International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

SECURE ELECTRONIC HEALTH RECORDS USING QUANTUM-RESISTANT BLOCKCHAIN

[1] P.V RAVI KUMAR, [2] MAKKALA VENKATA NAGA CHOWDA NIKHIL,[3] YARRA ANAND KUMAR REDDY,[4] KALUVA SRIKANTH,[5] SHAIK VASEEM, SRI SRINU

[1] PROFESSOR& INCHARGE, DEPARTMENT OF CSE (AI) & AIML, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY AND SCIENCES, DEVARAJUGATTU, PEDDARAVEEDU (MD), MARKAPUR.

[2,3,4,5,]STUDENT, DEPARTMENT OF CSE (AI) & AIML, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY AND SCIENCES, DEVARAJUGATTU, PEDDARAVEEDU (MD), MARKAPUR.

ABSTRACT

The rapid digitalization of healthcare systems has increased the demand for secure and reliable management of sensitive patient data. While blockchain technology offers strong security through decentralization and cryptographic techniques, it remains vulnerable to future quantum computing threats that could break traditional encryption methods. This study proposes a quantum-resistant blockchain framework for secure health data management by integrating post-quantum cryptographic algorithms with blockchain architecture. The system utilizes decentralized ledger technology to store and manage electronic health records (EHRs), ensuring data integrity, transparency, and controlled access. Smart contracts are employed to automate secure data sharing among authorized healthcare providers while preserving patient privacy. Additionally, quantum-resistant techniques such as lattice-based cryptography and hash-based signatures are incorporated to protect against quantum attacks. By combining blockchain immutability with quantum-safe encryption, the proposed system ensures long-term data security, prevents unauthorized access, and enhances trust in healthcare data management systems.

Keywords

Quantum-Resistant Blockchain, Healthcare Data Security, Post-Quantum Cryptography, Electronic Health Records (EHR), Smart Contracts, Data Privacy, Secure Data Sharing

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

I. INTRODUCTION

The healthcare sector is undergoing rapid digital transformation with the widespread adoption of electronic health records (EHRs), telemedicine, and cloud-based data management systems. While these advancements improve accessibility and efficiency, they also introduce significant challenges related to data security, privacy, and integrity. Medical data is highly sensitive, and unauthorized access or tampering can lead to serious consequences, including misdiagnosis, privacy breaches, and financial loss. Therefore, ensuring secure storage and transmission of healthcare data has become a critical concern.

Blockchain technology has emerged as a promising solution for secure data management due to its decentralized, transparent, and immutable nature. By storing data across distributed ledgers, blockchain eliminates the need for a central authority and reduces the risk of single-point failures. It also enables secure and traceable data sharing through cryptographic techniques and smart contracts, allowing only authorized users to access patient information. However, most existing blockchain systems rely on classical cryptographic algorithms such as RSA and ECC, which are vulnerable to attacks from emerging quantum computers.

Quantum computing has the potential to break widely used encryption methods, posing a serious threat to current cybersecurity systems. As quantum technologies continue to advance, there is an urgent need to develop quantum-resistant security mechanisms that can withstand such attacks. Post-quantum cryptography offers alternative cryptographic techniques designed to be secure against quantum attacks, including lattice-based, hash-based, and code-based algorithms.

II. LITERATURE REVIEW

Recent research highlights the growing adoption of blockchain technology in healthcare for secure data management, ensuring decentralization, transparency, and data integrity through distributed ledger systems [1][2]. The use of smart contracts has further enhanced automated and secure sharing of electronic health records (EHRs) among authorized stakeholders, reducing manual intervention and improving efficiency [3]. However, most existing blockchain frameworks rely on classical cryptographic algorithms, which are vulnerable to quantum computing attacks [4].

To address this issue, post-quantum cryptography has been introduced, providing quantum-resistant algorithms such as lattice-based, hash-based, and code-based techniques that ensure long-term data security [5]. Recent

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

studies propose hybrid models that integrate blockchain with quantum-resistant cryptographic methods, combining the immutability of blockchain with advanced encryption techniques to protect sensitive healthcare data [6]. Furthermore, research has focused on improving scalability, performance, and security of blockchain-based healthcare systems through optimized architectures and lightweight cryptographic solutions [7].

