AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.5, NO. 4(2025)

IMPROVING SECURITY IN CLOUD STORAGE: AUDITING BY IDENTITY, HIDDEN DATA, AND SECURE SHARING

Mr. Mohammed Zeeshan Ahmed, Mr. Mohammad Abrar Ahmed, Mr. Mohammed Sami Shaik, Mrs. Khutaija Abid[4]
[1,2,3]B.E. Student, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
[4] Assistant Professor, Department of IT, Lords Institute of Engineering and Technology, Hyderabad
khutaija@lords.ac.in

Abstract— Cloud storage services enable users to outsource data and share it remotely, but ensuring both integrity and privacy of sensitive information remains a critical challenge. Traditional remote data integrity auditing verifies correctness of stored files; however, in applications such as Electronic Health Records (EHRs), directly sharing files risks exposing confidential data, while encrypting entire files hides sensitive content but limits usability. To overcome this, we propose an identity-based remote data integrity auditing scheme that integrates sensitive information hiding with secure data sharing. The approach employs a sanitizer to replace sensitive data blocks with sanitized versions and transform their signatures into valid ones, enabling integrity verification without revealing hidden content. Additionally, proxy re-signatures facilitate efficient and secure user revocation, while a blockchain-based decentralized auditing process eliminates reliance on a trusted third party, thereby enhancing transparency and reliability. Security and performance evaluations demonstrate that the proposed scheme achieves strong privacy preservation, reduced computational overhead, and practical efficiency for real-world cloud storage applications.

Index Terms— Cloud storage; Remote integrity auditing; Data sharing; Privacy preservation; Identity-based cryptography; Blockchain.

I. INTRODUCTION

With the rapid expansion of data volumes, storing massive datasets locally has become increasingly impractical for users. As a result, both individuals and organizations are increasingly opting to outsource their data storage to cloud environments. Nevertheless, data stored in the cloud remains vulnerable to corruption or loss caused by unavoidable factors such as software defects, hardware failures, or human errors [1]. To ensure the correctness and reliability of outsourced data, numerous remote data integrity auditing mechanisms have been developed and widely studied [2][3].

In remote data integrity auditing frameworks, the data owner initially generates cryptographic signatures for individual data blocks prior to uploading them to the cloud. These signatures serve as proofs during the auditing phase, ensuring that the cloud indeed retains the corresponding data blocks. Once generated, both the data blocks and their associated signatures are uploaded to the cloud server. In practical cloud storage platforms such as Google Drive, Dropbox, and iCloud, stored data is frequently shared among multiple users. Data sharing, being a fundamental functionality of cloud services, enables users to provide access to their files with others. However, shared datasets often contain sensitive information that must be protected—for example, Electronic Health Records (EHRs) [4]

II. PROBLEM DEFINITION

In order to address above problems, we design a new efficient signature algorithm in the phase of signature generation. The designed signature scheme supports blockless verifiability, which allows the verifier to check the integrity of data without downloading the entire data from the cloud. In addition, it is based on identity-based cryptography, which simplifies the complicated certificate management.

In our proposed scheme, the PKG generates the private key for user according to his identity ID. The user can check the correctness of the received private key. When there is a desire for the user to upload data to the cloud, in order to preserve the personal sensitive information of the original file from the sanitizer, this user needs to use a blinding factor to blind the data blocks corresponding to the personal sensitive information of the original file. When necessary, the user can recover the original file from the blinded one by using this blinding factor. And then this user employs the designed signature algorithm to generate signatures for the blinded file. These signatures will be used to verify the integrity of this blinded file. In addition, the user generates a file tag, which is used to ensure the correctness of the file identifier name and some verification values. The user also computes a transformation value that is used to transform signatures for sanitizer. Finally, the user sends the blinded file, its corresponding signatures, and the file tag along with the transformation value to the sanitizer. When the above messages from user are valid, the sanitizer firstly sanitizes the blinded data blocks into a uniform format and also sanitizes the data blocks corresponding to the organization's sensitive information to protect the privacy of organization,

III. LITERATURE SURVEY

In order to verify the integrity of the data stored in the cloud, many remote data integrity auditing schemes have been proposed. To reduce the computation burden on the user side, a Third Party Auditor (TPA) is introduced to periodically verify the integrity of the cloud data on behalf of user. Ateniese et al. [2] firstly proposed a notion of Provable Data Possession (PDP) to ensure the data possession on the untrusted cloud. In their proposed scheme, homomor phic authenticators and random sampling strategies are used to achieve blockless verification and reduce I/O costs. Juels and Kaliski [3] defined a model named as Proof of Retrievability (PoR) and proposed a practical scheme. In this scheme, the data stored in the cloud can be retrieved and the integrity of these data can be ensured. Based on pseudorandom function and BLS signature, Shacham and Waters [4] proposed a private remote data integrity auditing scheme and a public remote data integrity auditing scheme. In order to protect the data privacy, Wang et al. [5] proposed a privacy-preserving

