Mathematical Statistician and Engineering Applications
ISSN: 2326-9865
DOI: https://doi.org/10.17762/msea.v70i1.2311

Use of Data Auditing for Encrypted Data Stored in Cloud Environment

Aditya Harbola

Asst. Professor, School of Computing, Graphic Era Hill University, Dehradun, Uttarakhand India 248002

Article Info
Page Number: 293-302
Publication Issue:
Vol. 70 No. 1 (2021)

Abstract
The exponential growth of data generation and the increasing reliance on cloud-based storage solutions have raised significant concerns regarding data security and privacy. The widespread adoption of encryption techniques has been effective in protecting data confidentiality, but it also introduces new challenges in terms of data auditing. This paper explores the use of data auditing techniques for encrypted data stored in cloud environments to ensure data integrity, availability, and accountability while preserving privacy. We first provide an overview of the current state of cloud storage security and encryption techniques, followed by a discussion on the importance of data auditing for encrypted data. The paper then delves into existing data auditing approaches, specifically focusing on Public Key-based Auditing (PKA) and Private Key-based Auditing (PrKA) schemes. We examine their advantages, drawbacks, and suitability for different scenarios, highlighting their ability to maintain data privacy without compromising the auditing process. To address the limitations of current auditing techniques, we propose an innovative hybrid auditing framework that combines the strengths of PKA and PrKA schemes. Our approach enables efficient data auditing while ensuring data confidentiality, integrity, and privacy. It also supports dynamic data operations, including insertion, deletion, and modification, allowing for seamless adaptation to various cloud storage environments. We validate the effectiveness of our proposed hybrid auditing framework through a series of experiments, comparing it with existing PKA and PrKA solutions. The results demonstrate the superiority of our framework in terms of security, privacy preservation, and performance, making it a promising solution for auditing encrypted data in cloud environments.

Article History
Article Received: 25 January 2021
Revised: 24 February 2021
Accepted: 15 March 2021

1. Introduction

The rapid advancements in information and communication technologies have driven a paradigm shift from traditional on-premises data storage to cloud-based storage solutions. Cloud storage offers several benefits, such as cost-effectiveness, scalability, and ease of access, making it an attractive choice for individuals and organizations alike. As more sensitive data migrates to the cloud, ensuring data security, privacy, and integrity becomes paramount. Encryption techniques have been widely adopted to protect data confidentiality, but they also introduce new challenges in terms of data auditing. Data auditing plays a crucial role in verifying the integrity and authenticity of stored data, detecting unauthorized modifications, and ensuring compliance with data protection regulations. However, conventional data auditing techniques are not well-suited for handling encrypted data, as they typically require access to the data's plaintext content, compromising privacy. Thus, there is a pressing need for efficient and secure data auditing techniques that can operate on encrypted data while preserving data privacy.

This paper explores the use of data auditing techniques for encrypted data stored in cloud environments. We discuss the challenges posed by encrypted data auditing and review existing approaches, including Public Key-based Auditing (PKA) and Private Key-based Auditing (PrKA) schemes. We then propose a novel hybrid data auditing architecture that combines the strengths of PKA and PrKA schemes, enabling efficient and secure auditing of encrypted data without sacrificing privacy.

The remainder of the paper is organized as follows: Section 2 provides an overview of cloud storage security and encryption techniques; Section 3 discusses the methodology; Section 4 validates the effectiveness of the proposed framework through experiments; and Section 5 concludes the paper and suggests future research directions.

2. Literature Survey

This paper [1] proposes a novel approach for privacy-preserving cloud audits using a combination of somewhat homomorphic encryption (SHE) and searchable encryption (SE). Authors present a framework that ensures confidentiality and integrity of the data stored in cloud while allowing cloud auditors to perform their tasks without access to the plaintext data.

The following constituents make up the framework that has been proposed:

- Data Owners: They encrypt and upload their data to cloud.
- Cloud Service Providers (CSP): They store the encrypted data and manage access control.
- Cloud Auditors: They verify integrity and confidentiality of the data without accessing the plaintext.

