Secured Data Sharing for Cloud Group Users using Public Auditing Mechanism

[1]Miss. Deliya P. Dhargalkar , [2]Prof. G.M. Kadam

[1] *Deliya P. Dhargalkar. Student, Computer Engineering, SKN SIT'S Lonavala, Maharashtra, India*
[2]*G.M.Kadam. Guide, Computer Engineering, SKN SIT'S Lonavala, Maharashtra, India*

ABSTRACT

Cloud storage is widely used for sharing data due to low cost maintenance. But, it is also necessary to secure data on cloud. Secure Data Sharing in Cloud focuses mainly on: a)Data recovery b) privacy and confidentiality c) key management and encryption d) secure data sharing without re-encryption and e) forward and backward access control f) Prevention of data tampering. When user wants to share data, it sends request to trusted party that generates a symmetric key which is used to encrypt the data for sharing. This key is used to compute two key shares for trusted party and user. For security purpose, once a user is revoked from the group, the blocks which were formerly signed by this revoked user need to be re-signed by an current user. In this paper, we propose a new privacy-aware public auditing mechanism for shared cloud data by constructing a homomorphic verifiable group signature. Unlike the existing solutions, our scheme requires at least m group managers to restore a trace key unitedly, which wipe out the misuse of single-authority power and provides nonframeability. Our system provides the public checking and efficient user revocation facility and also some nice properties, such as confidently, efficiency, countability and traceability of secure group user revocation. We also present an extension of our proposed scheme that enables the TPA to operate multiple auditing tasks at the same time.. Finally ,the security and experimental analysis show that, compared with schemes our scheme is also secure and efficient.

Keyword : - *Cloud Data sharing, Data recovery, Data tampering, Security, Key management*

---

1. INTRODUCTION

Because of the expanding number of uses of shared information, for example, iCloud, Google Docs, et cetera, clients can transfer their information to a cloud and offer it with different associates as a gathering. Lamentably, since cloud servers are powerless against inescapable equipment flaws, programming disappointments or human mistakes, information put away in the cloud might be ruined or lost [1]. In the most pessimistic scenarios, a cloud proprietor may even hide information blunder mischances keeping in mind the end goal to save its notoriety or maintain a strategic distance from benefit misfortunes [2],[3]. What's more, clients who lose coordinate control over their information don't know whether their cloud-put away information is in place or not. Thusly, respectability check for the common information in the cloud is a vital, yet auspicious issue for an expansive number of cloud clients. To guarantee the honesty of information put away in cloud servers, various instruments in view of different methods have been proposed. Specifically, keeping in mind the end goal to lessen the weight on clients, a confided in outsider examiner (TPA) is locked in to lead the confirmation, which is called open reviewing [4]. Nonetheless, the TPA may have superfluous access to private data amid the examining procedure [5]. In this way, scientists proposed some new plans to ensure security, including information protection [6], and character protection [7]-[9]. To be particular, the TPA can't take in each piece that is marked by a specific client in the gathering by building homomorphism authenticable ring signatures [7] or figuring labels in view of regular gathering private key [8].

Cloud storage has attracted extensive attention from academic and industrial communities for its huge advantages of costs, performance and management over traditional local storage. As a result, a growing number of organizations and individuals have been migrating their data to the cloud storage that is managed and maintained by professional cloud service providers (CSPs) [6]. Despite its considerable advantages, there is no denying that the

cloud storage also faces a series of security challenges, especially in terms of security and privacy [4]. One of the significant concerns is how to determine whether the CSP meets the legal expectations of users for data integrity, for which the reasons are twofold. First, due to losing local control of data, cloud users (data owners) can no longer verify the integrity of their data via traditional techniques popularly employed in local storage. Second, although the infrastructures of cloud storage are much more powerful and reliable than personal computing devices, they are more vulnerable to both internal and external security threats due to the open and shared nature of the cloud. More severe still is that some dishonest CSPs, having suffered Byzantine failures occasionally that corrupt data, may try to conceal the fact of data corruptions for their own selfinterest. To address this concern, the cloud storage auditing technique, also called the cloud data auditing, whose purpose is to verify the integrity of the outsourced data remotely, is popularly employed [5].

2. PROPOSED SYSTEM

In the cloud storage model as shown in Figure 1, there are three entities, namely the cloud storage server, group users and a Third Part Auditor (TPA). Group users are formed together of a data owner and a number of users who are authorized to access and reshape the data by the data owner. The cloud storage server is semi-trusted, who serves data storage services for the group users. TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. In our system, the data owner is able to encrypt and upload its data to the remote cloud storage server. Also, he/she shares the authority such as access and modify (compile and execute if necessary) to a number of group users. The TPA could expertly certify the purity of the data stored in the cloud storage server, even the data is regularly updated by the group users. The data owner is different from the other group users, he/she could securely remove a group user when a group user is found malicious or the service period of the user is expired.

