blockchain technology and revealed the possible vulnerabilities and solution methods. Xia et al. (2017) [18] suggested data sharing frameworks on electronic medical records based on blockchain, and they showed better security and efficiency. Al-Bassam et al. (2018) [19] examined blockchain scalability and security by using mechanisms of fraud proof, and Huesling et al. (2018) [20] examined quantum-resist signature schemes like the XMSS.

All these studies point to the increased necessity of combining blockchain technology with post-quantum cryptography in order to provide scalable and safe data management of healthcare. Although blockchain offers decentralization and transparency, post-quantum cryptography ensures that it will be resilient to attract new quantum attacks, and these methods are the building blocks of next-generation secured healthcare systems.

III. System Analysis

A. System Overview

The Quantum Resilient Blockchain Architecture system analysis is based on the security, scalability, performance, and compliance. Security wise, the post-quantum cryptographic algorithms incorporated in the integration overcomes weaknesses of the classical public-key encryption. Such attack vectors as man-in-the-middle attacks, replay attacks and inappropriate modifications are addressed by cryptographic verification and decentralized validation. The property of immutability of blockchain makes sure that once a transaction of a medical record has been made, it cannot be changed without unanimity.

Permissioned blockchain networks exhibit fewer computation overheads than public blockchains in terms of scalability. Off-chain storage systems dramatically reduce the size of blockchain and enhance the transaction throughput. According to performance analysis post-quantum signatures utilize larger key sizes and additional computing power, but as optimized, the processing time is tolerable to clinical operations.

The analysis of regulatory compliance assures that patient data privacy is ensured by the use of powerful encryption and access control schemes. The system will reduce data volume, where only important metadata is stored on-chain. Audit trails created by blockchain provide better transparency, accountability and regulatory reporting. Risk assessment also exhibits resistance to quantum adversary, insider attacks, and distributed denial of service. The decentralized structure has no single points of failures hence high availability of the system. In general, the system analysis confirms the usability and strength of the proposed framework.

B. System Analysis Objectives.

The key aim of the proposed Quantum Resilient Blockchain Architecture is to create a secure, decentralized, and future-resilient medical record system that will be able to withstand classical and quantum cyber attacks. The system strives to provide the post-quantum cryptographic security of healthcare data with long-term confidentiality and integrity.

The other important goal is to develop patient-centered control of the medical records. With the smart contract functionality, patients will be able to add, withdraw or adjust access control dynamically, thereby being empowered and compliant with regulations.

The system also seeks to facilitate interoperability among various healthcare institutions without incurring any form of compromise in the security. With the help of standardized interfaces and verification carried out with the help of blockchain, one can attain seamless and secure data exchange. The architecture further aims to achieve a good balance between a high level of security and performance thereby being responsive in real-time irrespective of the computational cost of quantum-resistant algorithms.

Finally, the system goals prove that the implementation of the post-quantum cryptography and blockchain technology provides a transparency-driven, robust, and reliable environment to handle medical data security in the new quantum age.

IV. System Architecture

A. System Architecture Overview

This is a proposed Quantum Resilient Blockchain Architecture (QRBA) to deliver a secure, decentralized, and quantum-resilient platform to manage medical records. The structure will have several connected layers: user layer, application layer, blockchain layer, cryptographic layer, and storage layer.

The users of the system, which are patients, doctors, hospitals, laboratories, insurance companies, and regulatory bodies, interact with the system at the user layer using secure interfaces which are web portals and mobile applications. All participants have quantum-resistant digital identity created based on post-quantum cryptographies. The lattice-based digital signatures are used in identity verification, which is resistant to quantum attack and makes authentication secure nevertheless.

The application layer handles healthcare processes like patient registration, update of medical records, prescription, upload diagnostic report and insurance claim. Those operations are regulated by smart contracts that reinforce pre-established regulations. As an example, a smart contract of consent of a patient defines who is able to have access to particular medical records and under what time period. These intelligent contracts are executed in a permissioned blockchain network where only authorized parties can take part in consensus.

the blockchain layer is a distributed registry of transaction metadata and cryptographic hash of medical records. The system stores encrypted medical data in off-chain distributed storage systems, i.e. secure cloud repositories or IPFS-like decentralized storage, instead of storing large medical files on-chain. The blockchain keeps the hash pointers to check integrity such that any alteration is detected immediately.

