IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

QUANTUM-SAFE CLOUD STORAGE FOR SECURE HEALTHCARE RECORDS

Quantum-safe cloud storage secures healthcare records using advanced cryptography that protects data even against future quantum computing threats.

[1]Sathish Kumar P, [2]Chandrakala S, [3]Aldan Jeri M, [4]Avinesh R, [5]Ganapathi M
[1]M.E Assistant Professor, [2]M.E Assistant Professor, [3]B.E.(Cyber) Student IV Year, [4]B.E.(Cyber) Student IV Year, [5]B.E.(Cyber) Student IV Year
[1,2,3,4,5]Department of Cybersecurity
[1]Paavai Engineering College (Autonomous), Namakkal, Tamil Nadu, India

Abstract: The rapid adoption of cloud computing in healthcare has improved data accessibility and scalability but introduced significant security challenges. Traditional encryption techniques, such as RSA and ECC, are vulnerable to potential attacks from quantum computers. This paper proposes a quantum-safe cloud storage framework for securing electronic health records (EHRs) using post-quantum cryptographic algorithms. The system integrates lattice-based encryption for secure data storage and quantum-resistant key exchange mechanisms to protect sensitive medical data. Additionally, role-based access control and data integrity verification techniques are implemented to ensure authorized access and prevent tampering. The proposed model enhances confidentiality, integrity, and long-term security of healthcare data against both classical and quantum threats. Experimental analysis demonstrates improved resilience with acceptable computational overhead, making it suitable for real-world healthcare applications.

Index Terms: Quantum-safe security, Post-quantum cryptography, Cloud storage, Healthcare data security, Electronic Health Records (EHR), Data privacy, Lattice-based cryptography, Digital signatures, Secure key management, Role-Based Access Control (RBAC), Data integrity, Encryption, Cloud security.

I. INTRODUCTION

The digital transformation of the healthcare sector has led to the widespread adoption of cloud computing technologies for storing, managing, and sharing electronic health records (EHRs). Cloud platforms provide significant advantages, including scalability, cost-effectiveness, and real-time accessibility, enabling healthcare providers to deliver faster and more efficient services. Patients' medical histories, diagnostic reports, and treatment data can now be accessed remotely, improving coordination among medical professionals and enhancing overall patient care. However, the migration of sensitive healthcare data to cloud environments has also introduced serious security and privacy challenges, as such data becomes a prime target for cyberattacks and unauthorized access.

To protect healthcare information, traditional cryptographic techniques such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) are commonly used. These methods have proven effective against classical computational threats and are widely implemented in existing cloud security frameworks. Despite their current reliability, these encryption schemes are fundamentally vulnerable to the rapid advancements in quantum computing. Quantum computers, leveraging algorithms such as Shor's algorithm, have the theoretical capability to break widely used public-key cryptosystems by solving complex mathematical problems like integer factorization and

discrete logarithms in significantly reduced time. This poses a critical threat to long-term data security, especially for healthcare records that must remain confidential for many years.

The concept of "harvest now, decrypt later" further intensifies this concern, where encrypted data stored today could be intercepted and decrypted in the future once quantum computing becomes sufficiently advanced. This scenario is particularly alarming in the healthcare domain, where data sensitivity and privacy are of utmost importance. As a result, there is an urgent need to transition from classical cryptographic approaches to quantum-resistant or post-quantum cryptographic (PQC) solutions that can safeguard data against both present and future threats.

In this context, the proposed research focuses on developing a quantum-safe cloud storage framework tailored for secure healthcare record management. The system integrates advanced post-quantum cryptographic algorithms, secure key exchange mechanisms, and robust access control strategies to ensure data confidentiality, integrity, and availability. By incorporating Role-Based Access Control (RBAC), the framework also ensures that only authorized users can access specific information based on their roles within the healthcare system.

The primary objective of this work is to design a secure, efficient, and future-proof cloud storage solution that addresses the limitations of existing systems. This includes mitigating vulnerabilities to quantum attacks, improving data protection mechanisms, and ensuring compliance with healthcare data security requirements. Through this approach, the study aims to contribute to the development of next-generation secure cloud infrastructures capable of protecting sensitive medical information in the evolving landscape of quantum computing.

