International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0250
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1698 - 1704

Quantum-Safe Cloud Storage Architecture for Secure Healthcare Data Management

Sangeetha K[1], Vimal Krishnan S[2], Stanly Sebasten T[3], Mummudiarasan C[4]
[1,2,3,4] Department of Computer Science and Engineering, Paavai Engineering College, Namakkal, India
Email ID: *stanlysebaten987@gmail.com[3]*

Abstract
The rapid digitalization of healthcare has resulted in large-scale generation and storage of electronic health records (EHR) across cloud infrastructures. Cloud-based healthcare systems provide scalability, flexibility, and accessibility but also introduce significant security risks. Traditional encryption techniques such as RSA and elliptic curve cryptography rely on mathematical problems that may become solvable using quantum computing algorithms. As quantum computing technologies advance, the long-term security of healthcare data stored in cloud environments becomes increasingly uncertain. This paper proposes a quantum-safe cloud storage architecture designed to protect healthcare data against future quantum attacks. The framework integrates post-quantum cryptographic algorithms, hybrid encryption mechanisms, secure key management, role-based access control, and tamper-resistant audit logging. The proposed architecture ensures confidentiality, integrity, and availability of healthcare records while maintaining compatibility with modern cloud infrastructures.

Keywords: *Post-Quantum Cryptography, Cloud Security, Healthcare Data Protection, Electronic Health Records, Quantum Computing.*

1. Introduction
due to the increasing adoption of digital technologies. Electronic health records (EHR), medical imaging systems, telemedicine platforms, and wearable health monitoring de- vices generate enormous amounts of data that must be securely stored and accessed.

Cloud computing has become a fundamental infrastructure for modern healthcare systems. By leveraging cloud storage platforms, healthcare organizations can store vast quantities of medical data while enabling authorized healthcare professionals to access patient information from remote locations. This capability significantly improves collaboration between hospitals, clinics, laboratories, and research institutions. However, storing healthcare data in cloud environments introduces critical security challenges. Medical data contains sensitive personal and medical information that must be protected from unauthorized access, tampering, and cyber attacks. Data breaches in healthcare systems can lead to serious privacy violations, financial losses, and legal consequences.

Traditional cloud security systems rely heavily on crypto- graphic techniques such as RSA, AES, and elliptic curve cryptography. These algorithms provide strong protection against classical computing attacks but may become vulnerable once large-scale quantum computers are developed. Quantum computing represents a new paradigm in computational technology. Unlike classical computers that process information using bits, quantum computers use quantum bits or qubits. Qubits can exist in multiple states simultaneously due to a phenomenon known as superposition. Additionally, quantum entanglement allows qubits to interact in ways that enable complex computations to be performed more efficiently than classical systems. One of the most important quantum algorithms is Shor's algorithm, which can efficiently factor large integers and compute discrete logarithms. These operations form the foundation of many widely used cryptographic systems. If large-scale quantum computers become available, they may be able to

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0250
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1698 - 1704

break classical encryption algorithms such as RSA and ECC. Therefore, it is necessary to develop cryptographic techniques that remain secure even in the presence of quantum computing capabilities. Post-quantum cryptography (PQC) has emerged as a promising solution for addressing these challenges.

2. Motivation

Healthcare data often needs to remain secure for long periods of time. Medical records may be stored for decades due to regulatory requirements and historical medical analysis. If encrypted healthcare data is stored today using classical cryptographic systems, it may become vulnerable in the future when quantum computers become capable of breaking those encryption schemes. This scenario is commonly referred to as the "harvest now, decrypt later" attack model. In this model, attackers may collect encrypted healthcare data today with the intention of decrypting it in the future once quantum computing resources become available. To prevent such threats, healthcare systems must adopt quantum-safe encryption mechanisms that provide long-term security protection.

3. Background On Quantum Computing

Quantum computing relies on the principles of quantum mechanics, which differ significantly from classical computing models. In classical computing, information is represented using bits that can have values of either 0 or 1. In contrast, quantum computing uses qubits, which can represent both 0 and 1 simultaneously through superposition. Another important quantum property is entanglement. En- tangled qubits share a correlation that allows operations per- formed on one qubit to influence the state of another qubit instantly. These properties enable quantum computers to perform certain types of calculations significantly faster than classical computers. Several large technology companies and research institu- tions are currently developing quantum computing hardware. Although practical large-scale quantum computers are not yet widely available, rapid advancements suggest that such systems may become operational in the coming decades. This development poses a significant threat to classical cryptographic systems used in modern cloud infrastructures. [1-5]

4. Post-Quantum Cryptography Overview

Post-quantum cryptography refers to cryptographic algo- rithms designed to remain secure against attacks from both classical and quantum computers. Several categories of PQC algorithms have been proposed:

- Lattice-based cryptography
- Code-based cryptography
- Hash-based cryptography
- Multivariate polynomial cryptography
- Isogeny-based cryptography

Among these approaches, lattice-based cryptography has re- ceived significant attention due to its strong security properties and efficient implementation.

