As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(09): 134-137, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809027
Available online at: http://www.ijmtst.com/vol8issue09.html

A Simple, Safe Auditing System for Shared Cloud Storage

M.Hemanth Ravi Kumar [1] | P Srinivasa Reddy [2]

[1]Master of Computer Applications (MCA), SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
M.Hemanth Ravi Kumar and P Srinivasa Reddy. A Simple, Safe Auditing System for Shared Cloud Storage. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 134-137. https://doi.org/10.46501/IJMTST0809027

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

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.

KEYWORDS: Hash graph technology, Third Party Medium , lightweight computing , data integrity.

1. 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 . 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) . 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 . Thus, the secure storage of data in the cloud has hindered the large-scale use of cloud computing in the IT field . To achieve the secure storage of cloud data, researchers have developed the cloud data integrity verification scheme.

2. LITERATURE SURVEY

In 2007, Ateniese et al. first proposed a Provable Data Possession (PDP) model, which can verify the integrity of cloud data without retrieving all of the data [5]. Then, Juels et al. proposed the Proofs of Retrievability (POR) scheme, which enables a back-up or archive service to produce proof that the data can be retrieved by the verifier [6]. In a subsequent study, Ateniese et al. implemented a PDP scheme that supports dynamic operations [7], 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 [8].

Differing from these works, the following schemes [9]–[14] focus on how to audit the integrity of the shared data. In this scenario, users can easily modify and share data as a group with the cloud services, where every group member in the group is not only able to access and modify the shared data but also share the version that he/she has modified with the rest of the group [11].

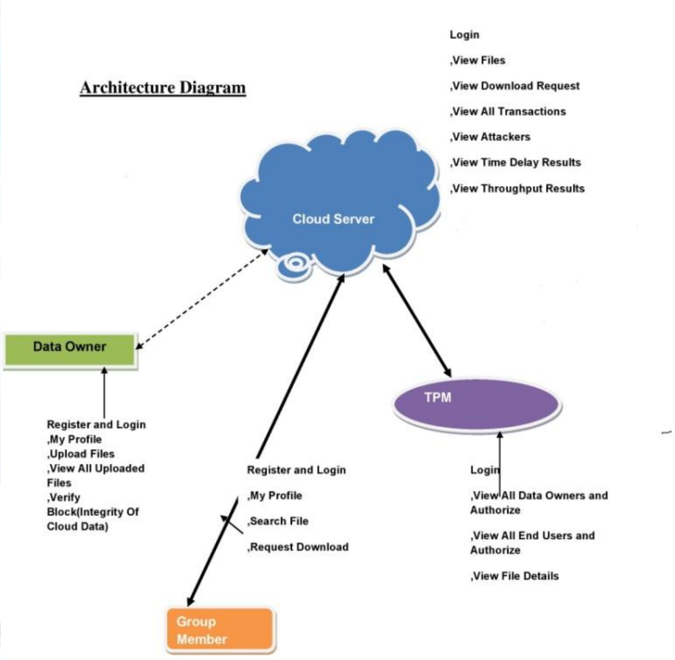
In 2016, Yang et al. proposed a BLS-based signature scheme supporting flexible management in the group [9]. Jiang et al. proposed data integrity based on the vector commitment technique, which is resistant to collusion attacks of a cloud service provider and a group member [10]. By combining proxy cryptography with the encryption technique, in 2017 Luo et al. proposed a scheme with secure user revocation [11]. 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 [12]. Huang et al. subsequently proposed a certificateless 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 [14].

In the above scheme [9]–[14], in order to verify the integrity of the shared data stored in the cloud, the group members need to block the data and then calculate the data authentication label for each block. Finally, the group member uploads the shared data along with the corresponding authentication labels to the cloud. The integrity verification of the shared data relies on the correctness of these data authentication labels. However, the cost of calculating the authentication label is generally great, because the formula requires a large number of exponentiations, e.g., when the block size is 2 KB, the authentication label generation overhead for a 10 GB file is nearly 18 hours. Therefore, it is necessary to propose a lightweight auditing scheme to reduce the resource utilization of users. Li et al. proposed a new cloud storage auditing scheme with a cloud audit server and a cloud storage server [15]. 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 [16], 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 [17], 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 [18]. 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. Although the scheme protects the data privacy and the identity privacy of group members in some ways, it does not consider the possibility of illegal access to shared data. Since the data of the malicious group member is also encrypted or blinded, it cannot be detected even after other people's data is randomly modified. What is even worse is that malicious group members can collude with agents for illegal profit.