II. LITERATURE REVIEW

Traditional cloud security mechanisms rely heavily on cryptographic algorithms such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) to ensure data confidentiality, integrity, and authentication. These techniques have been widely adopted in securing sensitive information, including healthcare records, due to their computational efficiency and strong resistance against classical attacks. However, with the rapid advancement of quantum computing, these conventional cryptographic approaches face significant limitations. In particular, algorithms like RSA and ECC are vulnerable to quantum-based attacks, especially those leveraging Shor's algorithm, which can efficiently solve integer factorization and discrete logarithm problems. Although symmetric encryption methods like AES are relatively more resistant, they still require larger key sizes to maintain security in a quantum environment.

To address these emerging threats, Post-Quantum Cryptography (PQC) has gained considerable attention as a promising solution for future-proof security. PQC includes a variety of cryptographic techniques designed to resist attacks from both classical and quantum computers. Among these, lattice-based cryptography is widely regarded for its strong security guarantees and practical performance, making it suitable for encryption and key exchange. Hash-based cryptographic methods provide secure digital signatures with proven resistance, while code-based cryptography offers robustness based on error-correcting codes.

Despite these advancements, existing cloud storage systems, particularly in the healthcare domain, still exhibit several shortcomings. Many lack adequate quantum resistance, making them vulnerable to future threats. Additionally, there are challenges related to efficient implementation, as some PQC algorithms introduce higher computational overhead. Furthermore, current systems often fail to provide fine-grained access control mechanisms, which are essential in healthcare environments where different users, such as doctors, patients, and administrators, require varying levels of data access. These limitations highlight the need for a more secure and efficient quantum-safe cloud storage framework tailored specifically for healthcare applications.

The rapid digital transformation of the healthcare sector has significantly increased the adoption of cloud computing for storing and managing electronic health records (EHRs), offering benefits such as scalability, cost efficiency, and real-time accessibility. This shift enables healthcare providers to access patient data remotely, improving diagnosis, treatment, and coordination among medical professionals. However, the storage of highly sensitive medical information in cloud environments also introduces serious security and privacy concerns, as healthcare data becomes a major target for cyberattacks.

Traditionally, cryptographic techniques such as AES, RSA, and ECC have been widely used to secure cloud data due to their strong protection against classical computational threats. Despite their effectiveness today, these algorithms are increasingly vulnerable to the emerging capabilities of quantum computing. In

particular, quantum algorithms such as Shor's algorithm have the potential to break widely used public-key cryptosystems by efficiently solving complex mathematical problems like integer factorization and discrete logarithms. This creates a critical risk for long-term data confidentiality, especially in healthcare, where records must remain secure for extended periods. Additionally, the concept of "harvest now, decrypt later" poses a significant threat, as encrypted data stored today could be intercepted and decrypted in the future when quantum technology becomes more advanced.

III. METHODOLOGY ARCHITECTURE ANALYSIS

The proposed methodology presents a comprehensive quantum-safe cloud storage framework tailored for securing healthcare records by integrating advanced post-quantum cryptographic mechanisms, robust access control, and efficient cloud architecture. The system is designed to address both current cybersecurity challenges and future quantum threats while maintaining usability and performance in real-world healthcare environments.

Initially, healthcare data such as patient records, diagnostic reports, and prescriptions are collected through a secure user interface used by authorized entities including doctors, patients, and administrative staff. Before transmission to the cloud, the data undergoes preprocessing steps such as formatting, validation, and segmentation to ensure consistency and efficient handling.

The core security layer of the system employs lattice-based post-quantum cryptographic algorithms, specifically CRYSTALS-Kyber for encryption and secure key encapsulation, which ensures that data remains confidential even against quantum-enabled adversaries. For authentication and integrity assurance, CRYSTALS-Dilithium is utilized to generate digital signatures, enabling verification of data origin and detection of any unauthorized modifications. Additionally, secure hashing algorithms are incorporated to produce unique message digests for each record, further strengthening integrity verification and enabling quick validation during data retrieval.

Once encrypted and signed, the data is transmitted through a secure communication channel (TLS-enhanced protocol) to the cloud storage infrastructure, where it is stored in an encrypted database. The cloud layer is designed with logical separation of storage and key management services to reduce the risk of centralized attacks. Encryption keys are handled through a secure key management module that leverages post-quantum key exchange mechanisms, ensuring safe distribution and storage of cryptographic keys without exposure to vulnerabilities.

