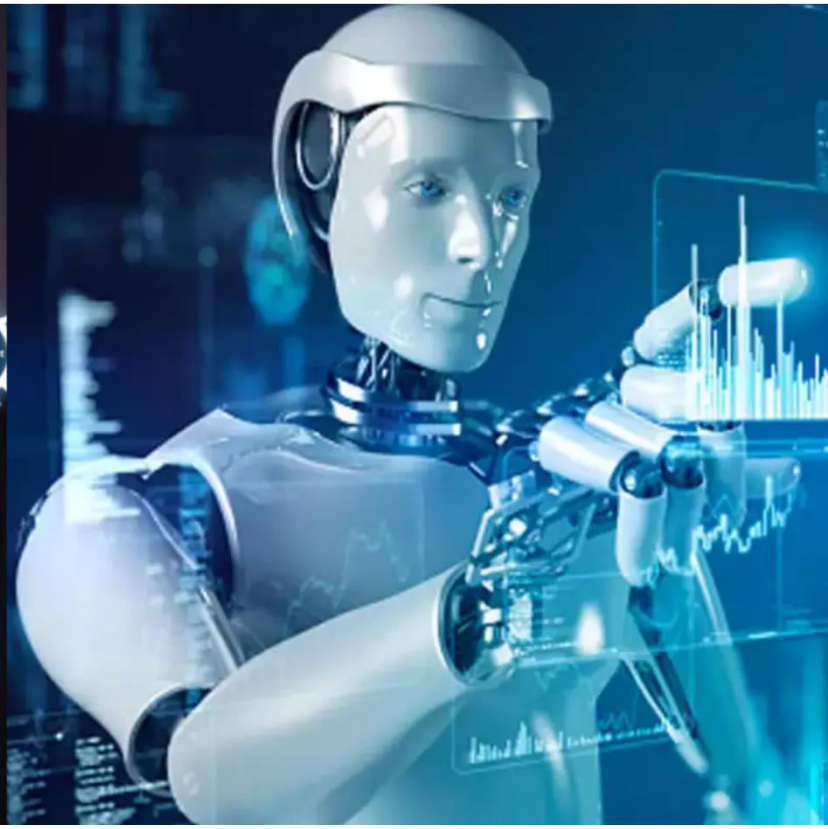
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503291|

Block chain-Enabled Privacy Preserving Cloud Data Auditing

Arulpandi.D[1], Parvaz.I[2], Shanmugasundaram.R[3], Vishwa.M[4], Elamathi.S[5]

Department of CSE, Sir Issac Newton College of Engineering and Technology, Pappakovil, Nagapattinam, India.[1-4]

Assistant Professor, Department of CSE, Sir Issac Newton College of Engineering and Technology, Pappakovil, Nagapattinam, India[5]

ABSTRACT: Cloud computing has become a fundamental technology for storing and managing large-scale data; however, it introduces critical challenges related to data security, privacy, and integrity. This paper presents a Blockchain-enabled privacy-preserving cloud data auditing system designed to ensure secure and reliable data management in cloud environments. The proposed system eliminates dependency on third-party auditors by leveraging decentralized blockchain technology to maintain tamper-proof audit records.

To enhance data security, the system integrates Post-quantum cryptographic (PQC) techniques, which provide resistance against both classical and quantum computing attacks. Additionally, Adaptive machine learning algorithms are incorporated to detect anomalies and potential threats in real time, improving overall system security. The framework supports efficient data auditing without exposing sensitive information, thereby preserving user privacy.

Furthermore, the system employs cryptographic hash functions and Merkle Hash Trees to verify data integrity, while blockchain ensures transparency, accountability, and traceability of all operations. The proposed architecture also supports dynamic data operations such as insertion, deletion, and modification with minimal overhead. Overall, the system provides a scalable, secure, and future-proof solution for cloud data storage and auditing by combining blockchain, quantum-resistant encryption, and intelligent threat detection mechanisms.

