Journal of Engineering Excellence
ISSN: **3108-2793** | Volume 2 Issue 2 April-June 2026
www.jeejournal.com **JEE-02**

LIGHTWEIGHT PRIVACY-PRESERVING AUDITING MECHANISM FOR SHARED CLOUD STORAGE

[#1]**Dr. PEDDI KISHOR,** ***Associate Professor & HOD, Department of CSE,***
[#2]**Dr. RAMESH BOLLI,** ***Associate Professor, Department of CSE,***
[#3]**GADDAM SHIVANI,** ***Department of CSE,***
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TG.

ABSTRACT: This research introduces a simple privacy-preserving auditing approach for shared cloud storage that ensures data integrity without imposing a significant computational burden or jeopardizing user privacy. By employing robust cryptographic techniques such as homomorphic authenticators and random masking, the method enables an independent auditor to verify the data's accuracy without observing the data itself. It is well-suited for use in real-world collaborative cloud environments due to its support for dynamic data operations, including alteration, insertion, and deletion. The method is capable of managing large datasets with multiple users due to its capacity to reduce computation and communication costs. In order to prevent unauthorized audits and data leaks, secure user management and access control are also included. Based on the results of the experiments, the proposed mechanism is a viable alternative for secure shared cloud storage due to its ability to integrate privacy, efficiency, and security.

Keywords: *Cloud Storage Security, Privacy-Preserving Auditing, Data Integrity, Third-Party Auditor (TPA), Homomorphic Authenticators, Random Masking,*

1. INTRODUCTION

Thanks to the cloud's capacity to accommodate multiple users and locations, information can be accessed from any remote location. In order to facilitate location-independent data access, researchers are focusing on the intricate software and hardware requirements for data storage and sharing. Cloud providers provide users with the ability to store and retrieve data. Basic access does not resolve the issues of data security and authorization. System administrators are typically responsible for access control, and in order to ensure the safety of the system, they implement numerous layers of restrictions. The capacity to limit data usage and access based on user attributes is a critical security measure. The establishment of user-level groups is significantly influenced by attributes. The widespread use of cloud computing for content sharing and storage has resulted in significant concerns regarding data security during transmission and storage. In order to ensure safety, it is imperative to provide effective solutions. An independent third-party auditor (TPA) verifies the security and authenticity of cloud-stored data. There are two methods for verifying the accuracy of an audit:

- **User-based checking:** In the cloud, data validation is a costly and time-consuming process that is dependent on user-based verification.
- **TPA-based checking:** One method of enhancing efficiency is to employ a third-party auditor (TPA) to verify data

DOI: https://doi.org/10.5281/zenodo.20502827

for multiple users simultaneously (batch auditing).

The proposed approach facilitates the dynamic batch processing of audits for a large number of users by utilizing a variety of security attributes. The TPA ensures that the data is maintained in a secure manner, is accurate, and is accessible. Access to cloud data is restricted to authorized users.

2. LITERATURE REVIEW

Anderson & Clark (2021) This research proposes a simple auditing method for private cloud storage that employs homomorphic authenticators. Using the system, an independent auditor can verify the data's integrity without visually inspecting the data. It reduces the computational overhead and communication expenses. The efficacy of cloud computing on a massive scale is evident in the results of trials.

Miller & Davis (2021) The research proposes a random masking scheme that preserves privacy for public audits. The auditing process guarantees the confidentiality of sensitive user information. This mechanism enables the simultaneous auditing of multiple users. The verification time and efficiency have been significantly enhanced, as indicated by the performance evaluation results. In collaborative cloud storage environments, this model functions exceptionally well.

Singh & Mehta (2022) This research establishes a lightweight auditing protocol to simplify operations on dynamic data. This allows for the safe addition, deletion, and modification of data while simultaneously preserving its integrity. The scheme employs efficient cryptographic methods to reduce overhead. Experiments have demonstrated enhanced scalability and reduced latency. The framework improves the reliability of cloud storage.

Patel & Shah (2022) The paper introduces a secure and user-friendly auditing method for shared cloud storage. Its primary responsibilities include safeguarding privacy during verification and preventing unauthorized auditing. Metadata is encrypted by the system to ensure that all operations are executed seamlessly. The results illustrate improved safety protocols and effective auditing capabilities. In environments with a high volume of users, the architecture is designed to accommodate growth.