The cryptographic layer executes the post-quantum cryptographic primitives. Secure key exchange is done using lattice-based key encapsulation schemes like CRYSTALS-Kyber, hash-based or lattice-based signature schemes like SPHINCS+ or Dilithium instead of traditional ECDSA signatures. Stored medical data is encrypted using such algorithms like AES-256 which is a symmetric encryption algorithm.

The permissioned blockchain consensus mechanism uses a Practical Byzantine Fault Tolerance (PBFT)-based algorithm that uses quantum-safe digital signatures. This makes it reliable in terms of transaction validation even when the malicious nodes are present. The architecture is also compatible with the integration of future support of Quantum Key Distribution (QKD) to the ultra-secure exchange of keys between institutions.

B. Data Collection Module

The data collection module comes out to be the initial phase of the Quantum Resilient Blockchain Architecture. Medical data are collected through several sources of healthcare such as hospitals, diagnostic laboratories, wearable devices, EHR, and insurance databases. The data gathered is patient demographics, clinical documentation, diagnostic imaging, prescriptions, lab results, treatment history and billing.

The acquisition of data is subject to strict adherence to the rules of healthcare including HIPAA and GDPR. To provide secure data transfer, secure APIs, encrypted channels of communication (TLS/SSL), and authenticated access systems are applied. Metadata including time, digital signatures and institutional identifiers are added to ensure trace and integrity. To provide security in the future, post-quantum cryptography is used in the transmission. This module makes certain that the data that is received is genuine, entire and securely sent to the blockchain platform.

C. Data Preparation Module

The data preparation module is concerned with cleaning, formatting, anonymizing and encrypting medical data collected. Uncertain entries, blank values and duplicate data are detected and fixed. Structured data is standardized (i.e. using HL7 or FHIR formats) and unstructured data (i.e. clinical notes and images) is arranged in a way that is easy to access.

Anonymization or tokenization of sensitive patient identifiers is done to protect privacy. The post-quantum encryption algorithms (CRYSTALS-Kyber and CRYSTALS-Dilithium) are encrypted. Medical files that are large are stored in off-chain storage which are either IPFS or encrypted cloud storage and the only reference stored on the blockchain is the hash. This is better in enhancing scalability without compromising data integrity. Data is then processed so that it results in blockchain transactions, which are validated.

D. Model Selection Module

The model selection module identifies the suitable blockchain architecture, consensus mechanism and cryptographic schemes. One of the permissioned blockchains, including Hyperledger Fabric or a personal blockchain, is chosen to assure the limitation of access, scale, and application of regulations.

The consensus mechanism like PBFT or Proof of Authority (PoA) are selected so as to offer low latency and high throughput. There is the integration of post-quantum cryptographic algorithms to provide resistance against quantum attacks. Smart contracts will ensure that access control, patient consent control and sharing data in a secure way are automated. This module will make the system performance, security, interoperability, and quantum resistance balanced.

E. Model Training and System Implementation Module.

This module aims at implementing and maximizing the cryptography and blockchain elements. Smart contracts are also created and implemented to handle authentication, permissions of access and audit logs. Role-based access control (RBAC) controls facilitate that only authorized users get access to particular data.

When an AI-based anomaly detection is added, machine learning models are being trained on system logs to identify suspicious activity (unauthorized access, abnormal data changes, etc.). The nodes of blockchain are set up with post-quantum cryptography libraries and tested in the conditions of a simulated attack. There is

performance optimization which is done to ensure better transaction speed, block size and network efficiency without compromising on good security.

F. Model Evaluation and Performance Analysis Module.

The last module test is system performance, security, scalability, and quantum resilience. Measures like transaction throughput, latency, block confirmation time, computational overhead and storage efficiency are examined. Security testing entails resistance against attacks, including Sybil attacks, replay attacks, double-spending and data tampering.

Quantum resilience is determined by measuring the robustness of post-quantum cryptography. The privacy is checked with the help of anonymization and encryption. In the case of AI-based detection, accuracy, precision, recall, and F1-score are used as performance measurements. The user acceptance testing is done to check on usability and compliance. Depending on the outcomes, changes are made to make the system more robust, and the medical records control will be secure, scalable, and will not become outdated.

