A Lightweight Secure Auditing Scheme For Shared Data In Cloud Storage

Sayyad Mathin, Sri.G.Ramesh Kumar, Sri.V.Bhaskara Murthy
Mca Student, Assistant Professor, Associate Professor
Dept Of Mca
B.V.Raju College, Bhimavaram

ABSTRACT
A cloud platform provides users with shared data storage services. To ensure shared data integrity, it is necessary to validate the data effectively. An audit scheme that enables group members to modify data conducts the integrity verification of the shared data, but this approach results in complex calculations for the group members. The audit scheme of the designated agent implements a lightweight calculation for the group members, but it ignores the security risks between the group members and the agents. By introducing Hashgraph technology and designing a Third Party Medium (TPM) management strategy, a lightweight secure auditing scheme for shared data in cloud storage (LSSA) is proposed, which achieves security management of the groups and a lightweight calculation for the group members. Meanwhile, a virtual TPM pool is constructed by combining the TCP sliding window technology and interconnected functions to improve agent security. We evaluate our scheme in numerical analysis and in experiments, the results of which demonstrate that our scheme achieves lightweight computing for the group members and ensures the data verification process for security.

I. INTRODUCTION

Cloud computing is a new computing mode that was created after peer-to-peer computing, grid computing, utility computing and distributed computing. The core concept of cloud computing is resource renting, application hosting and service outsourcing [1]. Through virtualization technology, it forms distributed computing nodes into a shared virtualization pool in order to provide services for users. With cloud computing technology, users and enterprises do not need to spend much on the acquisition and maintenance of hardware in their early stages.

In addition, powerful computing and storage capabilities also make users more willing to rely on the cloud to handle a variety of complex tasks. When users choose to deploy a large number of applications and data to the cloud computing platform, the cloud computing system accordingly becomes the cloud storage system. Cloud storage systems give users mass storage capacity at a relatively low price, and provide a platform for sharing data between users (data sharing means that a user in a group uploads data to the cloud, and the rest of the group can access/modify the data) [2]. However, highly centralized computing resources means cloud storage faces severe security challenges..

According to a survey conducted by Gartner in 2009, 70% of CEOs of surveyed companies refused to adopt cloud computing models on a large scale due to concerns about the privacy of cloud data. Furthermore, in recent years the security storage problem exposed by cloud operators has aroused people's concern. For example, in March 2011, Google Gmail failed, which caused data loss to approximately 150,000 users. In the same year, Amazon's enormous EC2 cloud service crashed, permanently destroying some users' data. While

the data loss was apparently small relative to the total amount of data stored, anyone who runs a website can immediately understand the horrible level of data loss [3]. Thus, the secure storage of data in the cloud has hindered the large-scale use of cloud computing in the IT field [4]. To achieve the secure storage of cloud data, researchers have developed the cloud data integrity verification scheme

II. EXISTING SYSTEM

In a subsequent study, Ateniese et al. implemented a PDP scheme that supports dynamic operations, which means that the data uploader has full control over any operation performed on the cloud data, including block deletion, modification, and insertion. Then, Waters et al. proposed a full-dynamic PDP scheme by utilizing the authenticated flip table.

In 2016, Yang et al. proposed a BLS-based signature scheme supporting flexible management in the group. Jiang et al. proposed data integrity based on the vector commitment technique, which is resistant to collusion attacks of a cloud service provider and a group member. By combining proxy cryptography with the encryption technique, in 2017 Luo et al. proposed a scheme with secure user revocation. Recently, Huang et al. realized efficient key distribution within groups based on the logical hierarchy tree, thereby protecting the identity privacy of the group members. Huang et al. subsequently proposed a certificate less audit scheme by eliminating key escrow, which further improved the user's privacy security [13]. Following Huang et al.'s pioneering work. Fu et al. proposed an audit scheme that can restore the latest correct shared data blocks by changing the binary tree tracking data in the group.

Li et al. proposed a new cloud storage auditing scheme with a cloud audit server and a cloud storage server. The cloud audit server generates authentication labels for users before uploading them to the cloud storage server. Although this scheme can reduce users' computation overhead, it fully reveals the user's private key and the user's data to the cloud audit server. As a result, malicious cloud service providers can pass the verification process without storing the user's data. Guan et al. used an indistinguishable confusing approach to build an audit scheme for cloud storage, thereby reducing the time that is required to generate authentication labels but increasing the time to verify the integrity of the cloud data.

Wang et al. introduced agents to assist group members in generating authentication labels and auditing data integrity, which alleviated the computational burden for group members. However, in order to guarantee data privacy, the group member needs to encrypt the data before sending them to the proxy, which inevitably increases the computational burden. Shen et al. proposed a lightweight audit scheme by introducing the Third Party Medium (called the agent) to replace group members with generating authentication labels. Different from Wang et al.'s scheme, the scheme uses blind data instead of encrypted data to generate authentication labels,further reducing the computational burden on the group members.

Disadvantages

- In the existing work, the system is less effective due to the cloud audit server generates authentication labels for users before uploading them to the cloud storage server.
- The system has less security while working with data verification from external attackers.

III. PROPOSED SYSTEM

The system is proposed by introducing an efficient blind method, this paper ensures the data privacy and identity privacy of the group members. By introducing a Hash graph, this paper avoids the hidden security risks of group

members, and simultaneously makes the user identity traceable.

