Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

Secure Group Management Enables Privacy-Preserving Public Auditing for Shared Cloud Data

K. Jaya Krishna 1, Nerella Varun Kumar 2

#1Associate professor in the department of MCA at Qis College of Engineering and Technology (Autonomous), Vengamukkapalem, Prakasam (DT)
#2MCA Student in the department of MCA at Qis College of Engineering and Technology(autonomous), Vengamukkapalem, Prakasam (DT)

ABSTRACT_ Users can keep their data in the cloud and easily access it from anywhere at any time with cloud storage services. However, because consumers no longer have direct access to their data when it is kept in the cloud, there is a risk of data loss. Numerous cloud storage auditing techniques have been researched as a solution to this issue. A public auditing system for shared data was put up by Tian et al. in 2019 and enables data privacy, identity traceability, and group dynamics. We note in this study that their system is vulnerable to tag forgery or proof forgery attacks, which means that even if the cloud server has destroyed certain outsourced data, it can still produce reliable evidence that the server had correctly saved the data. Then, we suggest a brand-new design that offers the same features and is safe against the aforementioned threats. In addition, we compare the outcomes' calculation and communication costs to those of competing systems.

1.INTRODUCTION

Cloud storage provides users with significant storage capacity and advantages such as a cost reduction, scalability, and convenient access to the stored data. Therefore, cloud storage that is managed and maintained by professional cloud service providers (CSPs) is widely used by many enterprises and personal clients [1]. Once the data are stored in cloud storage, the clients lose direct control over the stored files. Despite this, the CSPs must ensure that the client data are placed in cloud storage without any modification or substitution. The simplest way to achieve this is by checking the integrity of the stored data after downloading. When the capacity of the stored data is large, it is quite inefficient, and thus many methods for verifying the integrity of the data stored in the cloud without a full download have been proposed [2]–[34]. These techniques are called cloud storage auditing and can be classified into private auditing and public auditing according to the subject of the integrity verification. In private auditing, verification is achieved

by users who have ownership of the stored data. Public auditing is conducted by a third-party auditor (TPA) on behalf of the users to reduce their burden, and thus public auditing schemes are more widely employed for cloud storage auditing. Public auditing schemes provide various properties depending on the environment, such as privacy preservation [5]–[9], data dynamics [10]–[13], and shared data [14]–[33]. Privacy-preserving auditing is used to conduct an integrity verification while protecting data information from the TPA, and dynamic data auditing is where legitimate users are free to add, delete, or change the stored data. Shared data auditing means freely sharing data within a legitimate user group. In this case, a legitimate user group should be defined, and user addition and revocation should be carefully considered. Recently, schemes that satisfy identity traceability, a concept that can trace the abnormal behaviour of legitimate users in shared data auditing, have also been proposed. Tian et al. [25] proposed a scheme that supports privacy preservation, data dynamics, and identity traceability in shared data auditing. For efficient user enrolment and revocation, the authors adopted the lazy revocation technique. Moreover, to secure the design against collusion attacks between the revoked user and server, they apply a technique in which the group manager manages messages and tag blocks generated by the revoked user to the scheme. Because the lazy-revocation technique is applied to the scheme, even if a user is revoked, no additional operation occurs until additional changes are made to the block.

2.LITERATURE SURVEY

2.1 Paper Title: Privacy-Preserving Public Auditing for Secure Cloud Storage

Authors: Wang, C. et al.

Publication Venue: IEEE Transactions on Computers

Year: 2013

Abstract: This paper proposes a privacy-preserving public auditing scheme for secure cloud storage. The scheme allows a third-party auditor to verify the integrity of outsourced data on behalf of multiple users without learning the actual data content. It employs a random masking technique to hide data contents during the auditing process, ensuring data privacy. The proposed scheme provides efficient data integrity verification and privacy preservation, making it suitable for secure cloud storage applications.

2.2 Paper Title: Privacy-Preserving Public Auditing for Shared Data in Cloud Storage

Authors: Zhu, Y. et al.

Publication Venue: IEEE Transactions on Computers

Year: 2014

Abstract: This research presents a privacy-preserving public auditing scheme for shared data in cloud storage. The scheme enables multiple users to securely store and audit shared data while preserving data privacy. It utilizes a novel dynamic accumulator and a zero-knowledge proof technique to allow efficient data integrity verification without revealing the actual data. The proposed scheme achieves secure and efficient auditing for shared cloud data, making it suitable for collaborative applications.