remote data integrity auditing scheme with the employment of a random masking technique. Worku et al. [6] utilized a different random masking technique to further construct a remote data integrity auditing scheme supporting data privacy protection. This scheme achieves better efficiency compared with the scheme in.To reduce the computation burden of signature generation on the user side, Guan et al. [7] designed a remote data integrity auditing scheme based on the indistinguishability obfuscation tech nique. Shen et al. [8] introduced a Third Party Medium (TPM) to design a light-weight remote data integrity auditing scheme. In this scheme, the TPM helps user generate signatures on the condition that data privacy can be protected. In order to support data dynamics, Ateniese et al. [10] firstly proposed a partially dynamic PDP scheme. Erway et al. [11] used a skip list to construct a fully data dynamic auditing scheme. Wang et al. [12] proposed another remote data integrity auditing scheme supporting full data dynamics by utilizing Merkle Hash Tree.

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

To enable data sharing while concealing sensitive information, we adopt the concept of sanitizable signatures [10], whereby an authorized sanitizer is introduced to sanitize the sensitive portions of a file. However, directly applying this technique in remote data integrity auditing is impractical. First, the construction in relies on chameleon hashes, many of which suffer from key exposure vulnerabilities. To mitigate this issue, the scheme requires the use of strongly unforgeable chameleon hashes, which significantly increases computational costs [11]. Second, the signature scheme in lacks support for blockless verifiability, meaning that a verifier must retrieve the entire dataset from the cloud to check its integrity. This approach leads to excessive communication overhead and high verification latency, particularly in large-scale storage scenarios. Third, the scheme depends on a Public Key Infrastructure (PKI), which introduces the additional burden of complex certificate management.

B.

C.

D.

IV. RELATED WORK.

1. security of auditing mechanisms for secure cloud storage
2. One secure data integrity verification scheme for cloud storage
3. Cloud storage auditing and data sharing with data deduplication and private information protection for cloud-based EMR

1. Security of auditing mechanisms for secure cloud storage

Cloud computing is a novel computing model that enables convenient and on-demand access to a shared pool of configurable computing resources. Auditing services are highly essential to make sure that the data is correctly hosted in the cloud. In this paper, we investigate the active adversary attacks in three auditing mechanisms for shared data in the cloud, including two identity privacy-preserving auditing mechanisms called Oruta and Knox, and a distributed storage integrity auditing mechanism. We show that these schemes become insecure when active adversaries are involved in the cloud storage. Specifically, an active adversary can arbitrarily alter the cloud data without being detected by the auditor in the verification phase. We also propose a solution to remedy the weakness without sacrificing any desirable features of these mechanisms.

2. One secure data integrity verification scheme for cloud storage

Cloud computing is a novel kind of information technology that users can enjoy sundry cloud services from the shared configurable computing resources. Compared with traditional local storage, cloud storage is a more economical choice because the remote data center can replace users for data management and maintenance, which can save time and money on the series of work. However, delivering data to an unknown Cloud Service Provider (CSP) makes the integrity of data become a potential vulnerability. To solve this problem, we propose a secure identity based aggregate signatures (SIBAS) as the data integrity checking scheme which resorts Trusted Execution Environment (TEE) as the auditor to check the outsourced data in the local side. SIBAS can not only check the integrity of outsourced data, but also achieve the secure key management in TEE through Shamir's threshold scheme. To prove the security, security analysis in the random oracle model under the computational Diffie–Hellman assumption shows that SIBAS can resist attacks from the adversary that chooses its messages and target identities, experimental results also show that our solution *is viable and efficient in practice.*

3. Cloud storage auditing and data sharing with data deduplication and private information protection for cloud-based EMR

In the cloud-based electronic medical records (EMRs) system, the doctors upload EMRs to the cloud for storage and sharing. However, the integrity of EMRs stored in the cloud cannot be guaranteed and sharing EMRs may leak the patients' private information. Furthermore, shared EMRs contain a lot of duplicate data, leading to data redundancy. To solve the above issues, we propose a cloud storage auditing and data sharing scheme with data deduplication and private information protection for cloud-based EMR. In our proposed scheme, we introduce the sanitizer to sanitize the data blocks

containing the private information in EMR, and transform these blocks' authenticators into the authenticators of sanitized EMR. The authenticators are utilized to check the data integrity. Using the above method, the EMR stored in the cloud can be shared with researchers while ensuring the privacy of private information and the integrity of EMR. In addition, our scheme can achieve block-level deduplication, in which only one copy of the deduplicated blocks in EMR needs to be stored. The conducted security analysis and performance evaluation affirm the security and efficiency of the proposed scheme.

A. EXISTING SYSTEM

With the explosive growth of data, it is a heavy burden for users to store the sheer amount of data locally. Therefore, more and more organizations and individuals would like to store their data in the cloud. However, the data stored in the cloud might be corrupted or lost due to the inevitable software bugs, hardware faults and human errors in the cloud, used a skip list to construct a fully data dynamic auditing scheme. Wang *et al*. [12]. In order to verify whether the data is stored correctly in the cloud, many remote data integrity auditing schemes have been proposed.