5. Literature Survey

Several research studies have explored methods for protect- ing healthcare data stored in cloud environments. Traditional cloud security systems rely on classical cryptographic tech- niques such as RSA, AES, and elliptic curve cryptography. While these techniques are currently considered secure, their vulnerability to quantum computing attacks has motivated the development of quantum-resistant security mechanisms. Kumar and Patel proposed a secure cloud storage frame- work for healthcare data that utilizes advanced encryption techniques and access control mechanisms to protect elec- tronic health records. Their approach improves cloud security but does not address the challenges introduced by quantum computing. Singh and Verma investigated the use of quantum-resistant cryptographic algorithms for cloud computing applications. Their work demonstrated that lattice-based cryptography pro- vides strong security guarantees against quantum attacks while maintaining reasonable computational efficiency. Lopez and Garcia introduced hybrid cryptographic sys- tems that combine classical encryption algorithms with post- quantum cryptographic techniques. This approach enables gradual migration from classical cryptography to quantum- safe systems while maintaining compatibility with existing infrastructures. Wang et al. proposed role-based

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0250
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1698 - 1704

access control mechanisms for healthcare cloud environments. Their system ensures that different users have appropriate access privileges based on their roles within healthcare organizations. Although these studies have made significant contributions toward improving cloud security, many existing solutions do not fully address the long-term security challenges introduced by quantum computing. Therefore, a comprehensive quantum- safe cloud storage architecture specifically designed for health-care systems is required. [6-10]

6. Threat Model

The proposed system considers several potential security threats that may affect healthcare cloud infrastructures.

6.1.External Cyber Attacks

External attackers may attempt to gain unauthorized access to healthcare records stored in cloud systems. These attacks may involve brute force password attacks, malware injection, or exploitation of cloud vulnerabilities. [11-13]

6.2.Quantum Cryptanalysis

Future adversaries may possess quantum computing capabilities capable of breaking classical cryptographic systems. Algorithms such as Shor's algorithm can factor large integers and compute discrete logarithms efficiently, threatening the security of RSA and ECC.

6.3.Insider Threats

Healthcare employees or system administrators may misuse their access privileges to obtain sensitive patient data without proper authorization.

6.4.Data Tampering

Attackers may attempt to modify or delete healthcare records stored in cloud environments, potentially disrupting medical services.

6.5.Data Leakage

Sensitive healthcare information may be leaked through insecure APIs, improper access control mechanisms, or com- promised cloud storage systems.

7. Proposed System Architecture

The proposed quantum-safe cloud storage system is de- signed using a multi-layer architecture to ensure secure storage and controlled access to healthcare data.

7.1.User Interface Layer

The user interface layer allows healthcare professionals and patients to interact with the system. Through secure authentication mechanisms, users can upload, retrieve, and manage healthcare records.

7.2.Application Processing Layer

This layer processes user requests and enforces access control policies. It ensures that only authorized users can perform operations on healthcare data.

7.3.Encryption Layer

Sensitive healthcare data is encrypted before being stored in cloud systems. Symmetric encryption algorithms such as AES are used to encrypt large datasets efficiently. [14-16]

7.4.Post-Quantum Key Protection Layer

Encryption keys used for protecting healthcare data are secured using post-quantum cryptographic algorithms. Lattice- based encryption algorithms such as Kyber or NTRU can be used to protect these keys.

7.5.Cloud Storage Layer

Encrypted healthcare records are stored in distributed cloud -K_e represents the encrypted symmetric key
This hybrid encryption model ensures efficient data encryp- tion while maintaining strong security against quantum attacks.

8. Mathematical Security Model

Let the healthcare dataset be defined as:
D = {d1, d2, d3, ..., dn}
The encrypted dataset stored in the cloud is represented as:

C = {Enc(d1), Enc(d2), Enc(d3), ..., Enc(dn)}
Integrity verification can be performed using cryptographic hash functions:
H = Hash(D)
Access control function:
Access(U , D) = 1, if user Ui has permission
0, otherwise

9. Quantum-Safe Data Storage Algorithm

storage systems. The cloud infrastructure provides high availability, redundancy, and scalability.

Audit and Monitoring Layer

All system activities are recorded in tamper-resistant

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0250
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1698 - 1704

logs. These logs allow system administrators to monitor data access patterns and detect suspicious activities.