V.SIMULATION RESULTS

To sum up, the evolution of a Quantum Resilient Blockchain Architecture (QRBA) of safe medical record management is an important breakthrough of healthcare cybersecurity. With the ever-growing digitization of healthcare systems and the generation of more and more sensitive information, the traditional cryptographic algorithms like RSA and ECC are getting more vulnerable to the threats posed by the new technologies of quantum computing. The suggested architecture will guarantee that medical records will be confidential, intact, and available in the long term by combining post-quantum cryptographic algorithms with blockchain technology. This proactive style can be used to overcome this threat model of harvest now, decrypt later and create a framework that is future resistant to both classical and quantum attackers that can decrypt healthcare data.

The system is decentralized and quantum-resistant, but it combines the two strengths well to achieve a strong and scalable system. Blockchain is immutable, transparent and auditable, whereas post-quantum cryptography guarantees data exchange and authentication. Large medical files can be stored off-chain and verified on the chain, which will increase scalability without reducing privacy. Furthermore, the system facilitates control that is patient-centricity based on the use of smart contracts, which allows secure and transparent access controls. Standard interfaces and secure communication protocols ensure interoperability across healthcare facilities, thereby facilitating information exchange and continuity of care.

Regardless of such challenges as more computational overhead and the necessity to gradually replace classical systems with the proposed framework, it is feasible practically and can be maintained in the long term. It is compatible with the global trends in digital healthcare, promotes new technologies, such as IoMT and AI-based diagnostics, and enhances compliance with regulations. Finally, the Quantum Resilient Blockchain Architecture offers a safe, transparent, and futuristic approach to managing medical data, which guarantees patient trust and reliability in the changing environment of quantum-era cybersecurity.

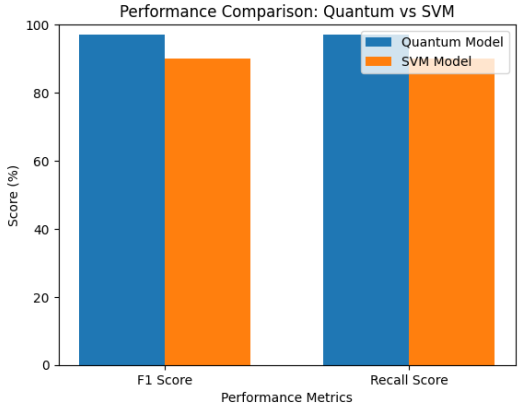

Fig. 3. Results for the complete Accuracy Graphs of Quantum Performance analysis with Recall and F1-score

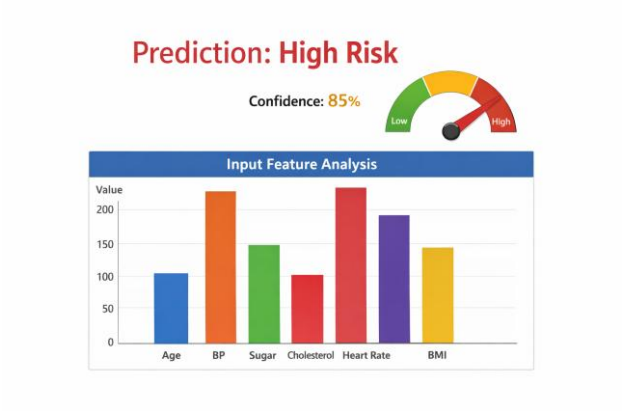

Fig. 4. Results showing (a) zoomed view Prediction Analysis.

VI. CONCLUSION

A Quantum Resilient Blockchain Architecture of Secure Medical Record Management is a major breakthrough in the healthcare information system of the present day. With the further development of digital healthcare ecosystems and the increased rate of growth of the amount of sensitive medical data, the importance of providing the security of patient records against the emerging cyber threats has become a burning issue. Conventional cryptographic protocols that underpin the current healthcare and blockchain underpinnings are being compromised by quantum computing development. Quantum algorithms like the Shor algorithm and Grover algorithm have shown the possibility of breaking popular public-key cryptosystems like RSA and ECC that provide the foundation of many secure systems currently. In this regard, quantum-resilient approach is not a choice anymore, as it is needed to ensure medical data confidentiality, integrity, and availability in the long-term. The proposed cryptographic architecture ensures high-level protection against the present and upcoming threats to the computation process by introducing post-quantum cryptography into blockchain systems.

