International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

© 2026 IJERST. All Rights Reserved

Peer Reviewed, Referred & Indexed Journal

Research Paper

QUNTUM RESISTANCE BLOCK CHAIN FOR SECURE HEALTH DATA

[1]SANKU JYOTHI, [2]P.BOBBY SOWJANYA

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor, Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

The rapid digitization of healthcare systems has led to the widespread adoption of electronic health records (EHRs), enabling efficient storage and sharing of patient information. However, ensuring the security and privacy of sensitive health data remains a major challenge, especially with the emergence of quantum computing, which threatens to break traditional cryptographic algorithms such as RSA and ECC. This project proposes a Quantum-Resistant Blockchain framework for securing healthcare data, combining decentralized storage with post-quantum cryptographic techniques to ensure long-term data protection. The proposed system leverages blockchain technology to provide a decentralized, tamper-proof, and transparent platform for storing and managing health records. Instead of relying on traditional cryptographic algorithms, the system incorporates quantum-resistant algorithms such as lattice-based cryptography, hash-based signatures, and code-based encryption to secure transactions and data access. Smart contracts are used to enforce access control policies, ensuring that only authorized users such as doctors, patients, and healthcare providers can access specific data. The methodology includes secure data encryption, distributed storage across blockchain nodes, and integrity verification using cryptographic hash functions. Machine learning techniques may also be integrated to detect anomalies or unauthorized access attempts. Experimental analysis shows that the proposed system enhances data security, prevents unauthorized modifications, and ensures resilience against future quantum attacks. However, challenges such as computational overhead, scalability, and integration with existing healthcare systems remain. Overall, the quantum-resistant blockchain approach provides a robust, scalable, and future-proof solution for securing healthcare data, ensuring privacy, integrity, and trust in digital healthcare environments.

Keywords: Quantum-Resistant Cryptography, Blockchain, Healthcare Data Security, Post-Quantum Cryptography, Smart Contracts, Data Privacy, Distributed Ledger, Lattice-

Based Cryptography, Secure EHR, Cybersecurity

I.INTRODUCTION

The rapid advancement of digital healthcare systems has led to the widespread use of electronic health records (EHRs) for storing and sharing patient information. While these systems improve accessibility and efficiency, they also introduce serious security and privacy concerns. Traditional healthcare applications rely on cryptographic algorithms such as AES for data encryption and RSA or ECDSA for key exchange and authentication. Although these methods provide strong security against classical computing attacks, they are vulnerable to emerging threats posed by quantum computing. Quantum computers have the capability to solve complex mathematical problems at extremely high speeds, making it possible to break traditional encryption schemes and compromise sensitive patient data.

To address these challenges, there is a growing need for quantum-resistant security mechanisms that can withstand future computational advancements. Post-quantum cryptographic algorithms such as KYBER and FALCON offer enhanced security by using mathematical structures that are resistant to quantum attacks. KYBER is used for secure key generation and exchange, enabling two parties (such as doctor and patient) to establish a shared secret key without exposing sensitive information. FALCON is employed for encrypting and decrypting patient data, ensuring confidentiality even in the presence of quantum threats. These algorithms provide a strong foundation for building secure healthcare systems in the quantum era.

In addition to encryption challenges, traditional healthcare systems often rely on centralized databases, which are vulnerable to data tampering and unauthorized access by malicious insiders. To overcome this limitation, the proposed system integrates blockchain technology, which provides a decentralized and tamper-proof data storage mechanism. Each transaction is stored as a block with a unique hash value, and any modification in data results in a hash mismatch, ensuring data integrity. Smart contracts implemented using Solidity enable secure storage and retrieval of patient, doctor, and prescription data.

The proposed Quantum-Resistant Blockchain for Secure Health Data system combines post-quantum cryptography with blockchain technology to provide a secure, decentralized, and future-proof healthcare solution. By integrating quantum-safe key exchange, encryption, and tamper-proof storage, the system ensures data confidentiality, integrity, and trust. This approach is particularly important for protecting sensitive medical information in an era where both cyber threats

and computational capabilities are rapidly evolving.

