
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

AUDITING SCHEMA FOR SECURE DATA STORAGE IN CLOUD

[1] P. Swetha, A [2] Hari Chandan Reddy, [3] G. Raghava, [4] G. Mounika, [5] B. Sai Krishna

[1]Assistant Professor Department of CSE (DS) TKR College of Engineering & Technology

[1] pswetha@tkrcet.com

[2,3,4 5] B.Tech (Scholar) Department of CSE (DS) TKR College of Engineering & Technology

[2] harichandanreddyalurri@gmail.com ,[3] gollapanilraghava4@gmail.com , [4] ajjemounika91@gmail.com , [5] saikrishna3965@gmail.com

ABSTRACT

Secure data storage and integrity are important challenges during cloud computing. This work describes a strong auditing scheme for secure data storage in the cloud with efficient and reliable integrity checking methods. This schema uses both cryptographic technology and thirdparty audit data stored to ensure that confidentiality, authenticity & availability are fully satisfied serving as a form of protection. It has four main modules, including a Sender module to encrypt data securely, a Feature module for integrity proofs, and a Receiver module to verify it together with the Key Generation Centre (KGC) to manage keys securely. This method can protect against new threats such as unauthorized access and data leaks, so that sensitive data is well protected even in destructive environments. Along with a Contact Us module for real-time support, it also allows robust transparency and trust by facilitating direct communication between users and the cloud service provider. It provides a schema that is scalable, lightweight and high-performance oriented to the needs of modern cloud environments

KEYWORDS: Internet of Things(IOT), Cloud Computing (CC), Data Integrity, Data Auditing.

1.INTRODUCTION

The cloud computing paradigm has gained substantial attention in recent years, offering numerous advantages such as scalability, flexibility, and cost-effectiveness. As a result, the use of cloud services for storing sensitive data has seen rapid growth across various industries, including healthcare, finance, and government. However, while the cloud provides numerous benefits, it also introduces significant security and privacy concerns. The potential risks associated with storing sensitive data in the cloud include unauthorized access, data breaches, and loss of control over the data. To address these concerns, it is crucial to have a robust and efficient auditing schema for secure data storage in the cloud. This schema should ensure that data stored in the cloud is secure and can be tracked, monitored, and validated

for integrity, confidentiality, and availability. An effective auditing framework would allow organizations to ensure compliance with security policies, detect potential security breaches, and guarantee the protection of sensitive data from unauthorized access.

Auditing plays a vital role in the overall security architecture of cloud storage systems. It involves the systematic examination and evaluation of data storage activities, including data access, modification, and deletion, to detect and investigate any suspicious or malicious behavior. Auditing can provide transparency into the security status of the data and can be used to monitor cloud providers, enforce security policies, and maintain regulatory compliance. The need for comprehensive auditing mechanisms has been further emphasized by regulatory frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), which require organizations to maintain detailed audit logs for sensitive data stored in the cloud.

This paper presents an overview of the auditing schema for secure data storage in the cloud, focusing on methodologies, proposed systems, and best practices. We discuss existing literature on the topic, outline a methodology for developing an effective auditing system, and propose a novel system designed to enhance data security in the cloud. The paper concludes by presenting the implementation details of the proposed system and evaluating its effectiveness in securing cloud storage.

2.RELATED WORK

The idea of auditing in cloud environments has been explored in various studies, particularly concerning the challenges of ensuring security and privacy for cloud-based data storage. Several approaches have been proposed to establish auditing mechanisms that provide security guarantees for cloud storage systems. One of the primary goals of cloud data auditing is to ensure the confidentiality, integrity, and availability of data while maintaining transparency and accountability for both cloud providers and clients.

In recent years, several research efforts have focused on access control and auditing for secure data storage in the cloud. The authors in [1] proposed a framework for cloud data auditing that combines cryptographic techniques and attribute-based access control to ensure data security. Their model uses public-key cryptography for data encryption and digital signatures to verify the integrity of data stored in the cloud. Similarly, [2] proposed an auditing model based on the combination of homomorphic encryption and secure hash functions to ensure data integrity and confidentiality during cloud storage. Their system allows cloud service providers to audit user activities without exposing sensitive information.

In a different approach, [3] introduced the concept of lightweight auditing in cloud storage using secure audit logs that track all activities related to data storage and retrieval. Their model employs a secure timestamping mechanism that ensures the

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

accuracy and consistency of the audit logs, thereby preventing data tampering or unauthorized modifications. Furthermore, the research conducted by [4] explored the role of blockchain technology in improving auditing in cloud storage. The study suggests that blockchain's decentralized nature can enhance data security and auditability by providing a transparent, immutable ledger of all transactions related to data access and modifications.

Several authors have also emphasized the importance of compliance with regulations and industry standards in cloud auditing. [5] highlighted the significance of regulatory frameworks such as HIPAA and GDPR in shaping cloud auditing requirements. Their research focuses on how cloud providers can meet the stringent demands of these regulations by implementing auditing mechanisms that allow for continuous monitoring and reporting of data activities. Moreover, [6] reviewed various auditing techniques in the cloud and identified the challenges in implementing effective auditing systems, including scalability, performance overhead, and privacy concerns.

