ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

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

[1]MR.A N L KUMAR, [2]BONTHU MOHANASAI

[1](Assistant Professor), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

ABSTRACT

The cloud storage services, customers can easily store their data in the cloud and access it efficiently from any location at any time. Since users no longer physically own their files when they save them in the cloud, data loss is a real possibility. In an attempt to tackle this problem, cloud storage auditing techniques have been thoroughly investigated. Tian et al. (2019) proposed a public auditing system for shared data to support data privacy, identity traceability, and group dynamics. Our research shows that their system is susceptible to assaults like tag forgery and proof fabrication. This means that their proof-generating powers may be used to prove, even after data deletion, that the cloud server had really stored the data. Next, we provide an alternate approach that avoids these dangers while maintaining the same functionality. We also compare the results to other approaches that take communication and computation costs into account.

1. INTRODUCTION

Significant storage space, cost reduction, scalability, and easy access to stored data are just a few of the benefits that customers enjoy with cloud storage. In light of this, many businesses and individuals rely on cloud storage that is overseen and maintained by CSPs [1]. Customers no longer have immediate access to their data after it is saved in the cloud. Regardless, CSPs are still responsible for protecting their clients' data when they upload it to the cloud and make sure nothing changes there. Verifying the data's integrity after

downloading is the quickest and easiest method to do this. It becomes very wasteful when the amount of data saved is huge, hence numerous ways for checking the data's integrity in the cloud without downloading it all have been suggested [2]_[34]. Cloud storage auditing refers to these methods, which may be categorized as either public or private auditing based on the topic of the integrity verification. Users who are the legal proprietors of the data are the ones who do the verification in private auditing. More and more cloud storage auditing schemes utilize public auditing, in which a third-party auditor (TPA) performs the audit on behalf of the customers to lighten their load. When it comes to auditing shared data, Tian et al. [25] suggested a system that helps with privacy protection, data dynamics, and identity tracing. The authors chose for the lazy revocation method for quick user registration and revocation. In addition, they provide a method where the group manager oversees the revoked user's messages and tag blocks to protect the design against collusion assaults involving the server. Even after a user is revoked, the scheme will not execute any more operations because to the lazy-revocation mechanism. This ensures that no further modifications to the block are necessary. This study presents a new strategy that offers the same functionality while being safe against the aforementioned attacks. It is shown that Tian et al.'s system [25] is vulnerable to tag forgery and proof fabrication. In this approach, a tag forgery may be executed by taking use of the tag's malleability, and a proof forgery can be executed by taking advantage of the secret value that is revealed to the server when further modifications are made to the block after the user's revocation. V. Here is a high-level overview of the study's contributions: Two kinds of attacks, tag forgeries and proof forgeries, render Tian et al.'s approach [25] vulnerable. Using tag forging, we demonstrate that an adversary may legitimately tag the altered message even in the absence of knowledge of the secret values. We demonstrate in the proof forgeries that an adversary may construct a legitimate proof for the supplied challenged message despite the deletion of certain _les kept in the cloud. Along with the same features—privacy preservation, data dynamics, data sharing, and identity

traceability—we create a new public auditing scheme that is safe against the aforementioned assaults. We improved privacy preservation by changing the data proof generating approach and removed the malleable property from the tag generation method. In order to prevent the CSP from gaining access to sensitive information, we revised the lazy revocation process and suggested an active revocation procedure that can be applied to different contexts with ease. Here is how the remainder of this paper is structured. We lay out the context in Section II, and then examine the plan put forward by Tian et al. [25] in Section III.In Section IV, we lay out our comprehensive plan for public auditing, and in Section V, we guarantee that our plan is both secure and efficient. In Section VI, we wrap up this paper.

2. LITERATURE SURVEY

The proposed public cloud audit scheme appears to address several critical concerns in UAV data management, including dynamic data updates, privacy protection, and efficient auditing. Let's break down the key components and benefits of the proposed scheme

Title: Unmanned Aerial Vehicles' Dynamic Data Supporting a Privacy-Preserving Public Cloud Audit Scheme

- TPS stands for Third-Party Server: customers' local computer resources are relieved by introducing a TPS between cloud service providers and customers. Users see a decrease in computing cost due to TPS's facilitation of digital signatures, integrity checking, and dynamic data operations.

- Data Encryption: Data uploaded by UAVs is encrypted before transmission to the TPS, ensuring privacy and security during data transfer.

- Distributed String Equality Check Protocol: This protocol enhances security by enabling the TPS to perform signature operations on encrypted data. To further fortify the system's defenses, it restricts access to cloud servers to authorized TPS with time limitations.

Title: An Authorization and Traceability-Based Privacy-Preserving Cloud Auditing Scheme for Multiple Users

➢ Certificateless Signature Technology: Without depending on group signature or ring signature methods, the approach guarantees user identity anonymity by using certificateless signing technology. This approach helps keep the tag compact while still preserving user privacy.

➢ Authorization and Traceability: The approach allows for numerous authorized users with traceability, so at least d managers may work together to find the identities of bad actors. This feature prevents single-manager abuse of power and provides non-frameability, enhancing the security of the system.

Title: Sanitizable Signatures

➢ Security Features: Sanitizable signatures offer several attractive security features, including the ability to restrict modifications to authorized entities, ensuring controlled and limited changes to the signed data. This helps maintain data integrity and authenticity while allowing for necessary modifications.

➢ Construction: The proposed constructions for sanitizable signatures are based on standard signature schemes and rely on common cryptographic assumptions. This ensures compatibility with existing cryptographic protocols and enhances the practicality of implementation.