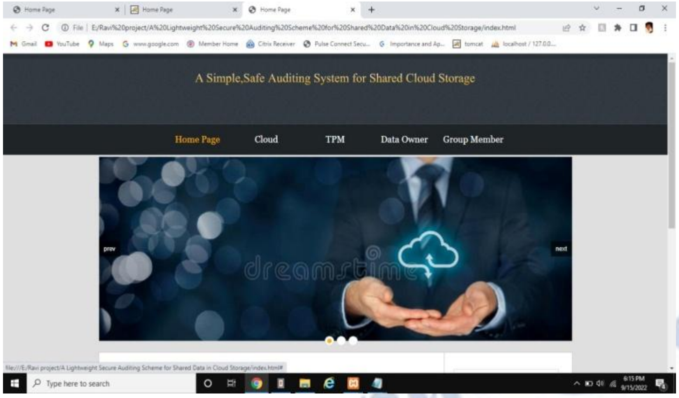
3.PROBLEM STATEMENT

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 certificateless audit scheme by eliminating key escrow, which further improved the user's privacy security . 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

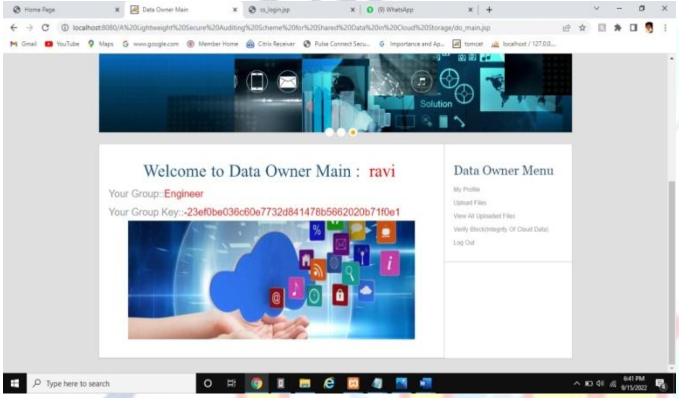
4. ARCHITECTURE



5. RESULTS


E:/Ravi%20project/A%20Lightweight%20Secure%20Auditing%20Scheme%20for%20Shared%20Data%20in%20Cloud%20Storage/index.html

A Simple,Safe Auditing System for Shared Cloud Storage


Welcome to Data Owner Main : ravi

Your Group::Engineer

Your Group Key::-23ef0be036c60e7732d841478b5662020b71f0e1

6. CONCLUSION

In this paper, we proposed a provable shared data possession for a lightweight and security audit process in cloud storage. By introducing a Hashgraph, the traceability of group membership is achieved, and the illegal behaviours of group members can be contained through Hashgraph 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.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] M. Armbrust et al., ''Above the clouds: A Berkeley view of cloud computing,'' Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009. [Online].

[2] P. Mell and T. Grance, ''The National Institute of Standards and Technology (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 files,'' 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 efficient 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 Appl. Cryptol. Inf. Secur. Berlin, Germany: Springer, 2008, pp. 90–

Authors Biography

M.Hemanth Ravi Kumar currently pursuing MCA in SVKP &Dr KS Raju Arts and Science College(A), Affiliated to Adikavi Nannaya Univesity ,Rajamahendravaram. His research interests include Data Structures, Operating Systems and Artificial Intelligence

P.Srinivasa Reddy is working as Associate Professor in SVKP &Dr K S Raju Arts & Science College, Penugonda, A.P. He received Masters Degree in Computer Applications from Andhra University. His research interests include Operational, Research ,Probability and Statistics , Design and Analysis of algorithm , Big Data Analytics