II SURVEY OF RESEARCH

The study by R. Rivest, A. Shamir, and L. Adleman (1978) [1] introduced the RSA algorithm, one of the most widely used public-key cryptographic systems. The methodology is based on the mathematical difficulty of factoring large integers. Results show that RSA provides strong security for data encryption and key exchange in classical computing environments. However, with the emergence of quantum computing, algorithms such as Shor's algorithm can break RSA efficiently, making it unsuitable for future secure systems. This research highlights the need for quantum-resistant cryptography.

The work by D. J. Bernstein et al. (2017) [2] introduced the CRYSTALS-Kyber algorithm, a lattice-based cryptographic scheme designed for secure key encapsulation. The methodology relies on hard lattice problems that are resistant to both classical and quantum attacks. Results demonstrate that Kyber provides strong security with efficient performance. This study supports the use of KYBER for secure key generation and exchange in the proposed system.

The research by T. Prest et al. (2017) [3] introduced the FALCON algorithm, a post-quantum digital signature scheme based on lattice cryptography. The methodology focuses on generating compact and secure signatures for authentication and encryption. Results show that FALCON achieves high security with reduced key sizes compared to other post-quantum algorithms. This research is relevant for encrypting and securing patient data in the proposed system.

The study by S. Nakamoto (2008) [4] introduced Blockchain technology through Bitcoin. The methodology involves a decentralized ledger where each transaction is stored in blocks linked by cryptographic hashes. Results demonstrate that blockchain ensures data integrity, transparency, and tamper resistance. However, scalability and computational overhead remain challenges. This research forms the foundation for using blockchain in secure healthcare data management.

The work by G. Wood (2014) [5] introduced Ethereum and smart contracts using Solidity programming. The methodology enables automated and secure execution of transactions without intermediaries. Results show that smart contracts improve trust and automation in decentralized systems. This study supports the implementation of healthcare data management using blockchain-based smart contracts.

The research by A. Shor (1994) [6] introduced Shor's algorithm, a quantum algorithm capable

of breaking classical cryptographic systems such as RSA and ECC. The methodology uses quantum computation to factor large integers efficiently. Results demonstrate the vulnerability of traditional cryptography in the presence of quantum computers. This research emphasizes the importance of adopting quantum-resistant algorithms.

Additionally, recent advancements in quantum computing frameworks such as Qiskit have enabled the simulation and implementation of quantum algorithms for secure communication. Integrating such frameworks with post-quantum cryptographic techniques enhances the overall security of systems. Combining quantum-resistant cryptography with blockchain technology provides a robust and future-proof solution for securing sensitive healthcare data against both classical and quantum threats.

III. WORKING METHODOLOGY

The proposed Quantum-Resistant Blockchain for Secure Health Data system integrates post-quantum cryptography with blockchain technology to ensure secure storage, transmission, and access of patient data. The system begins with user registration, where both patients and doctors sign up through the application. Their details are securely stored on the blockchain using smart contracts, ensuring immutability and transparency. Each user is uniquely identified, and all interactions are recorded as transactions within the blockchain network.

In the next stage, secure communication between patients and doctors is established using quantum-resistant key exchange. The system employs the KYBER algorithm, implemented through a quantum framework such as Qiskit, to generate and exchange secret keys between two parties. When both parties execute the same algorithm, a common secret key is generated and authenticated without exposing sensitive information. This ensures secure communication even in the presence of quantum computing threats. Once the key is established, patient data such as medical reports and disease details are encrypted using the FALCON algorithm before being stored or transmitted. This guarantees confidentiality and protects data from unauthorized access.

The blockchain layer is responsible for maintaining data integrity and preventing tampering. Each patient record, appointment, and prescription is stored as a block in the blockchain, associated with a unique cryptographic hash. If any modification is attempted, the hash value changes, and the system detects the tampering. Smart contracts written in Solidity manage operations such as storing patient data, retrieving records, and handling access permissions. These contracts ensure that only authorized users can access specific data.