I. INTRODUCTION

Cloud computing has emerged as a revolutionary technology that enables users to store, manage, and process data over the internet rather than relying on local storage systems. It offers on-demand services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), providing high scalability, flexibility, and cost efficiency. Due to these advantages, cloud computing is widely adopted across various domains including education, healthcare, business, and government sectors.

Despite its numerous benefits, cloud computing introduces significant security challenges. Since data is stored on remote servers managed by cloud service providers, users lose direct control over their data. This raises serious concerns regarding data confidentiality, integrity, and unauthorized access. Traditional cloud auditing mechanisms often rely on third-party auditors (TPAs) to verify data integrity, which can lead to privacy leakage and increased system complexity.

To address these limitations, advanced technologies such as cryptographic techniques, blockchain, and machine learning have been introduced. Blockchain technology provides decentralized and tamper-proof record keeping, ensuring transparency and eliminating dependence on centralized auditors. Cryptographic methods, particularly post-quantum cryptography, enhance data security by protecting against future quantum-based attacks. Additionally, machine learning techniques enable real-time threat detection by analyzing user behavior and identifying anomalies.
In this paper, we propose a secure and privacy-preserving cloud data auditing system that integrates blockchain, post-quantum cryptography, and adaptive machine learning. The system ensures data integrity without exposing sensitive information, supports dynamic data operations, and enhances overall security and reliability. By combining these advanced technologies, the proposed framework provides a robust, scalable, and future-proof solution for secure cloud data management.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503291|

II. IMPORTANCE OF CLOUD DATA SECURITY AND AUDITING

Cloud data security and auditing play a crucial role in ensuring the reliability and trustworthiness of modern cloud computing systems. As organizations increasingly store sensitive and large-scale data on remote cloud servers, they face significant risks such as unauthorized access, data breaches, and data tampering. Without proper security measures, users lose control over their data, making it essential to implement strong protection mechanisms. Cloud data auditing provides a systematic approach to verify the integrity and correctness of stored data without requiring full data retrieval. It enhances transparency by allowing users to ensure that their data remains intact and unaltered. Moreover, privacy-preserving auditing techniques protect sensitive information during the verification process, preventing data exposure to external entities. By incorporating advanced technologies such as encryption, blockchain, and intelligent threat detection, cloud data security and auditing not only safeguard user data but also build trust between users and cloud service providers, making them essential components of secure and efficient cloud environments.

III. ROLE OF MACHINE LEARNING AND BLOCKCHAIN IN CLOUD SECURITY

Machine learning and blockchain technologies play a vital role in enhancing security within modern cloud computing environments. Machine learning algorithms enable the system to analyze large volumes of data and identify unusual patterns, user behaviors, and potential security threats in real time. By continuously learning from past data and evolving attack patterns, these models improve the accuracy of threat detection and help in preventing cyberattacks such as unauthorized access, data breaches, and insider threats.

On the other hand, blockchain technology provides a decentralized and tamper-proof framework for maintaining records of data transactions and auditing activities. Each transaction is securely recorded in a distributed ledger using cryptographic techniques, ensuring transparency, immutability, and accountability. This eliminates the need for centralized third-party auditors and reduces the risk of data manipulation.

IV. NEED FOR AN INTEGRATED SECURE CLOUD AUDITING SYSTEM

The rapid growth of cloud computing has increased the demand for a comprehensive and secure framework that can address multiple challenges associated with data storage, sharing, and auditing. Traditional cloud systems often rely on separate mechanisms for security, auditing, and threat detection, which can lead to inefficiencies, increased complexity, and potential vulnerabilities. Moreover, dependence on third-party auditors raises concerns about data privacy and trust, as sensitive information may be exposed during the auditing process.

V. EXISTING SYSTEM

In traditional cloud storage environments, users outsource their data to third-party cloud service providers to reduce local storage and maintenance costs. However, once the data is uploaded, users lose direct control over it. To ensure data integrity, most existing auditing mechanisms rely on ThirdParty Auditors (TPAs) who periodically verify the correctness of the stored data.