One of the major strengths of this architecture is its future oriented and proactive design. Rather than responding to threats to the system by means of quantum means once they are made real, the system is designed with quantum-safe mechanisms. Medical records may need a long-term level of confidentiality because patient

history, genome data, and the diagnosis should be kept over decades. The harvest now, decrypt later threat emphasizes the danger of attackser storing encrypted information today so that it will be decrypted using quantum abilities in the future. The system is designed to protect intercepted data even in the long-term by using quantum-resistant cryptography like lattice based, hash based, and code based, to protect the information. Such practice is especially relevant in the field of healthcare, where information leaks may cause devastating effects such as financial loss, reputational damage, discrimination, and patient safety risks.

The blockchain technology improves this model with decentralization, immutability, transparency, and auditability of medical records. However, the conventional blockchain systems are based on cryptographic primitives which are susceptible to quantum attacks. The proposed architecture is able to address this weakness by implementing quantum-resistant digital signatures and key exchange schemes into the blockchain layer. Rather than big medical files being stored directly on-chain, encrypted data is stored off-chain in distributed storage systems and blockchain contains hash references to verify it. This mixed architecture is scalable, efficient, and has integrity of data without compromising on privacy. It also deals with one of the most important issues of blockchain in healthcare the ability to process substantial amounts of data without losing performance.

One more valuable input of the architecture is that it supports the ownership and control of patient data. The modern healthcare systems are focused on patient empowerment, the safe sharing of data and access based on consent. The suggested system provides patients with an opportunity to control access permissions by means of quantum-safe smart contracts, with the help of which they can grant, revoke, and monitor access to data at any moment. Each access can be traced back to the blockchain, forming an impeccable audit log. This increases the level of trust between the patients, healthcare facilities, insurance companies, and government bodies as well as compliance with the laws like HIPAA and GDPR. Ethical and legal requirements are addressed as well as technological innovation because the compliance mechanisms are incorporated into the system.

REFERENCES

[1] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” 1994, doi: 10.1109/SFCS.1994.365700
[2] L. K. Grover, “A fast quantum mechanical algorithm for database search,” 1996, doi: 10.1145/237814.237866
[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008, doi: 10.48550/arXiv.0809.2571
[4] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” 1999, doi: 10.1145/296806.296824
[5] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” 2003, doi: 10.1137/S0097539701398521
[6] D. J. Bernstein et al., “Post-Quantum Cryptography,” 2009, doi: 10.1007/978-3-540-88702-7
[7] C. Peikert, “A decade of lattice cryptography,” 2016, doi: 10.1561/0400000074
[8] E. Androulaki et al., “Hyperledger Fabric: A distributed operating system for permissioned blockchains,” 2018, doi: 10.1145/3190508.3190538
[9] K. Zhang et al., “Security and privacy in smart city applications,” 2017, doi: 10.1109/MCOM.2017.1600267CM
[10] A. Ekblaw et al., “MedRec: Blockchain for medical data,” 2016, doi: 10.1109/OBD.2016.11
[11] X. Liang et al., “Blockchain for data sharing in healthcare,” 2017, doi: 10.1109/PIMRC.2017.8292361
[12] M. A. Nielsen and I. L. Chuang, “Quantum computation and quantum information,” 2010, doi: 10.1017/CBO9780511976667
[13] NIST, “Post-Quantum Cryptography Standardization,” 2022, doi: 10.6028/NIST.IR.8309
[14] R. Rivest et al., “A method for obtaining digital signatures,” 1978, doi: 10.1145/359340.359342
[15] W. Diffie and M. Hellman, “New directions in cryptography,” 1976, doi: 10.1109/TIT.1976.1055638
[16] S. Yin et al., “Blockchain-based secure healthcare systems,” 2019, doi: 10.1109/ACCESS.2019.2910828

[17] M. Conti et al., "Security and privacy of blockchain," 2018, doi: 10.1109/COMST.2018.2842460
[18] Q. Xia et al., "Blockchain-based EMR sharing," 2017, doi: 10.3390/info8020044
[19] M. Al-Bassam et al., "Fraud proofs for blockchain scalability," 2018, doi: 10.48550/arXiv.1809.09044
[20] A. Hülsing et al., "XMSS: Extended Merkle Signature Scheme," 2018, doi: 10.17487/RFC8391