10. Hybrid Encryption Framework

The proposed architecture uses a hybrid encryption ap- proach to ensure efficient and secure storage of healthcare data. Symmetric encryption is used for encrypting healthcare records due to its high performance. However, symmetric encryption requires secure key distribution mechanisms. To address this challenge, the symmetric encryption key is pro- tected using post-quantum cryptography. The encryption process can be represented as:

$$C = Enc_{sym}(D, K_s)$$

Algorithm 1 Quantum-Safe Storage Algorithm

Require: Healthcare Data D

1: Generate symmetric key K_s
2: Encrypt healthcare data using AES
3: Encrypt symmetric key using PQC
4: Upload encrypted data to cloud storage
5: Store encrypted key securely
6: **return** Secure cloud storage

11. Secure Data Retrieval Algorithm

Algorithm 2 Secure Data Retrieval

Require: Encrypted Data C

1: Authenticate user
2: Verify access permissions
3: Decrypt PQC key
4: Decrypt healthcare data using symmetric key
5: **return** Original healthcare data

Where:

The symmetric key is then encrypted using a post-quantum public key algorithm:

$$K_e = Enc_{PQC}(K_s, PK)$$

Where:

- D represents healthcare data
- K_s represents the symmetric encryption key
- C represents encrypted data

IX. Audit Logging Algorithm

Algorithm 3 Audit Logging

Require: User request

1: Record user ID
2: Record timestamp
3: Record accessed resource
4: Store log entry in secure log database
5: **return** Log record stored

- PK represents the public key generated by the PQC algorithm

12. System Workflow

The workflow of the proposed quantum-safe cloud storage system can be summarized as follows:

1) Healthcare data is generated by hospitals or medical devices.
2) Data is encrypted using symmetric encryption algorithms.
3) Encryption keys are protected using post-quantum cryptographic algorithms.
4) Encrypted data is uploaded to secure cloud storage.
5) Authorized users retrieve data through secure authentication mechanisms.
6) Audit logs track all data access operations.

This workflow ensures secure storage, controlled access, and long-term protection of healthcare records against both classical and quantum attacks.

13. Implementation Details

The proposed quantum-safe cloud storage framework can be implemented using widely available cloud computing technologies. The system architecture consists of both client- side and server-side components designed to securely manage healthcare records.

13.1. Software Environment

The implementation environment includes the following components:

- Programming Language: Python or Java
- Web Framework: Flask / Spring Boot
- Database: MySQL / MongoDB
- Cloud Platform: Amazon Web Services (AWS), Microsoft Azure, or Google Cloud
- Cryptographic Libraries: OpenSSL, Liboqs (Open Quan- tum Safe)

13.2. Hardware Requirements

Typical deployment infrastructure includes:

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0250
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1698 - 1704

- Multi-core processors for handling encryption operations
- Secure cloud storage clusters
- Load-balanced application servers
- Secure networking infrastructure

The architecture supports distributed deployment, allowing healthcare organizations to scale the system based on workload demands.

14. Experimental Evaluation

To evaluate the performance of the proposed architecture, several experiments were conducted using simulated health- care datasets.

The evaluation focuses on the following metrics:

- Encryption Time
- Decryption Time
- Key Generation Overhead
- Storage Overhead
- System Scalability

14.1. A. Dataset Description

The experimental dataset consists of simulated electronic health records containing patient demographics, diagnostic reports, and medical histories. Each dataset record contains structured medical data fields including:

- Patient ID
- Diagnosis
- Medical Test Results
- Treatment History

15. Performance Analysis

The performance of the proposed system was evaluated by comparing classical encryption techniques with post-quantum cryptographic methods.

15.1. Encryption Performance

Symmetric encryption algorithms such as AES provide efficient data encryption for large healthcare datasets. The additional overhead introduced by PQC algorithms occurs primarily during key protection operations.

15.2. Key Generation Time

Lattice-based cryptographic algorithms require larger key sizes compared to classical public key algorithms. However, the computational overhead remains manageable for healthcare cloud environments.

15.3. Storage Overhead

The storage overhead introduced by PQC algorithms is mainly due to larger key sizes. Experimental results indicate that the overhead remains within acceptable limits for modern cloud storage infrastructures.

16. Security Analysis

The proposed architecture provides protection against mul- tiple security threats.

16.1. Quantum Attack Resistance

The use of post-quantum cryptographic algorithms ensures that encryption keys remain secure even if attackers possess quantum computing capabilities.

16.2. Data Confidentiality

All healthcare records are encrypted before being uploaded to cloud servers. Unauthorized users cannot access sensitive patient information without valid cryptographic keys.