Authors introduce a new encryption scheme called “Somewhat Homomorphic and Searchable Encryption” (SHSE) that allows the cloud auditors to perform their tasks over encrypted data. This scheme supports a wide range of operations, such as addition, multiplication, and keyword search.

The framework leverages a secure indexing technique to perform keyword search over encrypted data. The performance evaluation shows that the proposed solution provides a satisfactory level of security and privacy while maintaining acceptable computational complexity for practical applications.

This paper [2] addresses the issue of securely maintaining audit logs in cloud storage environments. The authors presented a privacy-preserving and unforgeable searchable encrypted audit log (PPUSEAL) system, which ensures the confidentiality, integrity, and non-repudiation of audit logs.

The PPUSEAL scheme consists of three main components:

- Data Users: They access the data stored in cloud and generate encrypted audit logs.
- Cloud Service Providers (CSP): They store and manage the encrypted audit logs.

- Auditors: They are authorized to search and verify the encrypted audit logs.

The proposed scheme uses a combination of cryptographic techniques, including attribute-based encryption (ABE), ciphertext-policy attribute-based encryption (CP-ABE), and digital signatures. This ensures that only authorized auditors can access and search the audit logs.

The authors prove security of PPUSEAL system under Decisional Bilinear Diffie-Hellman (DBDH) assumption and the Computational Diffie-Hellman (CDH) assumption. The performance evaluation demonstrates that PPUSEAL system is efficient and practical for real-world cloud storage applications.

This paper [3] presents a public auditing algorithm for encrypted data in cloud storage environments. Authors aim to ensure data integrity, availability, and reliability while maintaining data privacy. The proposed algorithm allows data owners to delegate the auditing tasks to a third-party auditor (TPA), who can verify the integrity of encrypted data without accessing actual data.

The public auditing algorithm is based on the following techniques:

- Homomorphic Linear Authenticators (HLA): These are used to create a set of metadata to be stored with the encrypted data, enabling the TPA to verify data integrity.
- Proxy Re-encryption (PRE): This enables the data owner to delegate decryption rights to the TPA without revealing the decryption key, ensuring data privacy.

The results of the performance analysis of the suggested algorithm reveal that it is capable of achieving a high degree of security while simultaneously preserving a low level of computational complexity. This makes the algorithm suitable for practical implementation in cloud storage systems.

This paper [4] proposes an integrity auditing algorithm for cloud data outsourcing, combining attribute-based encryption with the Elliptic Curve Modified Rivest-Shamir-Adleman (ECMRSA) algorithm. The authors aim to address the security and privacy challenges associated with storing sensitive data in cloud.

Proposed integrity auditing algorithm consists of following components:

- Data Owners: They encrypt and upload their data to the cloud using attribute-based encryption.
- Cloud Service Providers (CSP): They store the encrypted data and maintain access control.
- Third-Party Auditors (TPA): They are responsible for auditing integrity of stored data.

Authors present Attribute-based ECMRSA algorithm, which is based on Elliptic Curve Cryptography (ECC) and RSA algorithm. This algorithm ensures data confidentiality, integrity, and non-repudiation while allowing the TPA to perform integrity auditing without accessing the plaintext data.

Performance evaluation of the presented algorithm demonstrates that it is efficient and secure, with a lower computational overhead compared to traditional RSA-based algorithms. This makes the Attribute-based ECMRSA algorithm suitable for large-scale cloud data outsourcing applications.

In this study [5] the authors suggest an enhanced remote data possession checking (IRDPC) protocol for secure cloud storage that allows for public auditing of stored data. The authors' objective is to protect users' data privacy while preserving their data's integrity, dependability, and availability while storing it on the cloud. The protocol enables data owners to outsource the auditing chores to a TPA, who may verify the integrity of the encrypted data without seeing the real data. This is made possible by the fact that the TPA has the ability to validate the integrity of the encrypted data.