2.3 Paper Title: Privacy-Preserving Public Auditing for Secure Group Data Sharing in the Cloud

Authors: Yang, X. et al.

Publication Venue: Journal of Network and Computer Applications

Year: 2015

Abstract: This paper addresses the privacy-preserving public auditing problem for secure group data sharing in the cloud. The proposed scheme enables a group of users to jointly store and audit their shared data in the cloud while preserving data privacy. It employs a novel privacy-preserving signature scheme and a multi-level auditing mechanism to achieve secure and efficient auditing without exposing sensitive data. Experimental results demonstrate the effectiveness and efficiency of the proposed scheme for secure group data sharing in the cloud.

2.4 Paper Title: Privacy-Preserving Public Auditing with Secure Group Management for Cloud Storage

Authors: Sun, S. et al.

Publication Venue: Future Generation Computer Systems

Year: 2016

Abstract: This research presents a privacy-preserving public auditing scheme with secure group management for cloud storage. The scheme allows multiple users to securely store and audit their data in the cloud while ensuring data privacy. It utilizes a novel group signature scheme and a secure group management protocol to achieve efficient auditing and secure group membership management. The proposed scheme provides robust data integrity verification and privacy preservation for cloud storage with secure group management.

3.PROPOSED SYSTEM

1. We demonstrate that Tian et al.'s approach [25] is vulnerable to both tag forgeries and proof forgeries. We demonstrate tag forgery, where an attacker can produce a legitimate tag for the altered message without being aware of any secret information. We demonstrate proof forging in which an attacker can produce a legitimate proof for a challenged message even if some cloud-stored files have been erased.

2. We create a brand-new public auditing system with the same functions as the previous one—privacy protection, data dynamics, data sharing, and identity tracing—but that is secure against the aforementioned threats. We modified the data proof generating approach to improve privacy preservation and the tag generation method to get rid of the malleable property. In order to safeguard the confidential information from the CSP, we also modified the lazy revocation procedure and put forth a flexible active revocation approach.

3. We formally establish the suggested scheme's security. The theorems state that the attacker is unable to produce a valid proof or tag without first knowing the secret values or the original communications, respectively. In terms of computing and communication costs, we also present comparative findings with other methods.

3.1 IMPLEMENTATION

Data Owner

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud.

CSP

The cloud service provider manages a cloud to provide data storage service. And cloud can monitor all the actions

Private key generator

In this module private key generator will generate private key for user based on user request by using that secret user can download data.

Data disseminator

Data disseminator is the person who wishes to share data owner's data with other people (e.g., his friends, family members, colleagues). For security and access control considerations, data disseminator must be one of intended receivers defined by the data owner, who could decrypt the initial ciphertexts. The data disseminator can generate reencryption keys, and then send data re-encryption requests with these keys to the CSP to disseminate data owner's data to others. Only the attributes of data disseminator satisfy access policy and the pre-determined time arrives, data re-encryption request can be successfully executed by CSP.

Data Consumer/End User

In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. Users may try to access data files either

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

within their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. He is sending request to private key generator and data disseminator for data access after getting permission then user can download encrypted data.