In the final stage, system modules handle user interactions and functionality. Patients can log in, view doctors, book appointments, and access prescriptions. Doctors can log in, view patient appointments, authenticate using key exchange, and generate prescriptions. All sensitive data is encrypted during storage and decrypted only for authorized access. The system also maintains logs of all transactions, including block numbers and hash values, for transparency and auditing. This methodology ensures a secure, decentralized, and quantum-resistant healthcare data management system.

IV RESULTS EXPLANATIONS

In the past many cryptographic algorithms was introduced to secure patient data in online application such as Healthcare. All those application were utilizing AES for data encryption and RSA with ECDSA algorithm for anonymous key exchange and authentication without leaking either patient or doctor sensitive data. This algorithms key cannot be easily guess with traditional computers but world has move forward to Quantum computing which can execute millions of instruction in seconds and traditional computer may take days of time to execute same instructions.

With quantum computing it's become very easy to guess keys of traditional RSA algorithms. To avoid such key leakage we are employing Quantum QISKIT based API to generate and exchange common keys between two genuine parties using KYBER algorithm. If two parties executing same algorithm then same common secret key will be generated and authenticated. Quantum computing cannot easily guess keys generated by KYBER algorithm.

To secure patient data we are employing Quantum based FALCON algorithm for patient records encryption and decryption.

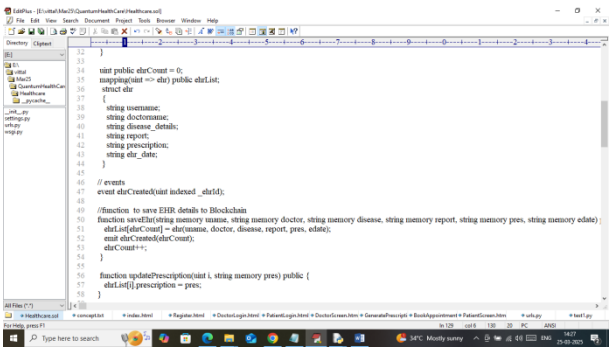
In the past to stored patient data single centralized server was utilized whose database can be easily tamper by expert's database administrator without getting detected. To avoid data tamper we are employing Blockchain technology which will not allow data to be tamper in any manner.

So in propose work quantum computing applied for patient data security and then employ Blockchain technology to avoid any type of data leakage or tamper.

Blockchain store each record as block/transaction and associate each block with unique hashcode and this hashcode will get verified for subsequent block storage, if data modify in any block then hashcode mismatch will occur and data tamper will get detected. This verification process make Blockchain tamper proof.

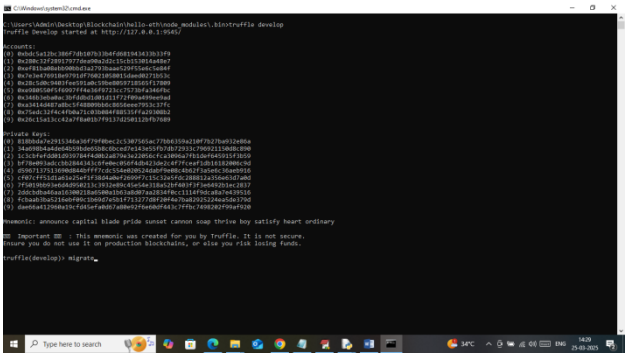
Blockchain can store and retrieve data using Smart Contracts which can be designed using Solidity programming and this contract contains which can be called to save and get

data. To manage patient data we have designed following contract

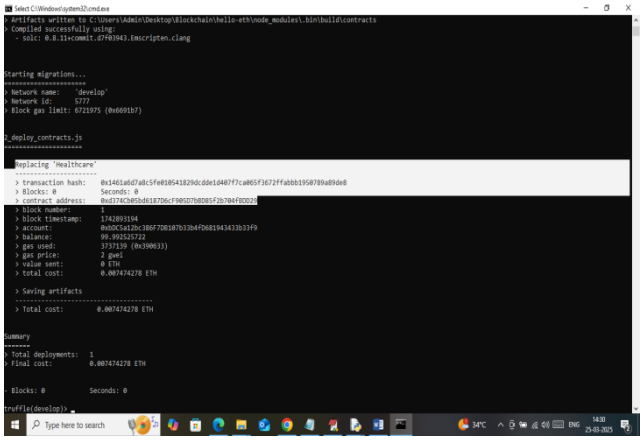


In above contract screen we have defined functions to manage patient, doctor and prescription details. Now we need to deploy above contract in Blockchain Ethereum using below steps