3.EXISTING SYSTEM

First proposed by Ateniese et al. [2], PDP is a proved data possession technique that makes use of homomorphic authenticators based on RSA. Two provably secure PDP algorithms were offered by them. Less communication and processing expenses are supported by this, which helps with public verification. Meanwhile, a sentinel-based POR technique with certain qualities was first presented by Juels et al. [3], along with the idea and formal security model of proof of retrievability (POR). Subsequently, Shacham et al. [4] enhanced the POR technique and introduced a novel public auditing system that is safe in the random oracle model and is constructed from the BLS signature [36]. Data privacy preservation, data dynamics, and shared data are just a few of the numerous features that have been the subject of cloud storage auditing's many recent research.

The PDP approach, which supports data dynamics via the use of a rank- based authenticated skip list, was first suggested by Erway et al. [10]. In response to the technique's high communication and computational costs, Wang et al. [11] introduced a new, easier auditing scheme based on the Merkle Hash Tree (MHT). Wang et al. [5] suggested a public auditing system that protects individuals' privacy, however their method is expensive in terms of computation and communication while updating data or conducting audits. An additional authenticated data structure, the index hash table (IHT), was suggested by Zhu et al. [12] as a means to facilitate data dynamics in their novel approach. This method was effective in decreasing computing and communication costs, but it failed to address the inefficiency of lookup and updating processes. A novel, efficient technique using a location array and a doubly linked information table was presented by Shen et al. [13]. Dynamic hash tables (DHTs) were suggested by Tian et al. [25] as a more effective strategy for data updating than IHTs [12]. Protecting personal information, Wang et al.

Disadvantages

➢ An existing system, the system doesn't have data auditing techniques to find data verification.

➢ The system doesn't have Dynamic Hash tables to maintain the blocks

3.1 PROPOSED SYSTEM

Two kinds of attacks, tag forgeries and proof forgeries, render Tian et al.'s approach [25] vulnerable. Using tag forging, we demonstrate that an adversary may legitimately tag the altered message even in the absence of knowledge of the secret values. Even if certain files saved on the cloud are destroyed, an attacker may still provide an acceptable evidence for the challenged message via proof forgery.

Along with the same features—privacy preservation, data dynamics, data sharing, and identity traceability—we create a new public auditing scheme that is safe against the aforementioned assaults. We improved privacy preservation by changing the data proof generating approac and removed the malleable property from the tag generation method. In order to prevent the CSP from gaining access to sensitive information, we revised the lazy revocation process and

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

suggested an active revocation procedure that can be applied to different contexts with ease. We provide formal proof that the suggested system is secure. It is impossible for an attacker to create a legitimate tag or proof without knowledge of the secret values or original messages, respectively, as stated in the theorems. Additionally, we provide data comparing our method to others in terms of communication and computing costs. The Benefits

➢ The suggested solution employs an extended dynamic hash table (EDHT) for the purpose of managing data blocks processed by revoked users.

➢ The group manager records activities for each block in the modification record table (MRT), a two-dimensional data structure that provides identity traceability, in the proposed system.

4. RESULTS

Home:

User Login:

Cloud:

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

Data Service Manager:

Trusted Authority:

5.CONCLUSION

One critical approach to guaranteeing the authenticity of data kept in the cloud is cloud storage auditing. Various solutions with varying degrees of security and functionality have been suggested because to the widespread demand for the notion. Claiming their approach is safe against cooperation attacks between CSPs and revoked users, Tian et al. [25] presented a solution in 2019 that provides data privacy, identity traceability, and group dynamics. Using their technique, we demonstrated in this work that it is possible to create a fake

tag using a legitimate message and tag combination, even without knowledge of the secret values. Even after deleting certain disputed communications, we demonstrated that a proof may still be using a collusion assault. Following this, we presented an alternative strategy that is both functionally equivalent to theirs and safe against the aforementioned threats. In addition, we analyzed the computational costs of both techniques and offered formal security proofs.

6. REFERENCE

[1] (Apr. 2021). *Cloud Storage-Global Market Trajectory and Analyt- ics*. [Online]. Available:https://www.researchandmarkets.com/reports/5140992/cloud-storage-global-market-trajectory-and

[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 _les," 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 veri_ability," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 9, pp. 1432_1437, Sep. 2011.

[7] K. Yang and X. Jia, ``An ef_cient 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, ``Privacy preserving 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 ef_cient 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 ef_cient 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, ``Ef_cient public integrity checking for cloud data sharing with multi-user modi_cation," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2014, pp. 2121_2129.

[19] J. Yuan and S. Yu, ``Public integrity auditing for dynamic data sharing with multiuser modi_cation," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1717_1726, Aug. 2015.

[20] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ``Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," *J. Syst. Softw.*, vol. 113, pp. 130_139, Mar. 2016.

[21] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, ``NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users," *IEEE Trans. Big Data*, vol. 8, no. 1, pp. 14_24, Feb. 2022, doi: 10.1109/TBDATA.2017.2701347.

[22] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ``Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 331_346, Feb. 2018.

[23] Y. Zhang, C. Chen, D. Zheng, R. Guo, and S. Xu, ``Shared dynamic data audit supporting anonymous user revocation in cloud storage," *IEEE Access*, vol. 7, pp. 113832_113843, 2019.

[24] G. Wu, Y. Mu, W. Susilo, F. Guo, and F. Zhang, ``Threshold privacy preserve in cloud auditing with multiple uploaders," *Int.*

J. Inf. Secur., vol. 18, no. 3, pp. 321_331, Jun. 2019.

[25] H. Tian, F. Nan, H. Jiang, C.-C. Chang, J. Ning, and Y. Huang, ``Public auditing for shared cloud data with ef_cient and secure group management," *Inf. Sci.*, vol. 472, pp. 107_125, Jan. 2019.