International Journal of Advanced Research Methodology in Engineering & Technology,
Volume 1, Issue 2, March 2017, ISBN 978-1-63535-889-6

Procedural working of user revocation based public auditing for shared data in the cloud

P. William
Computer Science and Engineering Department
Chhatrapati Shivaji Institute of Technology
Durg, India

Deepty Dubey
Computer Science and Engineering Department
Chhatrapati Shivaji Institute of Technology
Durg, India

***Abstract*—One of the most popular emerging technology is cloud computing which satisfies various technical competencies. Cloud environment is basically used for resource sharing and now – a – day's security threats and data confidentiality are most targeted issues in the cloud environment. In the cloud environment certain members can able to form a group and access the information by sharing. To ensure shared data, integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in Shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straight forward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this, a novel public auditing mechanism is proposed for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, we allow the cloud tore-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. This mechanism can significantly increase the efficiency of user revocation. Cloud data can be efficiently shared among the public verifier and a large number of users are able to handle a large number of reviewing tasks simultaneously and efficiently**

Keywords—Public auditing; shared data; user revocation; third party auditing (TPA); proxy re-Signatures

I. INTRODUCTION

Cloud is a huge collection of interconnected processors that is a most important change in how run application and store information. The main advantage of the cloud is low cost and the major disadvantage in this is security. Cloud Computing has been visioned as the next-generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: On demand self-service, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances.

This cloud computing security contains to control deployed to protect data, a set of policies, technology , application and the related organization of cloud computing. Some privacy and security issues their necessity to be considered. Owing to the growth in network bandwidth it befits earlier to deliver quality of services (QOS) as related to previous and also provision to moving the data between client and cloud without any complexity, because of releasing the hardware complexity. In online base computing, cloud provides large amount of resources and data storage to the local machine and then eradicate the local machine to keep individual data. These results users are at the obliged of their cloud service sources for the integrity and availability of their data.

A. Design Issues

One of the challenging design issues which demand great knowledge affecting on the security and performance of the overall system. Biggest concerns with cloud data storage is that truth verification of cloud data at untrusted server. In order to solve the problem of data integrity confirmation, there are many security models & scheme has been proposed. In these works, great efforts are made to build the solution that meet requirement like high efficiency, retrievability of data. Due to involvement of verifier i.e. TPA on behalf of the cloud customer, scheme is reduced into two categories: private auditability and public auditability before they presented. Although, private auditability achieve higher scheme efficiency and public auditability allow anyone, not only data owner but also publicly, to challenge the cloud server for correctness of the data storage while keeping no private information. Then, clients are given all the privilege to an independent third party auditor (TPA) without devotion of their computing supply. In cloud, clients are may not able to performing frequent integrity checks. So that, there is need to develop verification protocol which has public auditability.

B. Public Data Auditing in Cloud

In the cloud resources, we can able to store the data as a group and modify or share it within a group. Cloud data storage contains two entities. They are as follows:

Cloud members : Cloud user is a person who stores huge amount of data on cloud server which is maintained by the Cloud Service Provider (CSP). User can upload their data on cloud and share it within a group.

Cloud server or cloud service provider : A cloud service provider provides services to the cloud user. The main problem in cloud data storage is to obtain integrity of data and correctness stored on the cloud. Cloud Service Provider (CSP) has to provide some mechanism through which user will get the authorization that cloud data is secure or is stored as it is. No modification or data lossis done by unauthenticated member. So that, data auditing concept can be achieved in 2 ways for enhance the Security:

- Without trusted third party
- With trusted third party based on who does the verification.

II. Related Work

A. *Existing System*

The existing system uses the mechanism of provable data possession (PDP) a public auditing is evolved to check the data correction. It enables erasure codes-based data distributed on multiple servers that not only supports dynamic data but also indentifying the misbehaving server. It maintain a semi trusted protocol so that it does not cause any fault in malicious advisory such as incorrectness on shared data as well as reputation of its data services which leads to losing money on its data services. But by means of the mechanism the user cant able to trust the cloud with shared data integrity because there is a possibility of incorrectness due to the hardware/software failures or human errors happened in the cloud. In order to guarantee the TPA, It utilizes the homomorphic authenticator and random masking. It supports in eliminating the burden of cloud user but too expensive regarding the auditing task. It uses single key for computation based on that it is unable to affirm the identity of the signer on all block.