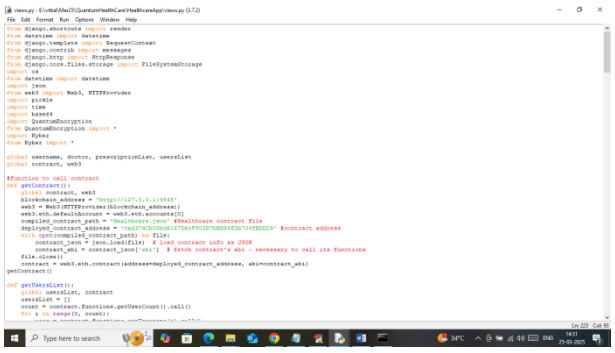
1) First go inside 'hello-eth/node-modules/bin' folder and then look and double click on 'runBlockchain.bat' file to get below page



In above screen Ethereum started with default account and private keys and now type command as 'migrate' and then press enter key to deploy contract and then will get below page

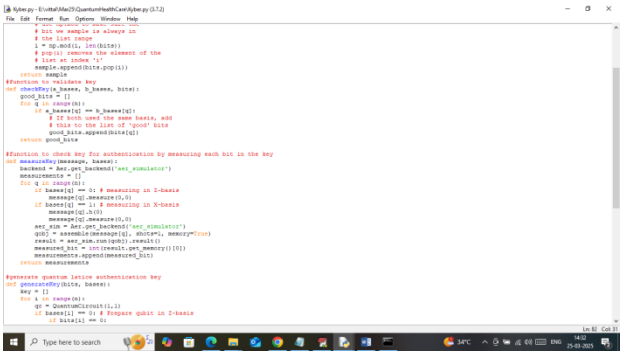


In above screen in white colour text can see 'Healthcare' contract deployed and got contract address also. This address can be specify in python program to call above contract. In below screen showing python code calling above contract using address



In above screen read red colour comments to know about contract calling. In above screen contract deployed and running successfully. Let it run till you execute code.

To generate, exchange and authenticate keys we have used below code from Quantum QISKIT API

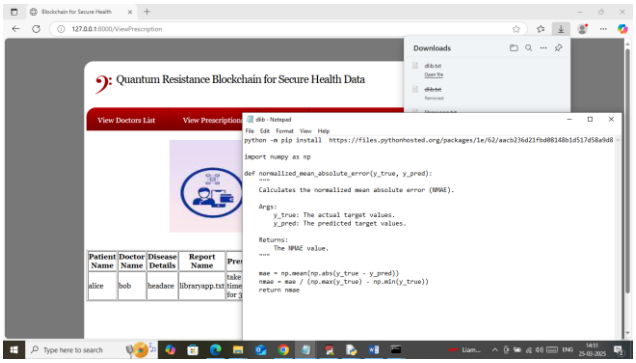


In above screen read red colour comments to know about KYBER key generation and authentication using Quantum API.