To control access, the system integrates a Role-Based Access Control (RBAC) model combined with attribute-based constraints, allowing fine-grained authorization based on user roles, responsibilities, and contextual attributes such as time or location. For instance, doctors may have full access to patient records, while patients may only view their own data, and administrators may manage system operations without accessing sensitive medical details.

During data access, authenticated users submit requests that are verified using digital signatures and role validation. Upon successful authentication, the system initiates a secure decryption process using the appropriate post-quantum keys. The system also incorporates redundancy and backup strategies within the cloud to ensure data availability and resilience against failures or attacks such as data loss or ransomware. Performance optimization techniques, including selective encryption, efficient key management, and lightweight cryptographic operations, are applied to reduce computational overhead typically associated with post-quantum algorithms.

IV. IMPLEMENTATION / CASE STUDY

4.1 System Architecture

The implementation of the proposed quantum-safe cloud storage system follows a layered architecture consisting of the user interface layer, application server layer, cryptographic module, and cloud storage layer. Each layer is designed to perform specific functions while maintaining strong security boundaries. The user interface enables interaction between users and the system, while the backend server processes requests and enforces security policies. The cryptographic module ensures data protection using post-quantum algorithms, and the cloud layer handles secure storage and retrieval of encrypted healthcare data. This modular design improves scalability, maintainability, and security.

4.2 User Interface and Data Input

The front-end of the system is developed using modern web technologies to provide a user-friendly interface for doctors, patients, and administrators. Users can register, log in, upload healthcare records, and request access to stored data. Input data such as patient details, prescriptions, and diagnostic reports are validated to ensure accuracy and consistency before further processing.

4.3 Cryptographic Implementation

The core security of the system is achieved through the integration of post-quantum cryptographic algorithms. CRYSTALS-Kyber is implemented for encryption and secure key encapsulation, protecting data from quantum-based attacks. CRYSTALS-Dilithium is used for generating digital signatures, ensuring authentication and data integrity. These algorithms are integrated using standardized cryptographic libraries, replacing traditional methods like RSA and ECC. Hashing algorithms are also applied to generate message digests for additional integrity verification.

4.4 Secure Data Transmission

During data transmission, secure communication protocols such as HTTPS with TLS are used to protect data from interception and man-in-the-middle attacks. Before transmission, healthcare data is encrypted, ensuring that even if data packets are intercepted, they remain unreadable. This layer provides end-to-end security between users and the cloud system.

4.5 Cloud Storage Integration

The encrypted healthcare data is stored in a secure cloud environment such as AWS S3, Google Cloud Storage, or Firebase. Data is stored in encrypted format, ensuring confidentiality even if unauthorized access occurs. The system maintains logical separation between storage and key management to minimize security risks. Cloud services also provide scalability and high availability for handling large volumes of healthcare data.

4.6 Key Management System

A dedicated Key Management System (KMS) is implemented to securely generate, store, distribute, and rotate cryptographic keys. The system uses quantum-safe key exchange mechanisms to prevent key exposure. Private keys are securely stored and accessed only through authenticated processes, ensuring strong protection against key compromise.

4.7 Access Control Mechanism

The system uses Role-Based Access Control (RBAC) to manage user permissions. Different roles such as doctor, patient, and administrator are assigned specific access rights. This ensures that users can only access data relevant to their role. Additional constraints such as time-based or location-based access can also be implemented to enhance security.

4.8 Data Retrieval and Decryption

When an authorized user requests data, the system verifies user identity and role permissions. The encrypted data is retrieved from the cloud and decrypted using secure post-quantum keys. The system ensures that only authorized users can access readable data, maintaining strict confidentiality.

4.9 Data Integrity Verification

To ensure that data has not been altered, hashing algorithms are used to generate unique message digests during data upload. These hashes are verified during data retrieval to detect any tampering. Digital signatures further enhance integrity verification by confirming the authenticity of the data source.

