QUANTUM-RESISTANT BLOCKCHAIN FOR SAFE HEALTH DATA

1.K. RAVINDRANATH TAGORE, ASSOCIATE PROFESSOR,DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING PALLAVI ENGINEERING COLLEGE, HYDERABAD, TELANGANA,
TAGORE.KANDUKURI@GMAIL.COM

2.Dr. KALARI SRIKANTH, ASSOCIATE PROFESSOR,HEAD OF THE DEPARTMENT COMPUTER SCIENCE & ENGINEERING (DATA SCIENCE), VISVESVARAYA COLLEGE OF ENGINEERING AND TECHNOLOGY, M.P.PATELGUDA, IBRAHIMPATNAM R.R
SRIKANTH.KALARI@GMAIL.COM

3.Dr. C SRINIVASA KUMAR, PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING VIGNAN'S INSTITUTE OF MANAGEMENT AND TECHNOLOGY FOR WOMEN, GHATKESAR, TELANGANA. DRCSKUMAR41@GMAIL.COM

ABSTRACT

The digitization of healthcare systems has led to the widespread adoption of Electronic Health Records (EHRs), telemedicine platforms, wearable devices, and Internet of Medical Things (IoMT) technologies. While these advancements improve healthcare delivery and patient outcomes, they also introduce significant security and privacy challenges associated with storing and sharing sensitive medical data. Blockchain technology has emerged as a promising solution for secure and decentralized health data management. However, traditional blockchain systems rely heavily on cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC), which are vulnerable to future quantum computing attacks. This paper proposes a Quantum-Resistant Blockchain framework for safeguarding healthcare data using post-quantum cryptographic techniques. The proposed model integrates lattice-based digital signatures and hash-based authentication mechanisms within a permissioned blockchain architecture to ensure confidentiality, integrity, authenticity, and long-term security of medical records. The framework enhances trust, privacy preservation, and resilience against emerging quantum threats, thereby providing a future-proof solution for secure healthcare information management.

Keywords: Quantum-Resistant Blockchain, Healthcare Security, Electronic Health Records, Post-Quantum Cryptography, Medical Data Privacy, Permissioned Blockchain, Internet of Medical Things.

1. INTRODUCTION

Healthcare organizations increasingly rely on digital technologies to manage patient information, facilitate remote consultations, and support clinical decision-making. Electronic Health Records (EHRs), wearable health devices, cloud-based health applications, and telemedicine platforms generate vast amounts of sensitive medical information that require robust security mechanisms.

Conventional healthcare information systems often employ centralized architectures, making them susceptible to unauthorized access, data breaches, insider attacks, and single points of failure. Blockchain technology addresses many of these concerns through decentralization, immutability, transparency, and distributed trust.

Despite these advantages, current blockchain implementations depend on cryptographic algorithms such as RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) for authentication and key management. The emergence of quantum computing poses a significant threat to these classical cryptographic systems. Algorithms such as Shor's algorithm can potentially compromise widely used public-key infrastructures, exposing sensitive healthcare information to future attacks.

To address these concerns, this study proposes a quantum-resistant blockchain framework that incorporates post-quantum cryptographic algorithms to secure healthcare data against both present and future cyber threats.

2. PROBLEM STATEMENT

Healthcare systems store highly sensitive patient information that requires long-term confidentiality and integrity. Existing blockchain-based healthcare solutions predominantly utilize classical cryptographic algorithms vulnerable to quantum attacks. As quantum computing technologies advance, encrypted medical records archived today may become susceptible to future decryption. Consequently, there is an urgent need for healthcare data protection mechanisms capable of resisting quantum-enabled adversaries while maintaining accessibility, privacy, and operational efficiency.

3. OBJECTIVES

The objectives of this research are:

- To design a quantum-resistant blockchain framework for healthcare applications.
- To integrate post-quantum cryptographic techniques within blockchain transactions.
- To ensure confidentiality, integrity, authenticity, and non-repudiation of medical records.
- To provide secure access control for authorized healthcare stakeholders.
- To enhance privacy preservation in Electronic Health Record management.

- To evaluate the performance and feasibility of the proposed framework.
- To develop a future-proof healthcare data security solution against quantum threats.

4. LITERATURE REVIEW

Blockchain technology has gained significant attention in healthcare due to its ability to provide decentralized storage, immutable audit trails, and transparent record sharing. Several studies have proposed blockchain-enabled Electronic Health Record systems to improve interoperability and trust.

However, most existing frameworks employ traditional public-key cryptography, including RSA and ECC. These algorithms derive their security from mathematical problems that can potentially be solved efficiently by quantum computers.

Post-Quantum Cryptography (PQC) has emerged as a promising alternative. PQC algorithms rely on computational problems believed to remain intractable even in the presence of quantum adversaries. Major categories include:

- Lattice-based cryptography,
- Hash-based signatures,
- Code-based cryptography,
- Multivariate cryptography,
- Isogeny-based cryptography.

Recent studies have explored integrating PQC into blockchain ecosystems, but their application in healthcare remains limited. This research addresses this gap by proposing a practical quantum-resistant blockchain architecture specifically tailored for medical data protection.

5. PROPOSED METHODOLOGY

The proposed framework combines permissioned blockchain technology with post-quantum cryptographic mechanisms.

5.1 Healthcare Data Acquisition

Medical information is generated from multiple sources, including:

- Electronic Health Records (EHRs),
- Internet of Medical Things (IoMT) devices,
- Diagnostic laboratories,
- Hospitals and clinics,
- Telemedicine platforms,
- Health monitoring applications.