Despite the significant contributions in the field of cloud data auditing, there are still challenges that need to be addressed. Some of the existing systems rely heavily on centralized logging and monitoring, which could introduce single points of failure or be susceptible to insider threats. Additionally, the need for real-time auditing to detect malicious activities has not been fully realized in many systems. Therefore, there is a growing demand for novel auditing schemas that address these challenges while providing a high level of security and privacy for cloud-based data storage.

3.LITERATURE SURVEY

The concept of cloud computing and the storage of sensitive data in the cloud has been a subject of intense research, particularly focusing on security and privacy. The emergence of cloud computing services has led to the centralization of data, enabling users to store and access data remotely. However, cloud storage introduces several security risks, such as unauthorized access, data breaches, data loss, and compromised integrity. This has led researchers to develop auditing schemas and mechanisms to enhance security and ensure that cloud providers and users follow best practices for data storage and access.

Authors like [7] emphasized the importance of auditing mechanisms in cloud storage for detecting potential attacks and ensuring compliance with data protection regulations. Their approach was based on continuous monitoring of cloud storage activities and generating audit logs that could later be used to trace malicious actions or data manipulations. The research by [8] further examined the role of auditing for verifying compliance with security policies in cloud storage systems. They proposed an approach for maintaining a secure audit trail that could be used to verify whether data was accessed, altered, or deleted in accordance with pre-defined security policies.

In terms of data integrity, [9] proposed a method based on cloud-based integrity verification schemes that leverage hashing

algorithms to ensure data consistency over time. They emphasized that auditing should not only focus on tracking access but also on confirming the integrity of stored data. Their proposed system used cryptographic techniques like Merkle hash trees to ensure that data modifications could be detected during auditing. Similarly, [10] introduced an approach using blockchain for securing audit trails and preventing unauthorized data modifications in cloud environments. By using a distributed ledger, blockchain ensures that all data access and modification records are securely stored and cannot be altered retroactively.

The need for privacy-preserving auditing systems has also been explored by several researchers. [11] proposed an auditing framework based on advanced cryptographic methods that protect sensitive information during the auditing process. Their system ensures that the cloud provider can audit the data without accessing the underlying sensitive content. The authors in [12] developed a solution for secure auditing using attribute-based encryption, which allows users to maintain control over their data while still enabling effective auditing by the cloud provider.

4.METHODOLOGY

To design an efficient auditing schema for secure data storage in the cloud, it is essential to adopt a systematic approach that incorporates several key components: data encryption, access control, auditing mechanisms, and reporting. The methodology can be broken down into the following steps:

1. Data Encryption: The first step involves encrypting sensitive data before it is uploaded to the cloud storage. This ensures that even if unauthorized individuals gain access to the storage, they will not be able to read or modify the data. Techniques such as symmetric and asymmetric encryption can be used to achieve this, depending on the specific requirements.

2. Access Control: Access to cloud-stored data should be regulated through access control policies, which determine who can access the data, under what conditions, and for what purposes. Role-based access control (RBAC) or attribute-based access control (ABAC) can be employed to ensure that only authorized users or applications can perform specific actions on the data.

3. Auditing Mechanism: An effective auditing system must track all actions related to data storage, including access, modification, deletion, and sharing of data. Audit logs should be created for every action performed on the data and should include information such as the identity of the user, the time of the action, and the nature of the activity.

4. Reporting and Alerts: The audit logs should be periodically analyzed to identify suspicious activities. Automated reporting and alert systems should be implemented to notify administrators of any potential security breaches or policy violations.

By implementing these components, organizations can ensure that their data

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

stored in the cloud remains secure and compliant with relevant regulations.

Proposed System

The proposed system for secure data storage auditing in the cloud leverages advanced encryption techniques, access control policies, and an auditing framework to ensure the confidentiality, integrity, and availability of data. The system incorporates a hybrid encryption scheme combining symmetric encryption for data confidentiality and asymmetric encryption for secure key management. This ensures that the data remains protected while minimizing the performance overhead.

The access control layer is built on an attribute-based access control model, where users are granted access to data based on specific attributes such as role, location, and time of access. The system also integrates a distributed auditing mechanism that ensures a real-time record of all data-related activities. The distributed ledger, built on blockchain technology, provides an immutable audit trail that can be accessed and verified by authorized parties.

5.IMPLEMENTATION

The implementation of the proposed system involves several stages. Initially, a cloud storage environment is set up with data encryption and access control layers. The encryption algorithm is implemented using standard libraries such as OpenSSL, while access control is managed using an attribute-based access control system. The audit logging mechanism is built using a secure logging framework that captures all activities related to data storage and retrieval. Blockchain technology is integrated into the system to ensure the immutability of the audit logs.

Once the system is implemented, the effectiveness of the auditing schema is evaluated based on its ability to detect unauthorized access, maintain data integrity, and ensure compliance with regulatory standards. Performance tests are conducted to evaluate the overhead introduced by the auditing mechanism, and the results are compared with traditional systems to assess the trade-off between security and performance.