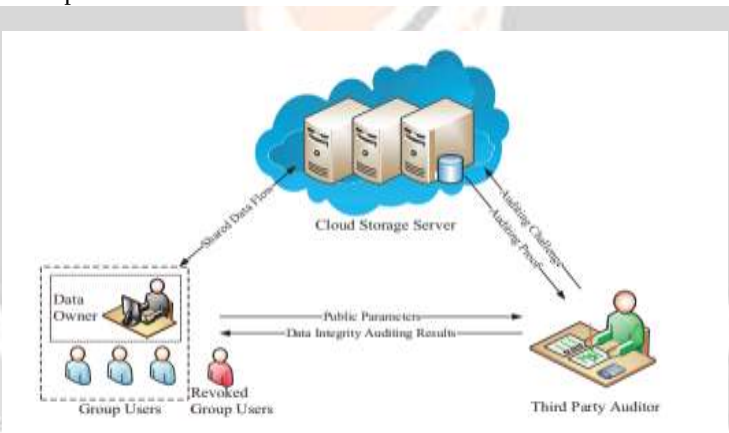

Figure 1 System Architecture

Our threat model deal with two types of attack: 1) An attacker out side the group (include the revoked group user cloud storage server) may obtain some knowledge of the plaintext of the data. Actually, this type of attacker has to at lease break the security of the accepted group data encryption scheme. 2) The cloud storage server connives with the removed group users, and they want to provide a illegal data without being detected. Actually, in cloud environment, we assume that the cloud storage server is semi-trusted. Thus, it is reasonable that a revoked user will collude with the cloud server and share its secret group key to the cloud storage server.

2.1 MATHEMATICAL MODEL

S= "Secured Data Sharing for Cloud Group Users using Public Auditing Mechanism "
S= {I,P,R,O}

Where,

I=Input

I={I1,I2}

Where, I1= Document Dataset

I2= File upload

P= Process

P1=Store file on cloud(simulated)

P2=Preprocessing

P3=Filtering

P4=Classification

P5=Prediction

P6=AES encryption

P7=Compare Result

P8=Value generation

P9=Secret key eject

P10=Send that key using email

P11=Attacker edit file

R=rules

R1=Sha md5 value compare

R2=Match file valid

R3=Group user authentication

O=Output

O1=Security is better that previous system

O2=prevention of data from attacker

O3=Data is being encrypted

3. RESULT AND ANALYSIS

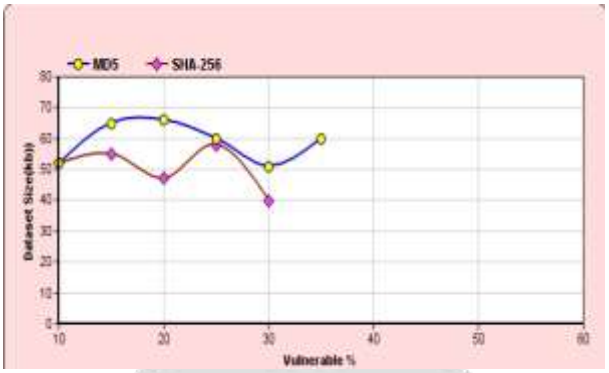

Chart -1

4. CONCLUSIONS

In this paper, we propose a novel multi-level privacy preserving public auditing scheme for cloud data sharing with multiple managers. During the process of key generation random key value has been added so it overcomes the file ambiguity.When the current file has been damaged we can generate latest correct version of the file.

5. ACKNOWLEDGEMENT

It gives me great pleasure to deliver sincere thanks to my project guide Prof. G.M.Kadam for his valuable guidance, constant encouragement and support. I appeal thanks to all the authors of the referenced papers as they help me and motivate me to work on this emerged area. Last but not least, I would like to deliver thanks to my family members, my colleague, and the people who directly or indirectly support me in this project work.

6. REFERENCES

1. Nisha Rathee et al ,"Addressing Techniques for Secure Data Sharing in Cloud", ICICCT,2018, pp : 499 - 503

2. Jian Shen et al,"Anonymous and Traceable Group Data Sharing in Cloud Computing", IEEE , Volume: 13 , Issue:4,2018,pp: 912 – 925

3. Shengmin Xu et al,"Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud",IEEE, Volume: 13,2018,pp: 2101 - 2113

4. Jaya Rao Gudeme et al,"Public Integrity Auditing for Shared Data with Efficient and Secure User Revocation in Clud Computing",IEEE,2018, pp : 588 – 593

5. Rupam Banerjee et al, "A Nobel Cryptosystem for Group Data Sharing in Cloud Storage",IEEE,2019, pp : 0728 – 0731

6. Amogh Santosh Pai Raiturkar et al, "Efficient and Secure Cloud Data Distribution and Sharing Scheme in Groups", ICOEI,2018, pp: 157 – 161

7. Jiguo Li et al,"Certificateless public integrity checking of group shared data on cloud storage",IEEE,2018,pp :1 – 1

8. S Samundiswary et al, "Public auditing for shared data in cloud with safe user revocation", ICECA, Volume: 1,2017,pp : 53 – 57

9. Linmei Jiang et al, "Dynamic Encrypted Data Sharing Scheme Based on Conditional Proxy Broadcast Re-Encryption for Cloud Storage", IEEE, Volume: 5,2017, pp:13336 – 13345