1.Scalability Issues: The existing system may struggle to handle large-scale data storage and sharing requirements. As more users and data are added to the system, the computational and storage overhead for identity-based integrity auditing and sensitive information hiding can become a bottleneck, leading to performance degradation.

2.**Complexity and Overhead**: Implementing identity-based integrity auditing and sensitive information hiding typically involves complex cryptographic operations and additional metadata management. This can introduce overhead in terms of processing power and storage, potentially slowing down data access and sharing operations.

3.**Key Management Challenges:** Managing cryptographic keys for identity-based integrity auditing and data sharing can be challenging. If not handled properly, it can lead to key exposure risks or difficulties in key revocation and rotation. The existing system may not provide an efficient and user-friendly key management mechanism, making it less practical for users.

B. PROPOSED SYSTEM

The system model involves five kinds of different entities: the cloud, the user, the sanitizer, the Private Key Generator (PKG) and the Third-Party Auditor (TPA), as shown in Fig 1.

1.Improved Usability: The proposed system may offer a more user-friendly interface and seamless integration with cloud storage services.

2.Enhanced Scalability: By optimizing resource usage and employing efficient cryptographic techniques, the proposed system can potentially offer better scalability. It may handle larger volumes of data and more users while maintaining acceptable performance levels, addressing one of the disadvantages of the existing system.

3.Robust Security: The proposed system could enhance security by implementing advanced encryption and access control mechanisms. It may also include robust key management solutions, reducing the risk of key exposure and ensuring the confidentiality and integrity of sensitive data.

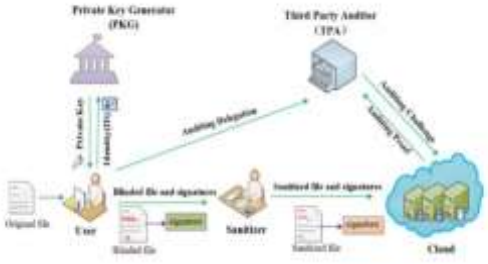

Figure 1: Architecture of the Proposed System

IV.RESULTS

Improving security in cloud storage involves several innovative approaches to ensure data integrity, privacy, and efficient sharing. Here are some key methods:

Identity-Based Integrity Auditing: One approach is the use of Secure Identity-Based Aggregate Signatures (SIBAS) combined with Trusted Execution Environment (TEE) for data integrity verification. SIBAS allows for the checking of data integrity while TEE, running on local infrastructure, acts as an auditor to verify the outsourced data and manage keys securely. This method reduces the risk of key leakage and ensures that users' private information remains confidential.

Hidden Data and Sensitive Information Protection: Another critical aspect is the protection of sensitive information within shared files. A proposed scheme enables data sharing while hiding sensitive information. This is achieved by selectively encrypting only the sensitive parts of the data, allowing the rest to remain accessible and usable by authorized users. This approach ensures that the integrity of the data is maintained without compromising privacy.

Lightweight Secure Auditing: For shared data in cloud storage, a lightweight secure auditing scheme can be implemented. This scheme introduces a Third Party Auditor (TPA) to conduct integrity checks and verify shared data. The TPA ensures that the auditing process is efficient and does not impose additional burdens on users, thereby enhancing both security and usability

These methods collectively enhance the security of cloud storage by addressing data integrity, privacy, and efficient sharing, making cloud services more reliable and trustworthy for users

V. CONCLUSION

we proposed an identity-based data integrity auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding. In our scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed. The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency to enhance the security and integrity of data stored in cloud environments. This project integrates identity-based auditing, which ensures that only authorized users can access and audit data, thereby maintaining privacy and traceability among group members.

Additionally, the project addresses the challenge of sharing

files containing sensitive information by proposing methods to hide this sensitive data while still allowing the file to be shared and used by others.

By doing so, it ensures that data integrity can be verified without exposing confidential information. Furthermore, the project explores the use of third-party auditors (TPAs) to independently verify the integrity of data stored in cloud storage, thereby providing an additional layer of security.

The proposed solutions aim to balance the need for secure data sharing with the necessity of maintaining data integrity and confidentiality, making cloud storage a more secure and reliable option for users.

VI. REFERENCES

[1]. K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.

[2]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

[3]. A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 584–597.

[4]. H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryp tol., vol. 26, no. 3, pp. 442–483, Jul. 2013.

[5]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[6]. S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, 2014.

[7]. C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric key based proofs of retrievability supporting public verification," in Computer Security—ESORICS. Cham, Switzerland: Springer, 2015, pp. 203–223.

[8]. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," J. Netw. Comput. Appl., vol. 82, pp. 56–64, Mar. 2017.

[9]. .J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, June 2010.

[10]. G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik, "Sanitizable signatures," in *Proc. 10th Eur. Symp. Res. Comput. Secur*. Berlin, Germany : Springer-Verlag, 2005, pp. 159–177.

[11]. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 213–222.

[12]. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.