4.10 Monitoring, Logging, and Security Auditing

The system includes logging mechanisms that record all user activities, including login attempts, data uploads, and access requests. These logs are monitored to detect suspicious activities and potential security threats. Auditing ensures accountability and helps in forensic analysis if a breach occurs.

4.11 Backup and Recovery

To ensure data availability, the system implements backup and recovery mechanisms using cloud-based redundancy. Data is periodically backed up and stored in multiple locations to prevent loss due to system failures or cyberattacks such as ransomware. This ensures reliability and continuous access to healthcare data.

4.12 Performance Optimization

Although post-quantum cryptographic algorithms introduce higher computational overhead, optimization techniques such as efficient key handling, selective encryption, and caching are applied to maintain system performance. The system is designed to balance high security with acceptable response time, making it suitable for real-time healthcare applications.

V. RESULTS AND KEY FINDINGS

5.1 Experimental Setup

The proposed quantum-safe cloud storage system was implemented in a simulated healthcare environment to evaluate its performance, security, and efficiency. The system was tested using sample electronic health records (EHRs) with varying data sizes. Post-quantum cryptographic algorithms, specifically CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for digital signatures, were integrated into the cloud framework. Performance metrics such as encryption time, decryption time, storage overhead, and access latency were analyzed and compared with traditional cryptographic methods.

5.2 Performance Analysis

The results indicate that the proposed system successfully secures healthcare data with a moderate increase in computational overhead. Encryption and decryption times were slightly higher compared to conventional algorithms like RSA and ECC due to the complexity of post-quantum techniques. However, the delay remained within acceptable limits for healthcare applications. The system demonstrated efficient data handling even for larger file sizes, ensuring scalability in real-world scenarios.

5.3 Security Evaluation

The implementation showed a significant improvement in security by providing resistance against both classical and quantum attacks. Unlike traditional cryptographic systems, the use of lattice-based algorithms ensures that sensitive healthcare data remains secure even in the presence of quantum computing threats. The integration of digital signatures and hashing techniques effectively prevented unauthorized access and data tampering. Additionally, the Role-Based Access Control (RBAC) mechanism ensured that only authorized users could access specific data, enhancing overall system security.

5.4 Storage and Overhead Analysis

The use of post-quantum cryptography introduced a slight increase in storage requirements due to larger key sizes and ciphertext expansion. However, this overhead was minimal when compared to the level of security achieved. Cloud storage capabilities efficiently handled the increased data size without affecting availability or performance.

5.5 Key Findings

- The proposed system provides quantum-resistant security, ensuring long-term protection of healthcare data.
- Data confidentiality and integrity are significantly improved through encryption and digital signatures.
- Access control mechanisms (RBAC) effectively restrict unauthorized data access.
- The system maintains acceptable performance despite increased computational overhead.
- Cloud integration ensures scalability, availability, and reliability for large-scale healthcare applications.

5.6 Summary

Overall, the results demonstrate that the proposed quantum-safe cloud storage framework is a secure and practical solution for protecting healthcare records. While there is a minor trade-off in terms of computational and storage overhead, the enhanced level of security and future readiness against quantum threats makes the system highly suitable for modern healthcare environments.

VI. DISCUSSION

6.1 Interpretation of Results

The results obtained from the implementation demonstrate that integrating post-quantum cryptographic techniques into cloud storage significantly enhances the security of healthcare data. While there is a noticeable increase in encryption and decryption time compared to traditional algorithms, the trade-off is justified by the system's ability to resist both classical and quantum-based attacks. The use of lattice-based cryptography ensures long-term confidentiality of sensitive medical records, addressing one of the most critical challenges in modern healthcare data management.

6.2 Comparison with Existing Systems

Compared to conventional cloud security systems that rely on RSA and ECC, the proposed model offers superior resistance to future threats posed by quantum computing. Existing systems primarily focus on current security needs and often neglect long-term risks. In contrast, the proposed framework adopts a forward-looking approach by incorporating quantum-safe algorithms. Additionally, the inclusion of Role-

Based Access Control (RBAC) provides more structured and fine-grained access management, which is often limited or inefficient in traditional systems.

6.3 Practical Implications

The proposed system has strong practical relevance in real-world healthcare environments, where data privacy and security are of utmost importance. Hospitals, clinics, and healthcare providers can adopt this framework to securely store and share patient records without compromising confidentiality. The system also aligns with the growing need for secure digital healthcare infrastructure, especially with the increasing use of telemedicine and remote patient monitoring.