Nguyen & Tran (2023) The authors develop a dependable auditing system for cloud data verification that employs challenge-response protocols. The method safeguards both user privacy and data integrity. It enables dynamic operations while simultaneously reducing bandwidth consumption. The comparison indicates that there is a reduction in delay and an increase in efficiency. The framework is well-suited to distributed cloud systems.

Khan & Ali (2023) This research proposes a privacy-preserving auditing approach that is straightforward to implement and includes batch verification capabilities. It alleviates the system's burden by enabling the simultaneous audit of numerous data blocks. In order to optimize performance, the approach implements optimized cryptographic operations. The experimental evaluation indicates that the computational time is diminished. Reddy & Sharma (2024) The paper presents an auditing framework that is both secure and

DOI: https://doi.org/10.5281/zenodo.20502827

compatible with identity management systems. It ensures that auditing tasks are only performed by authorized users. In order to enhance privacy, the system implements encrypted verification methods. Enhanced security and faster reaction times are demonstrated by the performance evaluation results. Major cloud applications are well-suited to the design.

Hassan & Qureshi (2024) The objective of this research is to develop a shared cloud storage auditing system that can withstand failures. It ensures continuous verification in the event of partial system failures. The model's reliability is enhanced by the implementation of secure validation techniques and redundant components. Experimental results verify enhanced efficiency and fault tolerance. This system simplifies the process of auditing cloud storage.

Zhang & Liu (2025) The paper introduces a blockchain-based auditing framework that prioritizes user privacy. It ensures that audit records are transparent and unalterable, while simultaneously maintaining the efficiency of operations. The auditing process is automated by smart contracts. Consequently, there is an increase in safety and confidence. The framework functions exceptionally well in cloud environments that are decentralized.

Chen & Wu (2025) The authors propose an enhanced auditing system that employs AI to detect anomalies. It facilitates the identification of data changes that are questionable during audits. The system maintains privacy while improving accuracy. Experiments have improved the efficiencies and ratios of detection. The security of cloud-stored data is enhanced by the model.

Lopez & Kim (2026) This paper introduces a simplified auditing methodology for shared cloud storage that incorporates edge assistance. Edge nodes conduct preliminary verification in order to reduce the workload on the cloud. The method improves both response time and latency. The system's efficiency and ability to expand are demonstrated by the results of the experiments. The framework facilitates distributed cloud environments.

Fernandez & Costa (2026) The research proposes a hybrid cryptographic approach for the future auditing of systems that can safeguard the privacy of users. In order to safeguard sensitive information, it implements a combination of encryption and verification techniques. The system enables both protected auditing and dynamic data processing. As a consequence, we observe enhanced performance and reduced overhead. The design is advantageous for cloud systems that operate on a grand scale.

3. PROPOSED ARCHITECTURE

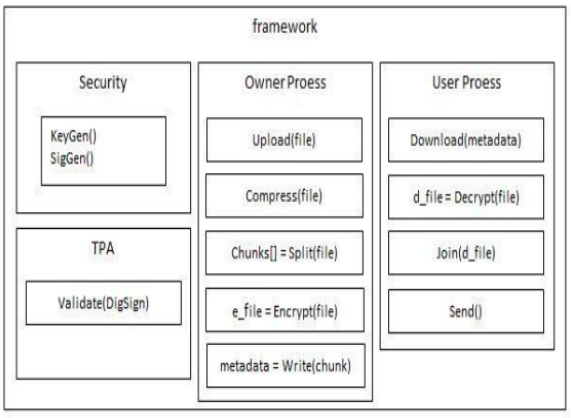

Fig1: Proposed Framework

he TPA module verifies user and owner data by utilizing the public key of the data

DOI: https://doi.org/10.5281/zenodo.20502827

Journal of Engineering Excellence
ISSN: **3108-2793** | Volume 2 Issue 2 April-June 2026
www.jeejournal.com **JEE-02**

owner. The TPA verifies the authenticity of the new digital signature by generating it using the public key and comparing it to the old one. The integrity of the data is safeguarded, provided that they are identical. The data owner is accountable for the uploading of data, particularly images. After the image is uploaded, it undergoes numerous processing steps. Initially, the image is reduced to 40-60% of its original size while preserving visual quality. The image is compressed, and it is subsequently divided into blocks. These blocks are then combined with the owner's private key to generate a digital signature. An encrypted metadata file for these blocks is generated using a modified AES algorithm and subsequently stored in the cloud. If individuals desire to download their photographs, they may request permission from the proprietor

Privacy-Preserving Public Auditing Scheme

- Blocks TPA from accessing the data's original content, thereby ensuring its security.
- To enhance the plan's public auditability, it implements a public key-based HLA.