The TPM management strategy is designed, and the virtual TPM pool is built by the group manager. The strategy ensures the security of agent (TPM) and results in lightweight calculations for the agent. Using the TPM instead of group members to calculate the authentication label and audit data integrity results in lightweight calculations for the group members.

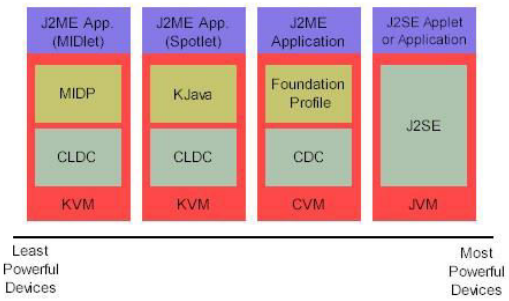
The security analysis of the scheme shows that the scheme is safe and can resist both replace attacks and replay attacks.

The experimental evaluation of the scheme shows that the scheme can achieve lightweight calculations for group members and the TPM.

Advantages

- To solve existing system challenging problems, The system proposed an effective a lightweight secure auditing scheme for shared data in cloud storage (LSSA).
- Identity traceability: The modification of data by illegal group members may lead to disputes among the group members using the same shared data.

IV. SYSTEM ARCHITECTURE



V. IMPLEMENTATION

MODULES

Data Owner:

In this module, the data provider uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations My Profile, Upload Files, View All Uploaded Files, Verify Block(Integrity Of Cloud Data).

Cloud Server: The Cloud server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers and performs the following operations such as View Files, View Download Request, View All Transactions, View Attackers, View Time Delay Result, View Throughput Results.

Group Member:

In this module, the member can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and can do the following operations like My Profile, Search File, Request Download.

TPM:

In this module, the TPM performs the following operations such as View All Data Owners and Authorize, View All End Users and Authorize, View File Details.

VI. CONCLUSION

In this paper, we proposed a provable shared data possession for a lightweight and security audit process in cloud storage. By introducing a Hash graph, the traceability of group membership is achieved, and the illegal behavior of group members can be contained through Hash graph technology. By specifying multiple TPMs for calculation and management according to the TPM management strategy,

each group member and each TPM are independent of one another, which ensures that the cloud data verification process is secure and achieves a lightweight calculation of the TPM. Through a security analysis, the scheme in this paper can avoid replay attacks and replace attacks while protecting the identity privacy and data privacy of group members and ensuring secure storage of the shared data. Therefore, this scheme has important significance and value for the secure storage of shared data.

REFERENCES

Appl. Cryptol. Inf. [1] M. Armbrust et al., ``Above the clouds: A Berkeley view of cloud comput-ing," Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, Berkeley,CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009. [Online].Available:https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[2] P. Mell and T. Grance, ``The National Institute of Standards and Technol-ogy (NIST) denition of cloud computing," NIST, Washington, DC, USA,NIST Special Publication 800-145, 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[3] K. Julisch and M. Hall, ``Security and control in the cloud," Inf. Secur.J. Global Perspective, vol. 19, no. 6, pp. 299_309, 2010.

[4] D. G. Feng, M. Zhang, Y. Zhang, and Z. Xu, ``Study on cloud computing security," J. Softw., vol. 22, no. 1, pp. 71_83, 2011.

[5] G. Ateniese et al., ``Provable data possession at untrusted stores," in Proc.14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598_609.

[6] A. Juels and B. S. Kaliski, ``Pors: Proofs of retrievability for large_les," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 584_597.

[7] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, ``Scalable and ef_cient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw. (ICST), Istanbul, Turkey, 2008, pp. 22_25.

[8] H. Shacham and B. Waters, ``Compact proofs of retrievability," in Proc.Int. Conf. Theory Secur. Berlin, Germany: Springer, 2008, pp. 90_107.

[9] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ``Enabling public auditing for shared data in cloud storage supporting iden-tity privacy and traceability," J. Syst. Softw., vol. 113, pp. 130_139,Mar. 2016. doi: 10.1016/j.jss.2015.11.044.

[10] 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. doi: 10.1109/TC.2015.2389955.

[11] Y. Luo, M. Xu, K. Huang, D. Wang, and S. Fu, ``Ef_cient auditing for shared data in the cloud with secure user revocation and computa-tions outsourcing," Comput. Secur., vol. 73, pp. 492_506, Mar. 2018. doi: 10.1016/j.cose.2017.12.004.

[12] L. Huang, G. Zhang, and A. Fu, ``Privacy-preserving public audit-ing for dynamic group based on hierarchical tree," J. Comput. Res. Develop., vol. 53, no. 10, pp. 2334_2342, 2016. doi: 10.7544/issn1000-1239.2016.20160429.

[13] L. X. Huang, G. M. Zhang, and A. M. Fu, ``Certi_cateless public veri_ca-tion scheme with

privacy-preserving and message recovery for dynamic group," in Proc. Australas. Comput. Sci. Week Multiconf., Melbourne, VIC, Australia, 2017, p. 76.

[14] 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, to be published. doi: 10.1109/TBDATA.2017.2701347.

[15] J. Li, X. Tan, X. Chen, D. S. Wong, and F. Xhafa, ``OPoR: Enabling proofN of retrievability in cloud computing with resource-constrained devices," IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 195_205, Apr. 2015. doi: 10.1109/TCC.2014.2366148.