Despite these advancements, existing solutions still face challenges in fully implementing quantum-resistant mechanisms and ensuring efficient real-world deployment, highlighting the need for a comprehensive and future-proof framework for secure healthcare data management [8].

III. EXISTING SYSTEM

The existing systems for securing healthcare data primarily rely on traditional blockchain technology combined with classical cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC). These systems use decentralized ledger mechanisms to store electronic health records (EHRs), ensuring data integrity, transparency, and tamper resistance. Smart contracts are commonly integrated to automate data access and sharing between healthcare providers, patients, and other stakeholders, improving efficiency and reducing manual intervention. Additionally, cloud-based storage is often used alongside blockchain to handle large volumes of medical data, enabling easy access and scalability.

IV. PROPOSED SYSTEM

The proposed system introduces a **Quantum-Resistant Blockchain framework** for secure healthcare data management, designed to overcome the limitations of existing systems by integrating post-quantum cryptographic techniques with blockchain technology. The system ensures secure storage, transmission, and controlled access of electronic health records (EHRs) while being resilient to future quantum computing attacks.

The architecture consists of multiple layers, starting with **data acquisition**, where patient data such as medical records, diagnostic reports, and prescriptions are collected from hospitals and healthcare providers. This data is then encrypted using **quantum-resistant cryptographic algorithms** such as lattice-based encryption and hash-based digital signatures, ensuring long-term security. The encrypted data is stored in a **blockchain network**, where each block maintains a secure, immutable record of transactions.

A **smart contract layer** is integrated to manage access control and automate data sharing between authorized users such as

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

doctors, patients, and healthcare institutions. These smart contracts enforce strict authentication and permission policies, ensuring that only authorized entities can access or modify the data. Additionally, a **distributed storage system** (such as IPFS or cloud storage) is used to store large medical files, while only secure hash references are maintained on the blockchain to improve scalability and efficiency.

V. METHODOLOGY

The proposed methodology for implementing a Quantum-Resistant Blockchain for secure healthcare data management follows a structured and systematic approach. The process begins with **data collection**, where patient information such as electronic health records (EHRs), diagnostic reports, and medical histories are gathered from healthcare providers. This data is then prepared through **data preprocessing**, which includes formatting, validation, and removal of inconsistencies to ensure accuracy and standardization.

Next, the system applies **quantum-resistant encryption techniques** to secure the data before storage. Post-quantum cryptographic algorithms such as lattice-based encryption and hash-based digital signatures are used to protect the data against potential quantum attacks. This ensures that sensitive healthcare information remains secure even with advancements in quantum computing.

After encryption, the data is stored using a **blockchain network**, where each transaction is recorded in blocks and linked using cryptographic hashes. This ensures immutability, transparency, and tamper resistance. To handle large medical files efficiently, a **distributed storage system** such as IPFS or cloud storage is used, while only the hash values and metadata are stored on the blockchain to reduce storage overhead.

VI. SYSTEM MODEL

System Architecture

VII. RESULTS AND DISCUSSIONS

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

In above screen click on 'New User Sign up' link to get below page

In above screen patient is getting registered and then press button to get below page

In above screen sign up process completed and then I am displaying entire log obtained from Blockchain after record storage. This log contains details like Transaction no, block no, hash code and many other details. Similarly you can add any number of patients

In above screen doctor is getting registered and then press button to get below page

In above screen doctor registration completed and now click on 'Patient Login' link to get below page

In above screen patient is login and after login will get below page

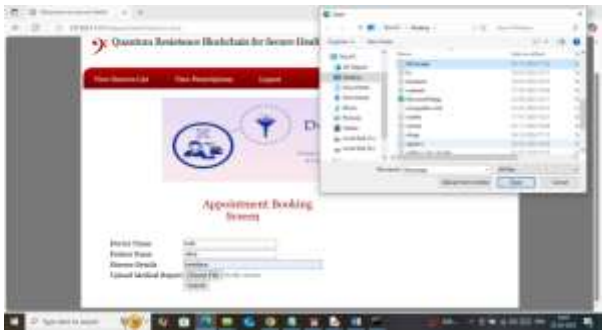
In above screen patient can click on 'View Doctors List' link to get below page

In above screen patient can view list of available doctors and can click on 'Click Here for Appointment' link to book appointment

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

with desired doctor and then will get below page



In above screen while booking appointment patient will enter disease details along with available reports which will get encrypted and now click on buttons to get below page