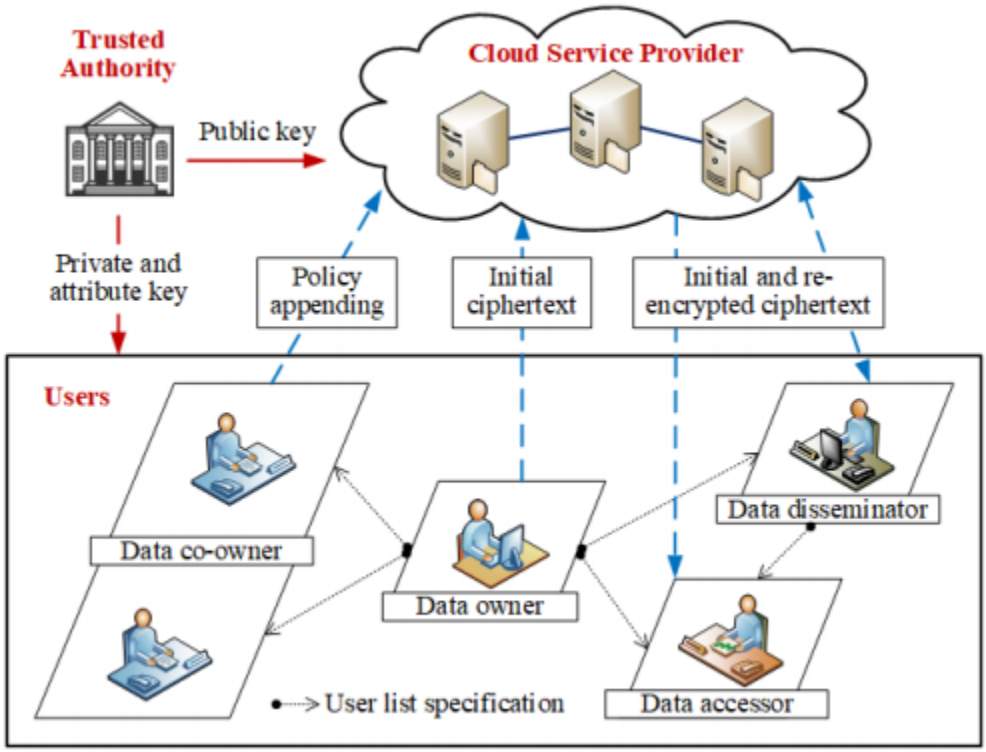

Fig 1: Architecture

4.RESULTS AND DISCUSSION

Table 1: Comparisons of computation cost

Schemes	Tag generation	Proof verification
[16]	$1Mul_{\mathbb{G}_1}+2Exp_{\mathbb{G}_1}+1hash_{\mathbb{G}_1}+2Pair$	$(c+2d)Mul_{\mathbb{G}_1}+(c+d)Exp_{\mathbb{G}_1}+chash_{\mathbb{G}_1}+dMul_{\mathbb{G}_T}+(d+1)Pair$
[19]	$sMul_{\mathbb{G}_1}+(s+2)Exp_{\mathbb{G}_1}+1hash$	$(c+1)Mul_{\mathbb{G}_1}+6Exp_{\mathbb{G}_1}+chash+2Mul_{\mathbb{G}_T}+3Pair$
[25]	$1Mul_{\mathbb{G}_1}+3Exp_{\mathbb{G}_1}+1hash$	$(\lvert IDX\rvert+\lvert D\rvert+4)Mul_{\mathbb{G}_1}+2Exp_{\mathbb{G}_1}+(\lvert IDX\rvert+\lvert D\rvert)hash+2Mul_{\mathbb{G}_T}+3Exp_{\mathbb{G}_T}+1Pair$
Ours	$1Mul_{\mathbb{G}_1}+2Exp_{\mathbb{G}_1}+1hash_{\mathbb{G}_1}$	$(\lvert IDX\rvert+\lvert D\rvert+6)Mul_{\mathbb{G}_1}+(\lvert IDX\rvert+\lvert D\rvert+2)Exp_{\mathbb{G}_1}+(\lvert IDX\rvert+\lvert D\rvert)hash_{\mathbb{G}_1}+2hash+2Mul_{\mathbb{G}_T}+6Exp_{\mathbb{G}_T}+2Pair$

Note: $Mul_{\mathbb{G}_1}$ denotes one multiplication in $\mathbb{G}_1$, $Exp_{\mathbb{G}_1}$ denotes one exponentiation in $\mathbb{G}_1$, *hash* denotes one hashing operation in $\mathbb{G}_1$, $Mul_{\mathbb{G}_T}$ denotes one multiplication in $\mathbb{G}_T$, $Exp_{\mathbb{G}_T}$ denotes one exponentiation in $\mathbb{G}_T$, and *Pair* denotes one pairing operation in $e:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_T$. In addition, c and $|IDX|$ are the number of challenged blocks, d and s are the number of subsets of the challenged blocks, and $|D|$ is the number of data blocks modified by the revoked users.