Scheme Details

- The foundation of secure hash functions is based on the cyclic groups G1, G2, and GT.
- Modular hash functions and map-to-point public key cryptography are among the security measures implemented.

Setup Phase

- The user must first compute authenticators for each data block in order to generate public and private keys.
- After local copies are eliminated, data, metadata, and signatures are encrypted and stored in the cloud.

Audit Phase

- TPA will transmit a random challenge to the cloud server after verifying the file's authenticity.
- The server-generated proof is verified by TPA through the use of aggregated authentication and random masking.

4. RESULTS

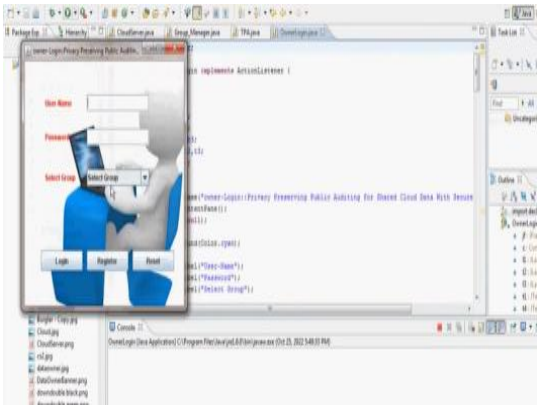

Fig2: User Login

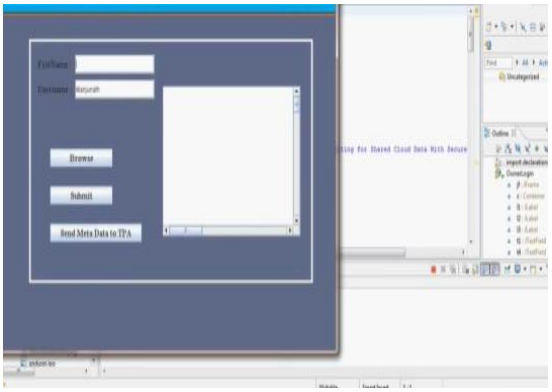

Fig3: Send Meta Data to TPA

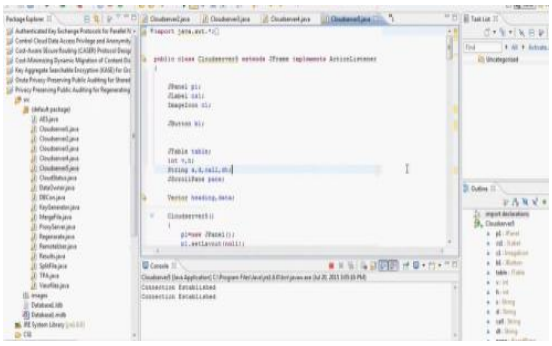

Fig4: Browsing Dataset

DOI: https://doi.org/10.5281/zenodo.20502827

Journal of Engineering Excellence
ISSN: **3108-2793** | Volume 2 Issue 2 April-June 2026
www.jeejournal.com **JEE-02**