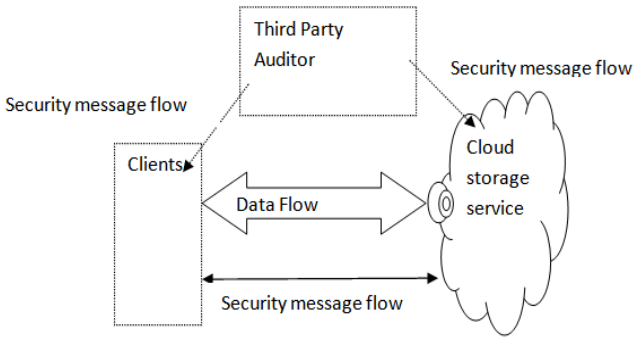

Fig.1 : Architecture of cloud data storage service

In this architecture; it is very difficult task to store the data centrally then managing this centralized data and providing security. So, TPA is used in this situation. The reliability is improved as data is handled by TPA but data integrity is not attained. TPA utilizes encryption technique to encrypt the contents of the file. In this paper Dropbox and Google Drive Applications can be used for ensuring user revocation.

B. *Proposed System*

It is based on public auditing system with user revocation which work based on these essential properties such as correctness, efficient – secure revocation, public auditing and scalability.

Correctness: While sharing the data, the public verifier should maintain the data integrity checking correctly.

Efficient Secure Revocation: If the user is revoked from the group the signed block can be resigned effectively. Only the existing user must valid the signature during shared data.

Public Auditing: Without retrieving the entire data the public verifier can do auditing even some of the blocks have been resigned by the cloud.

Scalability: The cloud environment is a vast environment and the number cloud users are in huge number as well as the data volume is also high. The public verifier must have the capacity in handling the large number of auditing tasks concurrently and proficiently.

Here, a public verifier will always be able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re- signed by the cloud. Moreover, the mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. But with this mechanism if a revoked user is able to collide with the cloud, which possesses a re-signing key, then the cloud and that revoked user together can be able to easily reveal the private key of an existing user. To overcome this limitation, some proxy re-signature schemes with collision resistance in which one can generate a re- signing key with a revoked user's public key and an existing user's private key, can be used. Unfortunately, how to design such type of collusion resistant proxy re-signature schemes while also supporting public auditing, that is, block less verifiability. Meanwhile, the storage overhead and encryption computation cost of this scheme are independent with the number of revoked users.

Public Audit ability and Data Dynamics for Storage Security in Cloud Computing can as well be enabled by identifying the difficulties and potential security problems with fully dynamic data updates. In particular, to achieve efficient data dynamics, proof of storage models can be enhanced by manipulating the classic Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, bilinear aggregate signatures can be used so that a TPA can perform multiple auditing tasks

simultaneously. But unfortunately with this mechanism only private data can be verified and hence this mechanism is not efficient. Also high amount of storage space is required. Assurance to the users of the correctness of the data in cloud is an important concern to be addressed. As the data is physically not accessible to the user, the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. Also checking the integrity of data without downloading them, known as public auditing. There are various techniques which are being used for privacy preservation and public auditing. Each one is better than other but at the same time all these mechanisms have both advantages as well as disadvantages. Hence it is very much public auditing so that efficient integrity check without losing the identity privacy can be done.

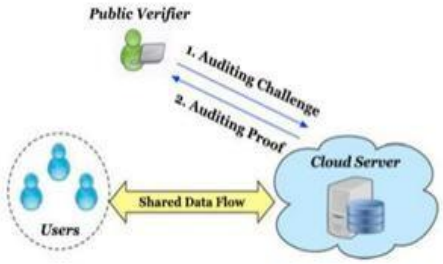

Fig.2 : System architecture with user, cloud server and public verifier

III. TECHNIQUE USED FOR PUBLIC AUDITING

The proposed system enables multiple resigning proxies in the cloud by storing the stored keys and data separately. Each proxy converts the signature and handles the revoked signature in the group by means of resigning keys. That enables the possibility of correcting the signatures when user revocation happens. That enables the data privacy and security which are compromised by an inside attacker. In addition to it our proposed system withheld a new proxy re-signature scheme which makes possibility on achieving block less verifiability and non-malleability thus enabling the proposed mechanism in well structured form.