4.1 EFFICIENCY ANALYSIS

In this part, we contrast our proposed plan and Panda [16]-[19] and Tian et al. 's conspire (PASCD) [25] as far as the calculation and correspondence costs. 1) Calculation COST We first think about the computational intricacy of every one of the four plans in the label age and confirmation check stages. In the label age stage, from Table 2, [19] has the most elevated calculation costs, which is sMulG1 +(s+2) ExpG1 +1hash. PASCD [25] and our plan have lower calculation costs than Panda [16] on the grounds that they don't need matching oper ations. During the evidence confirmation stage, Panda [16] has the most elevated calculation costs, i.e., (c + 2d)MulG1 + (c + d)ExpG1 + chashG1 + dMulGT + (d + 1)Pair, as d increments, though PASCD [25] and our plan play out a steady matching activity no matter what the size of d. Contrasting our plan and [19] and PACSD [25], our plan has a marginally higher calculation cost; notwithstanding, definitively, it tackles the security issue of PASCD [25] with practically a similar computational expense.

5.CONCLUSION

The issue of guaranteeing the integrity of stored data in cloud storage can be solved using the crucial approach of cloud storage auditing. Numerous schemes with various functionalities and security levels have been presented since there is a widespread need for the concept. A strategy that enables data privacy, identity traceability, and group dynamics was developed by Tian et al. [25] in 2019. They asserted that their scheme is secure against cooperation attacks between the CSPs and revoked users. In this work, we demonstrated how a tag may be created from a legal message and tag pair without the knowledge of any secret information using their approach. We also demonstrated how a collusion attack can be used to fabricate a proof, even when some of the disputed communications have been removed. Then, we suggested a brand-new design that offers the same functionality as their strategy while being safe from the aforementioned threats. Additionally, we offered explicit security justifications and a comparison of both techniques' computation costs

REFERENCES

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598–609.

[3] A. Juels and B. S. Kaliski, ‘‘PORs: Proofs of retrievability for large files,’’ in

Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Oct. 2007, pp. 584–597.

[4] H. Shacham and B. Waters, ‘‘Compact proofs of retrievability,’’ in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Berlin, Germany: Springer, 2008, pp. 90–107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy-preserving public auditing for data storage security in cloud computing,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[6] Z. Hao, S. Zhong, and N. Yu, ‘‘A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability,’’ IEEE Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432–1437, Sep. 2011.

[7] K. Yang and X. Jia, ‘‘An efficient and secure dynamic auditing protocol for data storage in cloud computing,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

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

[9] K. He, C. Huang, K. Yang, and J. Shi, ‘‘Identity-preserving public auditing for shared cloud data,’’ in Proc. IEEE 23rd Int. Symp. Quality Service (IWQoS), Jun. 2015, pp. 159–164.

[10] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, ‘‘Dynamic provable data possession,’’ in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2009, pp. 213–222.

[11] 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.

[12] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, ‘‘Dynamic

audit services for outsourced storages in clouds,’’ IEEE Trans. Services Comput., vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.

[13] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ‘‘An efficient public auditing protocol with novel dynamic structure for cloud data,’’ IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

[14] B. Wang, B. Li, and H. Li, ‘‘Knox: Privacy-preserving auditing for shared data with large groups in the cloud,’’ in Proc. 10th Interfaces Conf. Appl. Crypto. Netw. Secur., 2012, pp. 507–525.

[15] B. Wang, B. Li, and H. Li, ‘‘Oruta: Privacy-preserving public auditing for shared data in the cloud,’’ IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan./Mar. 2014.

[16] B. Wang, B. Li, and H. Li, ‘‘Panda: Public auditing for shared data with efficient user revocation in the cloud,’’ IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.

[17] T. Jiang, X. Chen, and J. Ma, ‘‘Public integrity auditing for shared dynamic cloud data with group user revocation,’’ IEEE Trans. Comput., vol. 65, no. 8, pp. 2363–2373, Aug. 2016.

[18] J. Yuan and S. Yu, ‘‘Efficient public integrity checking for cloud data sharing with multi-user modification,’’ in Proc. IEEE Conf. Comput. Commun.(IEEE INFOCOM), Apr. 2014, pp. 2121–2129

AUTHOR PROFILE

Mr. K. Jaya Krishna completed his master of technology (M.tech) in CSE, Currently working as an associate professor in the department of Master of Computer Applications at QIS college of engineering and technology.

Mr. N. Varun Kumar as MCA Student in the Department of Qis College of engineering and Technology (autonomous), Vengamukkapalem, Prakasam (DT). Areas of Interests are Networks & Cloud Computing.