While these methods improve trust in cloud storage, they suffer from several limitations. Many existing systems perform auditing in a non privacy-preserving manner, where the auditor must access or partially view user data during verification. This creates a potential risk of data leakage, especially when sensitive or confidential information is involved. Moreover, most systems fail to protect data shared among multiple users, lacking secure key management and proper access control mechanisms for group environments.

VI. DISADVANTAGES

- Lack of Privacy Preservation
- No Secure Sharing Mechanism
- High Computational Overhead
- Weak Support for Dynamic Data

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

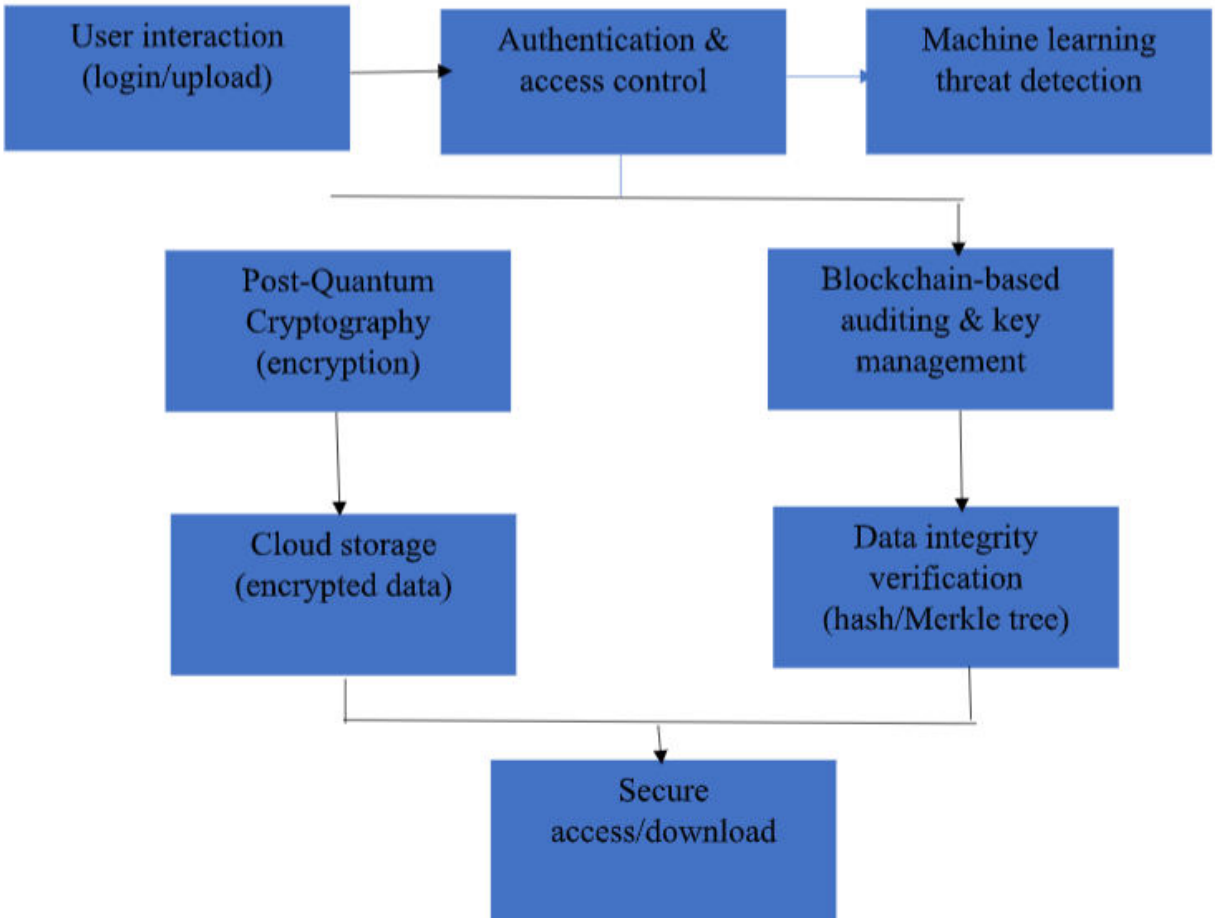
Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503291|