6.4 Limitations of the Study

Despite its advantages, the proposed system has certain limitations. The use of post-quantum cryptographic algorithms introduces higher computational overhead, which may affect performance in resource-constrained environments. Additionally, the implementation is tested in a simulated environment rather than a fully deployed real-world healthcare system. There may also be challenges related to integration with existing legacy systems and infrastructure.

6.5 Future Improvements

Future work can focus on optimizing the performance of post-quantum algorithms to reduce computational overhead. Integration with emerging technologies such as blockchain can further enhance data transparency and auditability. Additionally, implementing hybrid cryptographic models that combine classical and post-quantum techniques can provide a balanced approach during the transition phase toward quantum-safe systems. Expanding the system for real-time deployment and testing in large-scale healthcare environments would further validate its effectiveness.

6.6 Summary

In summary, the discussion highlights that the proposed quantum-safe cloud storage system provides a robust and future-ready solution for securing healthcare data. Although there are some performance and implementation challenges, the benefits of enhanced security, data integrity, and resistance to quantum threats make it a valuable advancement over traditional cloud security models.

VII. CONCLUSION

The increasing reliance on cloud computing in the healthcare sector has brought significant improvements in data accessibility, storage efficiency, and collaborative medical services; however, it has also introduced critical security and privacy challenges due to the sensitive nature of healthcare data. This research addressed these challenges by proposing a quantum-safe cloud storage framework specifically designed to protect electronic health records (EHRs) against both current cyber threats and future risks posed by quantum computing.

Traditional cryptographic techniques, while effective in today's computing environment, are fundamentally vulnerable to quantum-based attacks, making them unsuitable for long-term data protection. In response to this limitation, the proposed system integrates post-quantum cryptographic algorithms, including lattice-based encryption and quantum-resistant digital signature schemes, to ensure enhanced confidentiality, integrity, and authentication of healthcare data.

The implementation of the system demonstrates that it is possible to achieve a high level of security without compromising the practical usability of cloud-based healthcare applications. By incorporating advanced mechanisms such as secure key management, encrypted data storage, and Role-Based Access Control (RBAC), the framework ensures that only authorized users can access sensitive information while maintaining strict data protection policies.

Furthermore, the proposed framework is designed with scalability and adaptability in mind, allowing it to be integrated into existing cloud infrastructures with minimal disruption. Its modular architecture supports future enhancements and can accommodate evolving security requirements as quantum technologies continue to develop. The concept of "future-proofing" healthcare data is a key contribution of this work, ensuring that sensitive medical records remain protected not only today but also in the coming era of quantum computing.

In conclusion, this research presents a robust, efficient, and forward-looking solution for securing healthcare data in cloud environments. The adoption of quantum-safe cryptographic techniques, combined with strong access control and secure system design, provides a comprehensive approach to addressing both present and future security challenges. The proposed system lays a strong foundation for the development of next-generation secure healthcare infrastructures and highlights the importance of

transitioning towards quantum-resistant technologies to ensure long-term data protection and trust in digital healthcare systems.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.
[2] L. Chen et al., "Report on Post-Quantum Cryptography," National Institute of Standards and Technology (NIST), 2016.
[3] National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization," NIST, 2022.
[4] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography, Springer, 2009.
[5] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.
[6] J. Katz and Y. Lindell, Introduction to Modern Cryptography, CRC Press, 2014.
[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 1978.
[8] V. S. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology (CRYPTO), 1985.
[9] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of Computation, 1987.
[10] M. Ajtai, "Generating hard instances of lattice problems," Proceedings of the 28th ACM Symposium on Theory of Computing, 1996.
[11] C. Peikert, "A decade of lattice cryptography," Foundations and Trends in Theoretical Computer Science, 2016.
[12] R. C. Merkle, "A digital signature based on a conventional encryption function," Advances in Cryptology (CRYPTO), 1987.
[13] D. Micciancio and O. Regev, "Lattice-based cryptography," Post-Quantum Cryptography, Springer, 2009.
[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[15] A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control," IEEE Symposium on Security and Privacy, 2005.