In above screen can see appointment is confirmed with doctor along with Blockchain log details. Now click on 'View Prescription' link to get below page

In above screen patient can view prescription which is in pending state and now logout and login as doctor to generate prescription

In above screen doctor is login and after login will get below page

In above screen doctor can click on 'View Appointments' link to view list of appointment and then will get below page

In above screen doctor can view all patient details and can download patient report and can click on 'Click Here for prescription' link to generate prescription

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

In above screen doctor will write and upload some prescription and then press button to get below page

In above screen prescription successfully generated and now logout and login and patient to access prescription

In above screen patient can view entire prescription along with date and can click on 'Click Here' link to download prescription in decrypted format like below page

In above screen prescription is downloaded in decrypted format but at server side it will saved in quantum encrypted data like below page

In above screen can see file data saved in encrypted data.

So by using above application we can secured patient data using Quantum algorithms and can avoid any data tamper using decentralized Blockchain technology.

VIII. CONCLUSION

The proposed Quantum-Resistant Blockchain framework provides a secure and future-proof solution for managing sensitive healthcare data. By integrating blockchain technology with post-quantum cryptographic algorithms, the system ensures data integrity, privacy, and protection against both current and emerging cyber threats, including quantum computing attacks. The use of decentralized architecture and smart contracts enhances transparency, secure data sharing, and controlled access among healthcare stakeholders.

Additionally, the incorporation of distributed storage mechanisms improves scalability and efficiency in handling large medical datasets. The system overcomes the limitations of traditional blockchain-based healthcare solutions by addressing vulnerabilities in classical encryption methods and ensuring long-term security. Overall, the proposed

approach enhances trust, reliability, and efficiency in healthcare data management, making it a robust solution for next-generation secure healthcare systems.

IX. FUTURE WORK:

The proposed Quantum-Resistant Blockchain system can be further enhanced by exploring more advanced and efficient post-quantum cryptographic algorithms to improve security and reduce computational overhead. Future work may focus on optimizing these algorithms for real-time healthcare applications, ensuring faster encryption, decryption, and transaction processing.

Integration with emerging technologies such as artificial intelligence and machine learning can enable intelligent data analysis, anomaly detection, and predictive healthcare insights while maintaining data security. Additionally, the system can be extended to support interoperability across multiple healthcare institutions and blockchain networks, enabling seamless and secure data exchange on a larger scale.

Further research can also focus on developing lightweight blockchain frameworks and energy-efficient consensus mechanisms to improve scalability and reduce resource consumption. The implementation of user-friendly interfaces and mobile applications can enhance accessibility for patients and healthcare providers.

XI. REFERENCES

[1] Jajam Venkata Anil Kumar, Dr. G. Charles Babu, "Automating Content Utilizing Big Data Innovations", *Journal of Advances and Scholarly Researches in Allied EducationVol. 15, Issue No. 9, October-2018, ISSN 2230-7540,* IIFS : 1.6 (2014), INDEX COPERNICUS : 49060 (2018), IJINDEX : 3.46 (2018), pp.635-639, 2018.

[2] Jajam Venkata Anil Kumar, Dr. G. Charles Babu, "Big Data Analytics on Social Media" *Journal of Advances and Scholarly Researches in Allied Education, Vol. XII, Issue No. 23, October-2016, ISSN 2230-7540,* IIFS : 1.6 (2014), INDEX COPERNICUS : 49060 (2018), IJINDEX : 3.46 (2018), pp. 389-393,2016.

[3] Jajam Venkata Anil Kumar, Dr. G. Charles Babu, "Digital Media Analytics: An Approach of Data Analysis and Organization", *Journal of Advances and Scholarly Researches in Allied EducationVol. XIV, Issue No. 1, October-2017, ISSN 2230-7540,* IIFS : 1.6 (2014), INDEX COPERNICUS : 49060 (2018), IJINDEX : 3.46 (2018), pp. 676-679, 2018.

[4] D. Boneh and V. Shoup, "A Graduate Course in Applied Cryptography," 2020.

[5] NIST, "Post-Quantum Cryptography Standardization," National Institute of Standards and Technology, 2022.

[6] C. Cachin and M. Vukolić, "Blockchain Consensus Protocols in the Wild," *arXiv preprint arXiv:1707.01873*, 2017.

[7] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," *IEEE Internet of Things Journal*, 2017.