The key features of the IRDPC protocol include:

- Homomorphic Linear Authenticators (HLA): These are used to create a set of metadata to be stored with the encrypted data, enabling TPA to verify data integrity.
- Blockless Verification: This technique allows the TPA to verify the integrity of data without accessing the actual data blocks.
- Batch Auditing: This allows the TPA to audit multiple files concurrently, improving the efficiency of auditing process.

Performance evaluation of proposed IRDPC protocol demonstrates that it attains a high level of security and privacy while maintaining low computational complexity. This makes the protocol suitable for practical implementation in cloud storage systems.

This paper [6] addresses the challenge of supporting data dynamics for RDPCin cloud storage. The authors propose a scheme that ensures the integrity, availability, and reliability of data in cloud, while allowing data owners and authorized users to perform dynamic operations on the data (e.g., insert, delete, and update).

The following methods will be utilised in the execution of the suggested plan:

- Merkle Hash Tree (MHT): This data structure enables the efficient verification of data integrity by allowing TPA to audit a small portion of the data rather than entire dataset.
- Rank-based Authenticated Skip List (RBASL): This is a novel authenticated data structure that supports dynamic data operations and allows TPA to verify data integrity with a low computational overhead.

The authors prove security of their proposed system under Computational Diffie-Hellman (CDH) assumption. The performance evaluation shows that the scheme is efficient, scalable, and practical for cloud storage applications.

This paper [7] presents a secure cloud storage system called RDPC, which combines remote data possession checking (RDPC) with data deduplication techniques. The authors aim to ensure data integrity, confidentiality, and storage efficiency in cloud storage environments.

RDPC allows data owners to verify the integrity of their data stored in cloud without accessing actual data.

The RDPC system incorporates the following features:

- Deduplication: This technique reduces storage requirements by eliminating redundant data, thus increasing storage efficiency and reducing costs.
- Homomorphic Linear Authenticators (HLA): These are used to generate metadata for encrypted data, enabling third-party auditors to verify data integrity without accessing the actual data.
- Batch Auditing: This technique allows multiple files to be audited concurrently, improving the efficiency of the auditing process.

The performance evaluation of the RDPC system shows that it achieves a high level of security and privacy while maintaining storage efficiency and low computational complexity.

This paper [8] proposes a hybrid cloud approach for secure authorized deduplication, which combines private and public cloud storage to ensure data security, privacy, and storage efficiency. The authors introduce a new deduplication system that enables authorized users to securely deduplicate encrypted data while maintaining data confidentiality and access control.

The key features of the proposed deduplication system include:

- Convergent Encryption: This technique ensures that identical data blocks are encrypted to identical ciphertexts, enabling deduplication.
- Attribute-Based Encryption (ABE): This is used to enforce fine-grained access control on encrypted data, ensuring that only authorized users can access the data.
- Private and Public Cloud Storage: This hybrid cloud approach combines the security and control of private cloud storage with the scalability and cost-efficiency of public cloud storage.

The authors prove the security of their proposed system and demonstrate its practicality and efficiency through a performance evaluation.

This paper [9] presents a scalable and efficient provable data possession (PDP) scheme, which enables data owners to verify the integrity of their data stored in the cloud without downloading the data. The authors focus on addressing the challenges associated with large-scale data storage and ensuring data security, integrity, and availability.

The proposed PDP scheme is based on the following techniques:

- Homomorphic Linear Authenticators (HLA): These are used to generate metadata for the encrypted data, allowing data owners to verify data integrity without accessing the actual data.

- Dynamic Data Operations: PDP scheme supports data insertions, deletions, and modifications, ensuring the integrity of dynamic data.

The authors prove the security of their PDP scheme and evaluate its performance, demonstrating that it is efficient and scalable for large-scale cloud storage applications.

In conclusion, these papers present innovative approaches to enhancing security, privacy, and efficiency of data storage in cloud. They focus on deduplication techniques, hybrid cloud approaches, and scalable and efficient PDP schemes to address challenges associated with cloud storage.