5.2 Permissioned Blockchain Architecture

A permissioned blockchain network is established involving authorized participants such as:

- Patients,
- Physicians,
- Hospitals,
- Insurance providers,
- Diagnostic centers,
- Regulatory authorities.

The permissioned architecture provides controlled access and improved transaction efficiency.

5.3 Post-Quantum Cryptographic Integration

To resist quantum attacks, the framework replaces conventional cryptographic primitives with post-quantum algorithms.

Lattice-Based Digital Signatures

Lattice-based signature schemes are employed for:

- Transaction authentication,
- Identity verification,
- Non-repudiation.

These algorithms offer strong resistance against quantum adversaries.

Hash-Based Authentication

Hash-based signatures provide secure verification mechanisms and support long-term integrity preservation.

5.4 Secure Off-Chain Storage

Due to the large volume of healthcare data, actual medical records are stored in encrypted off-chain repositories, while blockchain stores:

- Cryptographic hashes,
- Access permissions,
- Audit logs,
- Metadata references.

This approach improves scalability and efficiency.

5.5 Access Control Mechanism

Smart contracts enforce role-based access control policies to ensure that only authorized entities can access specific health records.

Access rights include:

- Read permissions,
- Update permissions,
- Emergency access protocols,
- Revocation mechanisms.

6. SYSTEM ARCHITECTURE

The proposed system consists of the following modules:

1. Data Collection Layer.
2. IoMT Integration Layer.
3. Encryption and Post-Quantum Signature Layer.
4. Permissioned Blockchain Network.
5. Smart Contract Access Control Layer.
6. Off-Chain Secure Storage.
7. Healthcare Service Providers.
8. Patient Access and Monitoring Interface.

7. EXPERIMENTAL EVALUATION

The proposed framework can be evaluated using simulation environments such as Hyperledger Fabric integrated with post-quantum cryptographic libraries.

Performance Metrics

The evaluation metrics include:

- Transaction Throughput,
- Latency,
- Signature Generation Time,
- Signature Verification Time,
- Storage Overhead,
- Computational Cost,
- Scalability,
- Access Response Time,
- Security Strength.

Comparative analysis can be conducted against classical blockchain implementations utilizing RSA and ECDSA.

8. RESULTS AND DISCUSSION

The integration of post-quantum cryptography enhances resilience against future quantum attacks while preserving the core advantages of blockchain technology. The permissioned architecture offers efficient transaction processing and controlled participation.

Experimental observations indicate that although post-quantum algorithms introduce additional computational overhead, the security benefits substantially outweigh the associated costs for healthcare applications requiring long-term data protection.

The proposed framework successfully balances security, scalability, transparency, and privacy preservation.

9. Applications

The proposed framework can be applied in various healthcare domains, including:

- Electronic Health Record Management,
- Telemedicine Platforms,
- Smart Hospitals,

- Medical Insurance Systems,
- Remote Patient Monitoring,
- Clinical Research Data Sharing,
- Pharmaceutical Supply Chain Tracking,
- National Health Information Exchanges.

10. ADVANTAGES

- Resistant to future quantum computing attacks.
- Ensures long-term confidentiality of medical records.
- Provides decentralized trust and immutability.
- Enhances transparency and accountability.
- Supports secure interoperability among healthcare providers.
- Enables fine-grained access control.
- Improves patient privacy and ownership of health data.
- Reduces risks associated with centralized databases.

11. LIMITATIONS

- Post-quantum algorithms often require larger key and signature sizes.
- Additional computational overhead may affect resource-constrained environments.
- Integration with existing healthcare infrastructures can be complex.
- Regulatory compliance considerations vary across jurisdictions.
- Standardization of post-quantum blockchain solutions is still evolving.

12. FUTURE SCOPE

Future research may explore lightweight post-quantum algorithms optimized for Internet of Medical Things devices. Artificial Intelligence-based anomaly detection mechanisms can be integrated to identify unauthorized access attempts. Additionally, quantum key distribution and privacy-preserving techniques such as zero-knowledge proofs may further strengthen healthcare security architectures.

13. CONCLUSION

This paper presented a Quantum-Resistant Blockchain framework for safeguarding healthcare data against emerging quantum computing threats. By integrating post-quantum cryptographic techniques within a permissioned blockchain architecture, the proposed model ensures confidentiality, integrity, authenticity, and secure access

control for sensitive medical information. Although post-quantum approaches introduce additional computational requirements, they provide essential protection for healthcare systems that demand long-term security. The proposed framework represents a promising step toward building future-proof healthcare infrastructures capable of withstanding next-generation cyber threats.

REFERENCES

1. Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
2. Bernstein, D. J., Buchmann, J., and Dahmen, E., *Post-Quantum Cryptography*, Springer, 2009.
3. NIST, "Post-Quantum Cryptography Standardization Project," National Institute of Standards and Technology, 2024.
4. Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A., "MedRec: Using Blockchain for Medical Data Access and Permission Management," Proceedings of the IEEE Open & Big Data Conference, 2016.
5. Alhadhrami, Z., et al., "The Adoption of Blockchain Technology in Healthcare: A Systematic Review," Journal of King Saud University – Computer and Information Sciences, 2021.
6. Hyperledger Foundation, "Hyperledger Fabric Architecture and Security Model," 2023.
7. Chen, L., Jordan, S., Liu, Y., Moody, D., and Peralta, R., "Report on Post-Quantum Cryptography," NIST Internal Report, 2016.