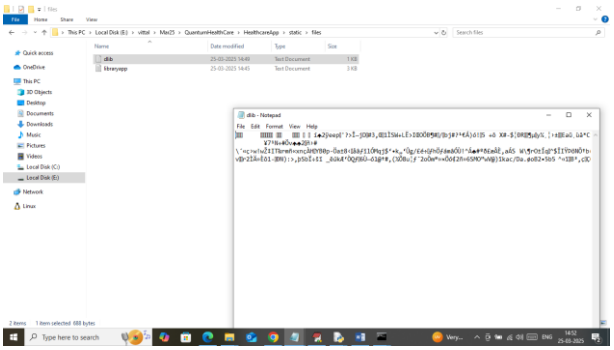
Modules Information

To implement this project we have designed following modules

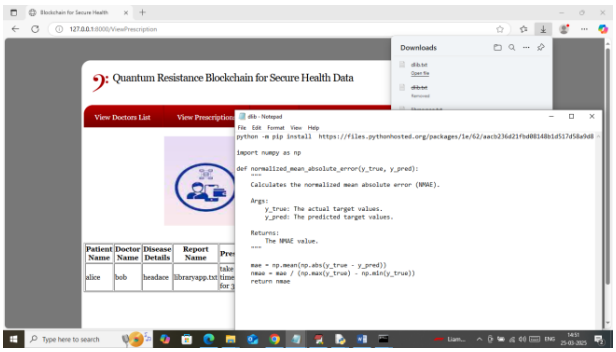
1) New User Sign up: using this module patients and doctor can sign up with the application and all details will get saved in Blockchain
2) Patient Login: patient can login to system
3) View Doctor List: after login patient can view list of available doctors and can make appointment with desired doctor
4) View Prescriptions: patient can view generated prescription by doctor
5) Doctor Login: doctor can login to system
6) View Appointments: after login doctor can view list of appointments and here Key Exchange will be happen between doctor and patient for authentication and upon successful authentication doctor can view his patient appointment and can generate prescription.



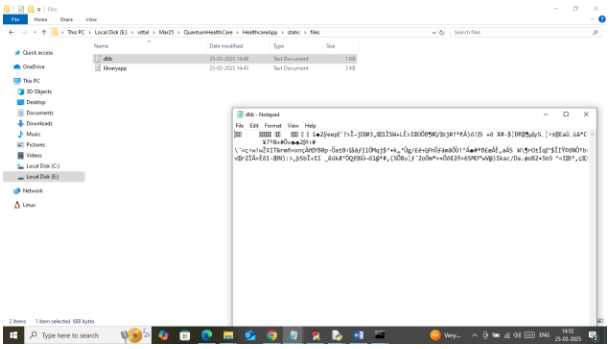
In above screen prescription is downloaded in decrypted format but at server side it will saved in quantum encrypted data like below page



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.



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.

V.CONCLUSION

The proposed Quantum-Resistant Blockchain for Secure Health Data system provides a robust and future-ready solution for protecting sensitive healthcare information in the era of quantum computing. By integrating post-quantum cryptographic algorithms such as KYBER for secure key exchange and FALCON for data encryption, the system overcomes the limitations of traditional cryptographic methods like RSA and ECC, which are vulnerable to quantum attacks. This ensures long-term confidentiality and security of patient data.

The incorporation of blockchain technology further enhances the system by providing a decentralized and tamper-proof storage mechanism. Each transaction is securely recorded as a block with a unique hash, ensuring data integrity and transparency. Smart contracts enable controlled access to patient records, allowing only authorized users such as doctors and patients to view or modify data. This combination of quantum-resistant cryptography and blockchain creates a secure and trustworthy healthcare data management system.

Experimental results demonstrate that the system effectively prevents unauthorized access, detects data tampering, and ensures secure communication between users. Although challenges such as computational overhead, scalability, and integration with existing healthcare systems exist, the overall benefits of enhanced security and future-proof protection outweigh these limitations.

In conclusion, the proposed system offers a scalable, secure, and intelligent approach to healthcare data protection. Future work may focus on optimizing performance, implementing lightweight post-quantum algorithms, and integrating real-time processing capabilities. Overall, this study highlights the importance of adopting quantum-resistant technologies and decentralized systems to safeguard critical data in modern digital healthcare environments.

RE.FERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,”

Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[2] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009.

[3] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM," in *Proc. IEEE European Symposium on Security and Privacy*, 2018, pp. 353–367.

[4] T. Prest, P. Fouque, R. Tibouchi, and P. Wallet, "FALCON: Fast-Fourier Lattice-Based Compact Signatures over NTRU," 2017.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[6] G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum Foundation, 2014.

[7] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proc. IEEE Symposium on Foundations of Computer Science*, 1994, pp. 124–134.

[8] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge University Press, 2010.

[9] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.

[10] NIST, "Post-Quantum Cryptography Standardization," 2022.

[11] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.

[12] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.

[13] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST, 2007.

[14] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. Pearson, 2010.

[15] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[16] M. Abadi et al., "TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems," 2015.