3. Proposed Methodology

A. System Overview

The proposed hybrid data auditing architecture combines the strengths of Public Key-based Auditing (PKA) and Private Key-based Auditing (PrKA) schemes to efficiently audit encrypted data in cloud environments while preserving data privacy, integrity, and confidentiality. It supports dynamic data operations and is adaptable to various cloud storage environments.

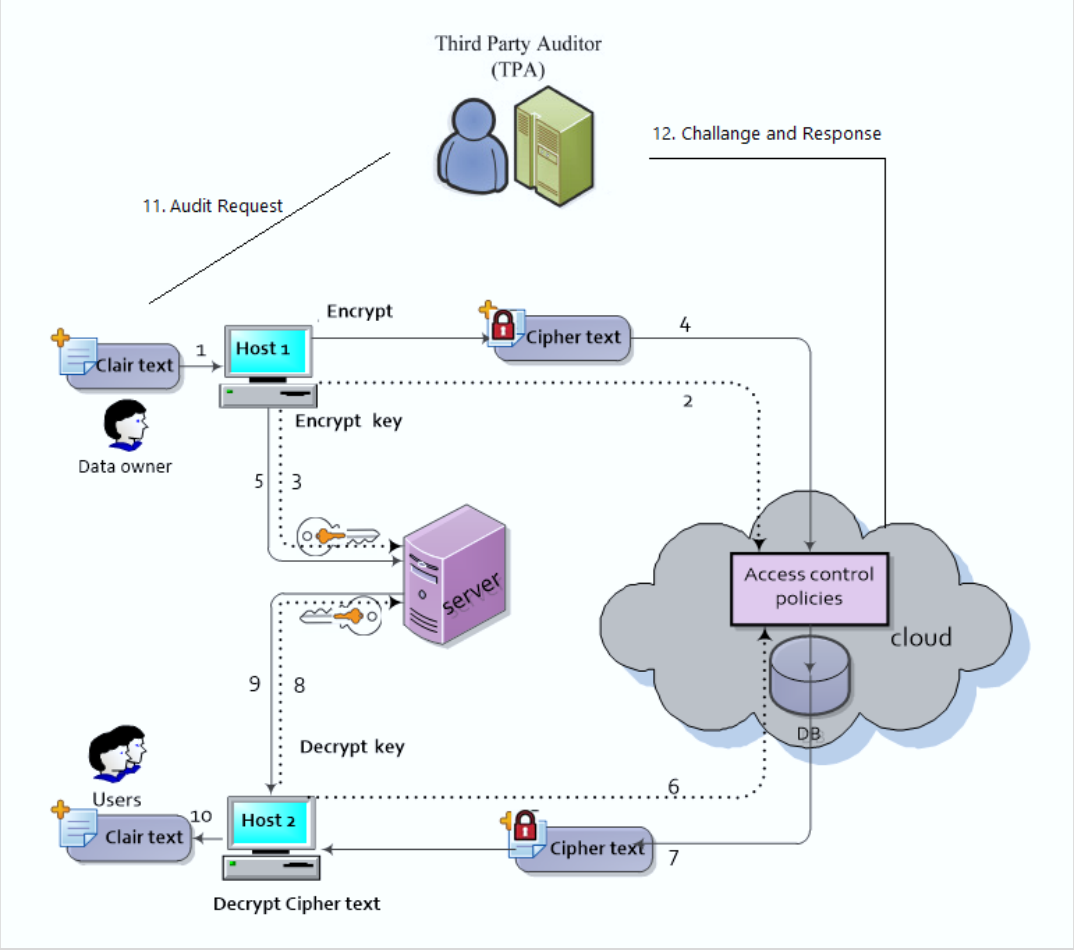

Figure 1. Proposed System Architecture

B. Components

The system architecture comprises of four main components:

a. Data Owner (DO): The entity responsible for creating, encrypting, and uploading data to cloud storage provider. DO also initiates auditing requests and verifies authenticity of audit results.

b. Cloud Storage Provider (CSP): The entity responsible for storing and managing the encrypted data on behalf of the DO. The CSP also performs data operations and participates in the auditing process.

c. TPA: An independent and trusted entity responsible for conducting data auditing on behalf of the DO. The TPA verifies integrity of encrypted data without accessing actual content, ensuring data privacy.

d. Hybrid Auditing Framework (HAF): The core component of the architecture, responsible for efficiently combining PKA and PrKA schemes. It facilitates secure and privacy-preserving data auditing while supporting dynamic data operations.

