www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

# ENHANCING CLOUD STORAGE SECURITY: IDENTITY-BASED AUDITING, CONCEALED DATA PROTECTION, AND SECURE DATA SHARING

[1]Dr. S. Vijayarangam,[2]M. Saketh Prudhvi,[3]P. Vaishnavi Goud,[4]M. N. Kevin,[5]M. Vivek Vardhan,[6]Sampath Reddy
[1] Assistant *Professor,* [23456]*B.Tech Students*
*Department Of Computer Science & Engineering*
*Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam*

**ABSTRACT**

Cloud storage services enable users to store data remotely and share it with others. Ensuring the integrity of stored data is critical, and remote data integrity auditing has been introduced to address this need. However, in systems like Electronic Health Records (EHRs), stored files may contain sensitive information that should not be exposed during sharing. While encrypting the entire file can hide sensitive data, it renders the file unusable for others. Currently, achieving both data sharing and sensitive information protection in remote data integrity auditing remains an unexplored challenge.

This paper proposes a remote data integrity auditing scheme that supports data sharing while concealing sensitive information. Our approach introduces a sanitizer that removes sensitive data blocks and transforms their corresponding signatures into valid ones for the sanitized file. These signatures ensure the integrity of the modified file during auditing. The scheme leverages identity-based cryptography, simplifying certificate management. Security analysis and performance evaluations demonstrate that our approach is secure and efficient, enabling cloud-stored files to be shared and utilized while safeguarding sensitive information.

## I. INTRODUCTION

The rapid development of communications and networks has significantly increased data transmission and exchange. With the growing demand for multimedia (e.g., video, images, and audio), the cost of IT services has surged for individuals and businesses. Cloud computing offers an efficient and cost-effective solution for IT services due to its economic advantages (Tian et al., 2019).

Cloud storage is a fundamental technology in cloud computing, providing scalable, on-demand storage with global accessibility. However, outsourcing data to third-party cloud service providers (CSPs) introduces security challenges, particularly concerning data integrity and privacy. Users relinquish control over their data, making it vulnerable to corruption, loss, or unauthorized access.

### 1.1 Problem Statement

Existing cloud storage auditing schemes focus on verifying data integrity but lack

mechanisms for secure data sharing with sensitive information protection. Encrypting entire files ensures confidentiality but hinders usability. Thus, there is a need for a solution that:

- Ensures data integrity through remote auditing.
- Allows selective hiding of sensitive data while maintaining file usability.
- Simplifies key management using identity-based cryptography.

### 1.2 Objectives

This research aims to:

1. Develop an identity-based auditing scheme for cloud storage.
2. Introduce a sanitizer to conceal sensitive data while preserving file usability.
3. Ensure secure data sharing with efficient integrity verification.

### 1.3 Contributions

- A novel auditing scheme supporting data sharing with sensitive information hiding.
- Integration of identity-based cryptography to eliminate certificate management overhead.
- Performance evaluation demonstrating security and efficiency.

## II. LITERATURE SURVEY

### 2.1 Identity-Based Integrity Auditing

Asha et al. (2020) proposed an identity-based auditing scheme for cloud storage, addressing the challenge of sensitive data hiding. Their sanitizer-based approach ensures data integrity while concealing sensitive blocks.

### 2.2 Key-Exposure Resilience

Mary Virgil Nithya (2021) introduced an identity-based auditing scheme resilient to key exposure, eliminating the need for certificate verification. The scheme supports batch auditing and protects against replace attacks.

### 2.3 Secure Data Sharing

Nagaraju et al. (2022) presented a method for secure data sharing in cloud storage, using a sanitizer to transform sensitive data blocks while maintaining integrity.

### 2.4 Cloud Data Security Challenges

Yang et al. (2023) surveyed data security and privacy issues in cloud storage, emphasizing encryption and access control as key countermeasures.

### 2.5 Auditing Schemes in Cloud Computing

Yadav and Garg (2023) discussed cloud data security using auditing schemes, highlighting the need for scalable and efficient integrity verification.

## III. METHODOLOGY

### 3.1 System Architecture

The proposed system consists of:

1. **User:** Uploads and shares files.
2. **PKG (Private Key Generator):** Manages identity-based keys.
3. **Sanitizer:** Removes sensitive data blocks and transforms signatures.
4. **TPA (Third-Party Auditor):** Verifies data integrity.
5. **Cloud Server:** Stores and manages data.

### 3.2 Identity-Based Cryptography

- Eliminates certificate management.

- Uses user identities (e.g., email) as public keys.

**3.3 Sanitizer Mechanism**

1. Identifies sensitive data blocks.
2. Removes or masks them.
3. Generates valid signatures for the sanitized file.

**3.4 Auditing Process**

1. **Challenge:** TPA requests proof of data integrity.
2. **Proof Generation:** Cloud server computes proof using transformed signatures.
3. **Verification:** TPA validates the proof.

## IV. EXISTING SYSTEM

**4.1 Limitations**

- **Scalability Issues:** Struggles with large-scale data.
- **Complexity:** High computational overhead for integrity checks.
- **Key Management:** Relies on complex certificate-based systems.

**4.2 Disadvantages**

- Inefficient for dynamic data sharing.
- Lacks mechanisms for selective sensitive data hiding.

## V. PROPOSED SYSTEM

**5.1 Advantages**

- **Improved Usability:** Simplified key management.
- **Enhanced Scalability:** Efficient auditing for large datasets.
- **Robust Security:** Identity-based cryptography ensures secure data sharing.

**5.2 Algorithms**

1. **Key Generation:**
- PKG generates private keys based on user identities.
2. **Sanitization:**
- Sensitive blocks are identified and removed.
- Signatures are transformed for the sanitized file.
3. **Auditing:**
- TPA verifies integrity using transformed signatures.

## VI. RESULTS AND DISCUSSION

**6.1 System Testing**

- **Test Case 1:** Login validation (invalid credentials rejected).
- **Test Case 2:** User registration (duplicate IDs detected).

**6.2 Performance Evaluation**

- **Efficiency:** Reduced computational overhead compared to traditional schemes.
- **Security:** Resistant to replace attacks and unauthorized access.

**6.3 Screenshots**

- **Home Page:** User interface for accessing cloud storage.
- **Registration Page:** Secure user onboarding.
- **Admin Dashboard:** Management of user data and audits.

## VII. CONCLUSION

This paper presented a secure cloud storage auditing scheme supporting data sharing with sensitive information hiding. The proposed system leverages identity-based cryptography for simplified key management and introduces a sanitizer to conceal sensitive data. Performance evaluations

confirm the scheme's efficiency and security.

### 7.1 Future Scope

- Extend the scheme to support multi-user collaborative environments.
- Explore blockchain integration for decentralized auditing.

## REFERENCES

1. Asha, S., Punitha, K., & Joshi, T. (2020). *Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage.*
2. Nithya, S. M. V. (2021). *Identity-Based Public Auditing Scheme for Cloud Storage with Strong Key-Exposure Resilience.*
3. Nagaraju, D., Bhavani, R., & Srinivas, K. (2022). *Empower Identity-Based Integrity Auditing and Information Distribution with Confidential Data Defeat for Safety Cloud Storage.*
4. Yang, P., Xiong, N., & Ren, J. (2023). *Data Security and Privacy Protection for Cloud Storage: A Survey.*
5. Yadav, A. K., & Garg, M. L. (2023). *Cloud Data Security using Auditing Scheme.*