VII. SYSTEM ARCHITECTURE

The proposed system architecture is designed to provide a secure and privacy-preserving cloud data storage and auditing environment. The process begins with user registration and login, where users authenticate themselves through the user authentication and access control module. This module verifies the identity of users and ensures that only authorized individuals can access the cloud system. It also manages user roles and permissions, providing controlled access to data and system resources. After successful authentication, users can upload or share their data in the cloud storage system. Before the data is stored, it is protected using PostQuantum Cryptography (PQC) encryption techniques.

SYSTEM ARCHITECTURE



VIII. TESTING

System testing plays a vital role in evaluating the performance, reliability, and security of the proposed cloud data auditing system. It ensures that all modules, including authentication, encryption, blockchain auditing, machine learning threat detection, and data integrity verification, function correctly and meet the specified requirements. The primary objective of testing is to identify errors, verify system functionality, and ensure that the system operates efficiently under various conditions.

Testing is conducted at multiple levels to ensure comprehensive validation. Unit testing is performed on individual modules such as encryption and authentication to verify their correctness. Integration testing ensures that different

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503291|

components of the system work together seamlessly, especially the interaction between blockchain, cloud storage, and machine learning modules. System testing evaluates the complete system as a whole to confirm that it meets performance and security standards. Additionally, security testing is carried out to detect vulnerabilities and ensure protection against unauthorized access and cyber threats.

Performance testing is also conducted to analyze system behavior under different workloads, ensuring scalability and efficiency in handling large volumes of cloud data. By implementing thorough testing strategies, the proposed system guarantees reliability, accuracy, and robustness, making it suitable for real-world cloud computing environments.

IX. TYPES OF TESTING

The proposed cloud data auditing system undergoes various types of testing to ensure its functionality, performance, security, and reliability. Each type of testing focuses on a specific aspect of the system to identify errors and improve overall system quality. These testing methods help ensure that all modules work correctly both individually and as an integrated system.

- Unit Test
- Functional Test
- Integration Test
- Security Testing
- System Test
- Performance test
- Acceptance Test

X. SYSTEM IMPLEMENTATION

SYSTEM MODULE

- User Authentication and Access Control Module
- Post-Quantum Cryptography (PQC) Encryption Module
- Data Storage and Sharing Module
- Blockchain-Based Auditing and Key Management Module
- Adaptive Machine Learning Threat Detection Module
- Data Integrity Verification Module

XI. CONCLUSION

The proposed system presents a comprehensive and robust framework for secure cloud data management while ensuring strong privacy preservation. By effectively integrating post-quantum cryptography, blockchain technology, and adaptive machine learning-based threat detection, the system addresses critical security requirements in modern cloud environments. It guarantees confidentiality encrypting user data with quantum-resistant algorithms, safeguarding it against both current and future cyber threats. Data integrity is maintained through blockchain-based auditing and hash verification mechanisms, ensuring that any unauthorized modification is immediately detectable.

Additionally, the system ensures accountability by immutably recording all transactions, data uploads, and access activities on the blockchain, thereby providing complete traceability and transparency. Real-time security is further enhanced through adaptive machine learning techniques that continuously monitor system behavior and promptly detect potential threats. Overall, the system offers a reliable and efficient solution for secure cloud storage, enabling protected data sharing and access for authorized users while maintaining high standards of security, transparency, and performance.

REFERENCES

[1]. B. Wang, B. Li and H. Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,” IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 43–56, 2014.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503291|

[2] Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013

[3]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable Data Possession at Untrusted Stores," Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–609.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), 2008, pp. 90–107.

[5] K. Ren, C. Wang and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[6]. Kevin Yang et al., "Blockchain-Based Public Auditing for Cloud Storage," 2018.

[7]. Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details