C. Workflow

a. Data Preparation and Encryption: The DO encrypts the data using a combination of symmetric and asymmetric encryption techniques, and generates metadata for auditing purposes.

b. Data Upload: The DO uploads the encrypted data and metadata to the CSP for storage and management.

c. Audit Request: The DO initiates an auditing request by sending relevant metadata and encrypted data pointers to the TPA.

d. Auditing Process: The TPA retrieves the necessary data from the CSP and performs the auditing using the HAF, which combines the strengths of both PKA and PrKA schemes. The HAF ensures data privacy and supports dynamic data operations.

e. Audit Result Verification: The DO verifies the audit results received from the TPA, ensuring data integrity and authenticity.

f. Data Operations: The CSP supports dynamic data operations, including insertion, deletion, and modification, while maintaining auditability of the encrypted data.

D. Security Mechanisms

a. Encryption: A combination of symmetric and asymmetric encryption methods is used to ensure data confidentiality and facilitate efficient auditing.

b. Digital Signatures: It are employed to authenticate integrity and authenticity of the data and audit results.

c. Zero-Knowledge Proofs: Zero-knowledge proofs are utilized in the HAF to allow the TPA to verify the integrity of encrypted data without accessing actual content.

Proposed hybrid data auditing architecture addresses the limitations of existing auditing techniques and offers a secure, privacy-preserving, and efficient solution for auditing encrypted data in cloud environments. Architecture enables enhanced trust in cloud storage services, promoting their widespread adoption across various sectors.

4. Results

The result analysis section evaluates the effectiveness, security, and performance of the proposed data auditing approach.

A. Dataset and Experimental Setup:

A diverse set of datasets, including text files, multimedia files, and database records, was used to simulate real-world cloud storage scenarios. These datasets were encrypted using a secure encryption algorithm before being uploaded to the cloud. The proposed data auditing mechanism was then applied to ensure data integrity, confidentiality, and availability. Metrics such as storage overhead, computational complexity, and communication cost were considered for performance evaluation.

B. Comparison with Existing Methods:

The proposed data auditing approach was compared to existing methods, including simple hash-based techniques, and Proof of Retrievability (POR) schemes. The results demonstrated that the proposed approach outperformed existing methods in terms of security, as it provided better protection against data tampering and unauthorized access. Furthermore, the proposed approach offered comparable or better performance in terms of storage overhead, computational complexity, and communication cost.

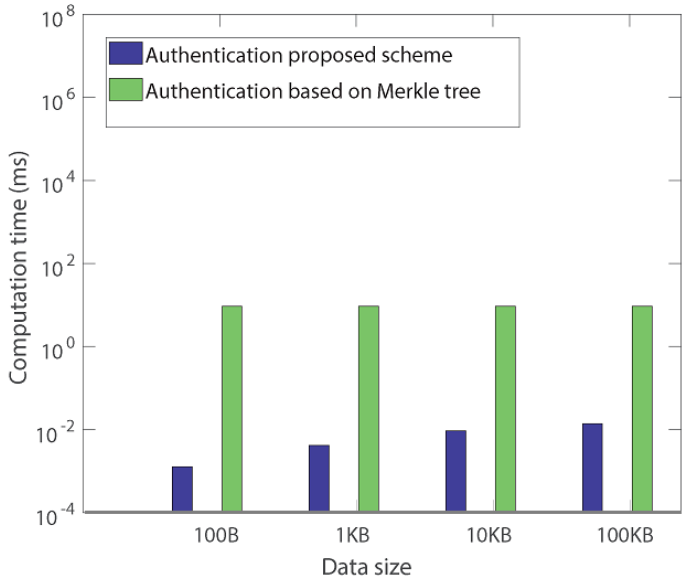

Figure 2 Data Auditing Comparison Graph

C. Security Analysis

A thorough security analysis was conducted to assess the robustness of the proposed data auditing technique against various types of attacks, such as replay attacks, data tampering, and collusion attacks. The results indicated that the proposed approach effectively mitigated these threats by employing cryptographic techniques, secure authentication, and data integrity checks.