It includes six phases: KeyGen, ReKey, Sign,ReSign, ProofGen, ProofVerify. In KeyGen, every user in the group generates his/her public key and private key. In ReKey, the cloud computes are-signing key for each pair of users in the group. When the original user creates shared data in the cloud, he/she computes a signature on each block as in Sign. After that, if a user in the group modifies a block in shared data, the signature on the modified block is also computed as in Sign. In ReSign, a user is revoked from the group, and the cloud re-signs the blocks, which were previously signed by this revoked user, with a re-signing key. The verification on data integrity is performed via a challenge-and-response protocol between the cloud and a public verifier. More specifically, the cloud is able to generate a proof of possession of shared data in ProofGen under the challenge of a public verifier. In Proof-Verify, a public verifier is able to check the correctness of a proof responded by the cloud. In ReSign, without loss of generality, we assume that the cloud always converts signatures of a revoked user into signatures of the original user. The reason is that the original user acts as the group manager, and we assume he/she is secure in our mechanism. Another way to decide which re-signing key should be used when a user is revoked from the group, is to ask the original user to create a priority list (PL). Every existing user's id is in the PL and listed in the order of re-signing priority. When the cloud needs to decide which existing user the signatures should be converted into, the first user shown in the PL is selected.

After the re-signing,the original user removes user u_i's id from UL and signs the new UL.By leveraging Shamir Secret Sharing *s* multiple proxies is used, each re-signing key is divided into *s* pieces and each piece is distributed to one proxy. These multiple proxies belong to the same cloud, but store and manage each piece of a re-signing key independently. since collusion-resistant proxy re-signature schemes generally have two levels of signatures (i.e., the first level is signed by a user and the second level is re-signed by the proxy), where the two levels of signatures are in different forms and need to be verified differently, achieving blockless verifiability on both of the two levels of signatures and verifying them together in a public auditing mechanism is challenging.

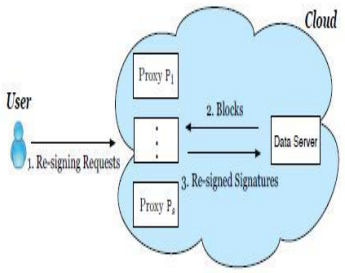

Fig.3 : Multiple re-signing proxies in the cloud

IV. CONCLUSION

A new public auditing mechanism is there for shared data with user revocation in the cloud. Cloud computing is world's biggest innovation which uses advanced computational power and improves data sharing and data storing capabilities. As every coin has two sides it also has some drawbacks. Privacy security is a main issue for cloud storage. To ensure that the risks of privacy have been mitigated a variety of techniques that may be used in order to achieve privacy. It increases the ease of usage by giving access through any kind of internet connection. When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with

proxy re-signatures. Experimental results show that the cloud can improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D.Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), pp. 598-610, 2007.

[2] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Intl Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT08), pp. 90- 107, 2008.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[4] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Intl Conf. Applied Cryptography and Network Security (ACNS12), pp. 507-525, June 2012.

[5] B.Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE CLOUD, pp. 295-30 2, 2012.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no.2, pp. 220-232, Jan. 2012.

[7] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013

[8] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans.Services Computing, vol. 6, no. 4, pp. 551-559, Oct.- Dec. 2013

[9] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems (TPDS13), vol. 24, no. 6, pp. 1182-1191, June 2013

[10] A.Juels and B.S. Kaliski, Jr., "Pors:proofs of retrievability for large files," in CCS"07: Proceedings of the 14th ACM conference on Computer and communications security.

[11] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage,"Cryptology ePrint Archive, Report 2008/489, 2008.

[12] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," In Proceedings of SecureComm " 08, pp. 1–10, 2008.

[13] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," In Proceedings of ICDCS "08, pp. 411–420,2008.