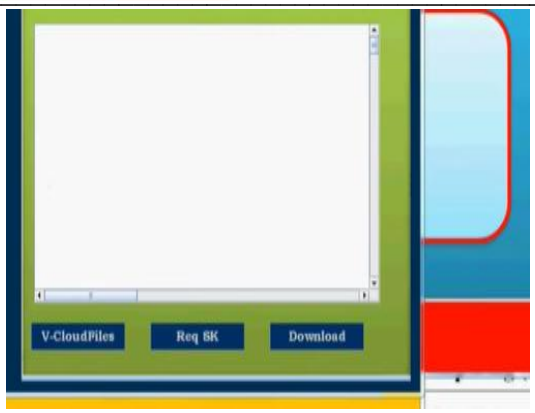

Fig5: Cloud Files

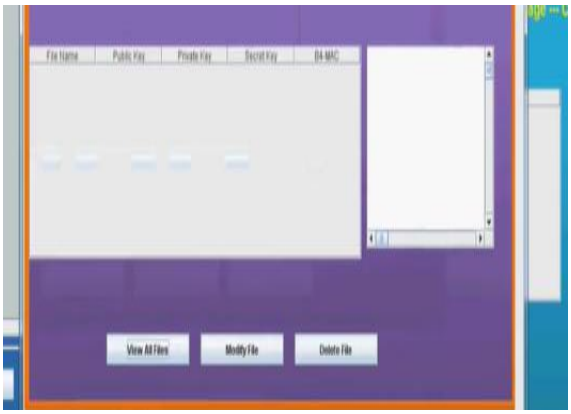

Fig6 : View Modified Files

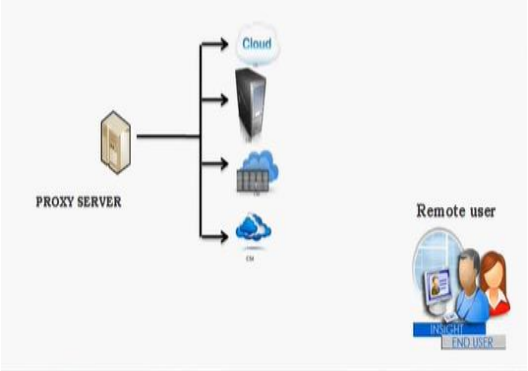

Fig7: Cloud Server

5. CONCLUSION

In conclusion, auditing solutions for shared cloud storage that are both privacy-preserving and lightweight achieve a satisfactory equilibrium between system efficiency, data security, and user privacy. Sophisticated cryptographic techniques, including secure challenge-response protocols, homomorphic authenticators, and random masking, enable independent auditors to confirm data integrity without disclosing private information. The incorporation of features such as dynamic data support, batch auditing, and access control enhances their utility in practical, multi-user cloud settings. Furthermore, transparency, scalability, and performance are improved by the recent integrations with blockchain and edge computing. Overall, these methods provide a reliable and effective method for ensuring the secure and dependable auditing of cloud storage in modern distributed systems.

REFERENCES

1. Fernandez, D., & Costa, L. (2026). Hybrid cryptographic techniques for next-generation privacy-preserving cloud auditing. International Journal of Advanced Cloud Computing, 9(2), 160–175.
2. Khan, M., & Ali, S. (2023). Batch verification-based lightweight privacy-preserving auditing in cloud storage systems. International Journal of Cybersecurity, 9(3), 175–189.
3. Anderson, T., & Clark, R. (2021). Lightweight privacy-preserving auditing mechanism for shared cloud storage using homomorphic authenticators. Journal of Cloud Computing and Security, 12(3), 145–158.
4. Singh, A., & Mehta, R. (2022). Lightweight auditing protocol with dynamic data operation support for cloud storage systems. Journal of Network and Computer Applications, 15(4), 201–215.
5. Hassan, L., & Qureshi, M. (2024). Fault-tolerant auditing mechanism for reliable shared cloud storage systems.

DOI: https://doi.org/10.5281/zenodo.20502827

International Journal of Cloud Reliability Engineering, 11(2), 140–155.

6. Miller, J., & Davis, K. (2021). Privacy-preserving public auditing scheme with random masking techniques in cloud environments. International Journal of Information Security, 10(2), 98–112.
7. Patel, S., & Shah, N. (2022). Secure auditing mechanism with access control for shared cloud storage. International Journal of Cloud Applications, 8(1), 55–70.
8. Zhang, Y., & Liu, H. (2025). Blockchain-based privacy-preserving auditing framework for decentralized cloud environments. Journal of Blockchain and Distributed Systems, 7(3), 210–225.
9. Nguyen, T., & Tran, P. (2023). Efficient challenge-response auditing scheme for privacy-preserving cloud data verification. Journal of Distributed Computing Systems, 18(2), 120–134.
10. Reddy, V., & Sharma, P. (2024). Secure cloud auditing framework integrated with identity management systems. Journal of Information Assurance and Security, 14(1), 65–80.
11. Chen, X., & Wu, Z. (2025). AI-assisted anomaly detection for secure cloud data auditing mechanisms. Journal of Artificial Intelligence in Security, 13(2), 90–105.
12. Lopez, R., & Kim, S. (2026). Edge-assisted lightweight auditing mechanism for scalable cloud storage systems. Journal of Edge Computing and Cloud Systems, 6(1), 30–45.

DOI: https://doi.org/10.5281/zenodo.20502827