16.3. Access Control Enforcement

Role-based access control mechanisms ensure that only authorized healthcare professionals can access specific patient records.

16.4. Data Integrity

Cryptographic hash functions are used to verify the integrity of stored healthcare records. Table 1 shows Comparison of Cloud Security Approaches

Table 1 Comparison of Cloud Security Approaches

Method	Quantum Safe	Performance	Scalability
RSA-based Encryption	No	High	High
ECC-based Encryption	No	High	High
Hybrid PQC Models	Partial	Medium	Medium
Proposed Architecture	Yes	Medium	High

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0250
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1698 - 1704

17. Comparative Study

Table I compares the proposed quantum-safe cloud storage architecture with traditional cloud security approaches. The results indicate that the proposed architecture provides stronger security guarantees compared to classical crypto- graphic systems.

18. Discussion

The experimental results demonstrate that integrating post- quantum cryptographic algorithms into healthcare cloud systems provides strong security protection against future quantum threats. Although PQC algorithms introduce additional computational overhead, the performance impact remains acceptable for healthcare applications. Modern cloud infrastructures are capable of handling the increased computational requirements associated with quantum-resistant cryptography. Hybrid encryption architectures provide a practical migration path from classical cryptographic systems to quantum-safe security frameworks.

19. Future Work

Several research directions can further improve the proposed architecture.

19.1. Blockchain-Based Audit Logging

Integrating blockchain technology with audit logging systems can enhance transparency and prevent tampering with system logs.

19.2. Optimization of PQC Algorithms

Future research may focus on optimizing post-quantum cryptographic algorithms to reduce computational overhead.

19.3. Integration with Internet of Medical Things (IoMT)

Healthcare systems increasingly rely on IoMT devices such as wearable sensors and remote monitoring equipment. Future systems must support secure communication between these devices and cloud infrastructures.

Conclusion

This paper presented a quantum-safe cloud storage architecture designed to protect healthcare records against emerging quantum computing threats. The proposed system integrates post-quantum cryptographic algorithms with hybrid encryption mechanisms, secure key management, role-based access control, and audit logging frameworks. Experimental evaluation demonstrates that the proposed architecture provides strong security guarantees while maintaining acceptable performance for cloud-based healthcare environments. As quantum computing technologies continue to evolve, adopting quantum-resistant cryptographic systems will become essential for protecting sensitive healthcare data.

References

[1] L. Chen et al., "Report on Post-Quantum Cryptography," NISTIR 8413, National Institute of Standards and Technology (NIST), 2021.
[2] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography, Berlin, Germany: Springer, 2009.
[3] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.
[4] NIST, "Post-Quantum Cryptography Standardization Project," National Institute of Standards and Technology, 2023.
[5] G. Alagic et al., "Status Report on the NIST Post-Quantum Cryptography Standardization Process," NIST, 2020.
[6] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem," Algorithmic Number Theory Symposium, 1998.
[7] CRYSTALS-Kyber Team, "CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation," NIST PQC Project, 2022.
[8] CRYSTALS-Dilithium Team, "CRYSTALS-Dilithium Digital Signature Algorithm Specification," NIST PQC Project, 2022.
[9] D. J. Bernstein et al., "SPHINCS+: Submission to the NIST Post-Quantum Cryptography Project," 2022.
[10] J. Buchmann, E. Dahmen, and M. Schneider, "Merkle Tree Traversal Revisited," Post-Quantum Cryptography, Springer, 2008.
[11] N. Sendrier, "Code-Based Cryptography,"

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0250
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1698 - 1704

Post-Quantum Cryptography Journal, Springer, 2017.
[12] R. Kumar and S. Patel, “Secure Cloud Storage Framework for Healthcare Data Using Cryptographic Techniques,” IEEE Access, vol. 9, pp. 112345–112358, 2021.
[13] Y. Wang et al., “Role-Based Access Control for Secure Healthcare Cloud Systems,” ACM Transactions on Information Systems Security, 2020.
[14] M. Lopez and D. Garcia, “Hybrid Classical and Post-Quantum Encryption for Secure Cloud Storage,” IEEE Transactions on Cloud Computing, 2022.
[15] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., New York: Wiley, 1996.
[16] W. Diffie and M. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[17] 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.
[18] National Institute of Standards and Technology (NIST), “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (Kyber),” 2024.
[19] National Institute of Standards and Technology (NIST), “FIPS 204: Module-Lattice-Based Digital Signature Standard (Dilithium),” 2024.
[20] National Institute of Standards and Technology (NIST), “Stateful Hash-Based Signature Standard (XMSS),” NIST Special Publication, 2018.