6.RESULTS AND DISCUSSION

The implementation of the proposed system was successful in providing a secure and transparent auditing framework for cloud data storage. The encryption mechanisms ensured that sensitive data remained confidential, and the access control policies prevented unauthorized access. The distributed auditing framework provided real-time monitoring of data activities, and the blockchain-based audit trail ensured the immutability and integrity of the audit logs.

Performance tests indicated that the system introduced a moderate overhead, primarily due to the encryption and blockchain processes. However, the overhead was within acceptable limits, and the security benefits far outweighed the performance trade-offs. The system demonstrated its ability to effectively detect and prevent unauthorized access while maintaining regulatory compliance.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

7.CONCLUSION

In conclusion, the development of an effective auditing schema for secure data storage in the cloud is essential for ensuring the confidentiality, integrity, and availability of sensitive data. The proposed system leverages advanced encryption techniques, access control policies, and a distributed auditing framework to achieve these goals. The implementation results demonstrated the system's effectiveness in providing a secure and transparent environment for cloud-based data storage, while also highlighting the importance of balancing security and performance. As cloud computing continues to grow, the need for robust auditing mechanisms will only increase, making this research highly relevant for organizations looking to secure their cloud-based data.

8.REFERENCES

1. Wang, C., Ren, K., & Yu, S. (2014). "Towards Secure and Privacy-Preserving Data Storage in Cloud Computing." *IEEE Transactions on Knowledge and Data Engineering, 26*(3), 1016-1029.
2. Gude, S., & Kanth, P. (2013). "Privacy-preserving Cloud Data Auditing with Secure Log Management." *International Journal of Computer Applications, 69*(23), 1-8.
3. Li, J., Li, X., & Yang, Z. (2016). "Cloud Data Auditing with Cryptographic Verification." *Journal of Cloud Computing: Advances, Systems and Applications, 5*(1), 1-11.
4. Zhang, X., & Liu, J. (2017). "A Secure Cloud Data Storage and Auditing Framework for Data Integrity." *International Journal of Security and its Applications, 11*(3), 21-32.
5. Kothari, S., & Singh, N. (2015). "Cloud Data Security and Privacy Preservation: A Survey." *International Journal of Computer Science and Information Security, 13*(7), 31-40.
6. Sun, Y., & Chen, Z. (2019). "Blockchain-Based Auditing Framework for Cloud Data Security." *Journal of Cloud Computing: Theory and Applications, 8*(2), 45-59.
7. Zhang, Y., & Xu, Z. (2018). "Towards Privacy-Preserving and Auditable Cloud Storage." *Journal of Cloud Computing, 6*(4), 82-92.

8. Smith, R., & Johnson, M. (2014). "Ensuring Data Integrity in Cloud Storage: An Auditing Approach." *IEEE Transactions on Cloud Computing, 3*(2), 124-136.
9. Liu, Q., & Wang, J. (2016). "Secure Cloud Data Access and Audit with Encryption and Blockchain." *Future Generation Computer Systems, 56*, 59-70.
10. Gupta, A., & Singh, R. (2017). "Audit Log-Based Data Integrity Verification in Cloud." *International Journal of Computer Science and Technology, 8*(1), 102-109.
11. Koc, A., & Ibrahim, S. (2015). "Auditing Cloud Data Access Using Blockchain Technology." *Journal of Information Security and Applications, 22*, 51-62.
12. Kumar, R., & Sharma, V. (2014). "A Survey of Security and Privacy Issues in Cloud Computing." *International Journal of Computer Applications, 98*(16), 16-23.
13. Liu, Z., & Zhang, L. (2017). "Privacy-Preserving Auditing of Cloud Data Using Homomorphic Encryption." *Computers, 6*(3), 45-56.
14. Chen, H., & Wang, X. (2019). "Cloud Storage Security: Challenges and Solutions." *International Journal of Cloud Computing and Services Science, 7*(4), 33-46.
15. Xu, X., & Chen, Y. (2020). "Cloud Storage Security Auditing Mechanisms: A Review." *Future Internet, 12*(1), 12-24.
16. Zhou, L., & Song, H. (2018). "Design of a Cloud Data Auditing System Based on Multi-Factor Authentication." *Journal of Cloud Computing: Advances, Systems and Applications, 7*(2), 21-34.
17. Walia, G., & Singh, P. (2016). "Cloud Data Integrity: Ensuring Accountability with Secure Auditing." *International Journal of Computer Applications, 139*(5), 58-63.
18. Wang, L., & Zhang, H. (2015). "A New Framework for Secure Data Storage and Auditing in Cloud Computing." *Journal of Information Science and Engineering, 31*(4), 1011-1027.
19. Gupta, P., & Jain, S. (2019). "Secure Cloud Data Auditing Based on Public Key Cryptography." *International Journal of Cloud Computing and Services Science, 8*(2), 77-89.
20. Yang, X., & Li, F. (2018). "Secure and Efficient Cloud Data Auditing with Redundant Data Storage." *International Journal of Information and Computer Security, 16*(3), 202-215.