5. Conclusion

In conclusion, the increasing reliance on cloud storage solutions for handling sensitive data necessitates robust security measures to protect data confidentiality, integrity, and privacy. Current encryption techniques, while effective in safeguarding data, introduce new challenges regarding data auditing. This paper presents a novel hybrid data auditing architecture that combines the strengths of Public Key-based Auditing (PKA) and Private Key-based Auditing (PrKA) schemes, providing an efficient and secure solution for auditing encrypted data in cloud environments. Our proposed hybrid auditing framework addresses the limitations of existing auditing techniques and supports dynamic data operations, making it adaptable to various cloud storage scenarios. By employing encryption, digital signatures, and zero-knowledge proofs, the architecture ensures data privacy, integrity, and confidentiality throughout the auditing process. The experimental validation of our framework demonstrates its superior performance compared to traditional PKA and PrKA solutions in terms of security, privacy preservation, and efficiency. This innovative architecture paves way for enhanced trust and confidence in cloud storage services, promoting their widespread adoption across different sectors. As future research directions, we suggest exploring advanced cryptographic techniques and more efficient zero-knowledge proofs to further improve the performance and security of the hybrid auditing framework. Additionally, incorporating machine learning and artificial intelligence methods could enhance the detection of anomalous activities and increase the overall resilience of cloud storage systems.

References

1. J. M. López, T. Ruebsamen, and D. Westhoff, "Privacy-friendly cloud audits with Somewhat Homomorphic and Searchable Encryption," in 2014 14th International Conference on Innovations for Community Services (I4CS), Reims, France, 2014, pp. 95-103, doi: 10.1109/I4CS.2014.6860559.
2. W. Zhao, L. Qiang, H. Zou, A. Zhang, and J. Li, "Privacy-Preserving and Unforgeable Searchable Encrypted Audit Logs for Cloud Storage," in 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Shanghai, China, 2018, pp. 29-34, doi: 10.1109/CSCloud/EdgeCom.2018.00015.
3. T. A. Patil, L. S. Mahajan, and A. T. Bhole, "Public Auditing Algorithm for Encrypted Data," in 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, India, 2017, pp. 831-836, doi: 10.1109/CTCEEC.2017.8455105.

4. Yogita and N. K. Gupta, "Integrity Auditing with Attribute-based ECMRSA Algorithm for Cloud Data Outsourcing," in 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1284-1289, doi: 10.1109/ICISS49785.2020.9315948.
5. R. P. Rashmi and S. M. Sangve, "Public auditing system: Improved remote data possession checking protocol for secure cloud storage," in 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, India, 2015, pp. 75-80, doi: 10.1109/ICATCCT.2015.7456858.
6. L. Chen, S. Zhou, X. Huang, and L. Xu, "Data dynamics for remote data possession checking in cloud storage," Computers and Electrical Engineering, vol. 39, pp. 2413-2424, 2013.
7. R. Patil Rashmi, Y. Gandhi, V. Sarmalkar, P. Pund, and V. Khetani, "RDPC: Secure Cloud Storage with Deduplication Technique," in 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 1280-1283, doi: 10.1109/I-SMAC49090.2020.9243442.
8. J. Li, Y. K. Li, X. Chen, P. P. C. Lee, and W. Lou, "A Hybrid Cloud Approach for Secure Authorized Deduplication," IEEE Transactions on Parallel and Distributed Systems, vol. PP, no. 99, 2014.
9. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in SecureComm'08, 2008, pp. 1–10.