International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Public Audit of Cloud Shared Data by Using Efficient Privacy Preserving Scheme

Franklin Malugu[1], K. Suresh Babu[2]

[1]M.Tech Scholar, Department of Computer Networks and Information Security, School of IT Jawaharlal Nehru Technological University Hyderabad, India
[2]Assistant Professor, Department of Computer Networks and Information Security, School of IT Jawaharlal Nehru Technological University Hyderabad, India

Abstract: ***Public auditing for cloud storage is of critical importance as the users relies on semi-trusted cloud storage service for data sharing which does not guarantee/assure the integrity of the data being stored. With public auditing of clouds, users resort to a third party auditor (TPA) who verify and assure the internal consistency/lack of corruption of their data in cloud storage services. Despite the good work previously done by researchers in auditing while preserving privacy, still available mechanisms do not efficiently conceal users' privacy from TPA during sharing of data and yet supporting data and group dynamics. In this paper, we propose privacy preserving auditing scheme that exploits the ring signature to calculate verifications needed to audit data integrity. In this proposed approach, the identities of the user are kept private from public verifier and dynamic groups are supported –that is a new user can be added into the group and an existing group member can be revoked during data sharing.***

Keywords: Public Auditing, Cloud Storage, Privacy-preserving, TPA

1. Introduction

Cloud computing is transforming the nature of how business and people uses information technology today. This computing paradigm shift provides a scalable environment for growing amounts of data and processes that work on various application and services by means of on demand self services. Particularly, the outsourced storage in clouds is a new profit generating area by providing a uniformly low cost, scalable, geographically location-independent platform for managing users' data. The cloud storage services lighten the burden for storage management and maintenance. Nowadays it is a routine for most users to leverage cloud storage services to share data with others in a group, as data sharing becomes a standard features in most cloud storage offerings including Google Drives, iClouds and Dropbox.

However, the exciting advantages which are provided by cloud storage services, storing data in a cloud does not give any guarantee on data integrity and availability. Users' data is put at risk of losses or being incorrect during sharing as the cloud service providers are separate administrative distance, out of the control of users. These security risks can be caused by: the internal and external threats in clouds infrastructures, for example there are various motivations for cloud service providers to behave unfaithfully towards the clouds users as well as the dispute due to lack of trust on Cloud storage service. Cloud users may not be aware of this behaviour even if these disputes may results into users own's improper operation [4].

Following these and related challenges, public auditing, in particular privacy preserving one is suggested by researchers as trust worthy solution to be enhanced in cloud storage service so as to check for correctness of users data. In privacy preserving public auditing, the third party auditor is resorted to publicly verify the integrity of users' data stored in clouds before being shared among multiple users without knowing the data and users' identities privacy. A traditional approach provides only public auditing while preserving data privacy. This conventional approach will provide public auditing while keeping private users identities from third party auditor in a dynamic group data sharing environment.

2. Background and Related Work

As per Atieniese et al**,** a provable data possession (PDP) model was designed for remote data checking: user's data that is stored in an untrusted server can be verified if it is the original data without retrieving it. The model produces probabilistic proofs of possession by sampling random sets of blocks from the server. The client maintains a constant amount of metadata to verify the proof. This approach provides an effective foundation to accommodate the requirements for public auditability in remote storage, however when used directly, their approach is not provably privacy preserving, which expose users' data information to auditor.[1][5]

An improved Proof of Retrievability Scheme with full proofs of security was established by Shacham et al.[6] from the security model by Juels et al [7] where spot checking and error –correcting code are used to ensure both "possession" and "retrievability" of data files on archive service systems. They use publicly verifiable homommorphic authenticators built from BLS signatures, based on which the proofs can be aggregated into a small authenticator value and public retrievability was achieved.

A public audit scheme that preserves the content of private data belonging to a personal user was also proposed by Wang et al [2]. It efficiently checks for integrity of cloud data without retrieving the local copy of data. This scheme eliminates the burden of cloud user from tedious work and possibly expensive auditing tasks and efficiently preserves the user data to the third party auditor but it allows the third party auditor to learn identity privacy in cloud data sharing.

As per B. Wang et al,[3], a privacy preserving public auditing mechanism for a shared data in untrusted cloud was introduced which is referred as "oruta". It utilizes ring signatures to construct hormomophic authenticators so that the integrity of shared data can be checked by third party auditor without retrieving the entire data –while preserving identity privacy. The drawback of this scheme is that it doesn't support the dynamic group data sharing, it supports only static group where users are predefined.

3. Problem Definition

It is very common for users' data in the cloud to be shared across multiple users in the group whereby a user digitally signs documents when making changes to data before he/she can share again with other users in the same group. The unseen signatures tagged in data can possibly be learnt by auditor or cloud service provider during audit process. If that information gets to the knowledge of an authorized outsider, it is easy for kind of relationship and the roles placed by each user to be understood, which in turn can lead for an interested attacker to know which target to attack (keep in mind semi-trusted auditor can be easily manipulated for the sake of money or any other reason that can make him/her being interested). Think of market plan information for xyz company for instance, if competitors know exactly the major player by deducing his/her identities from that piece of shared information, the focused business will easily face stiff competition from their rivalry. Enforcing data privacy against publicly auditor does not keep him from learning users identities. This fact grabbed researchers' attention to come up with some auditing scheme that addresses identity privacy. Identity privacy preserving auditing shared data in a cloud on dynamic groups' environment where a new user is added into a group and an existing group member can be revoked has never been fully addressed. How to achieve an efficient and secure audit scheme that supports both public audit and data dynamics to the clouds is still an open challenging tasks in cloud computing.

4. Project Objectives

The main goal of this project is to provide a solution that will efficiently and effectively publicly verify shared data in the cloud storage without the verifier(TPA) being able to learn the users privacy during the audit process thereby preserving users privacy to be accessed by unauthorized individuals. The following composes the specific objectives to a proposed system:

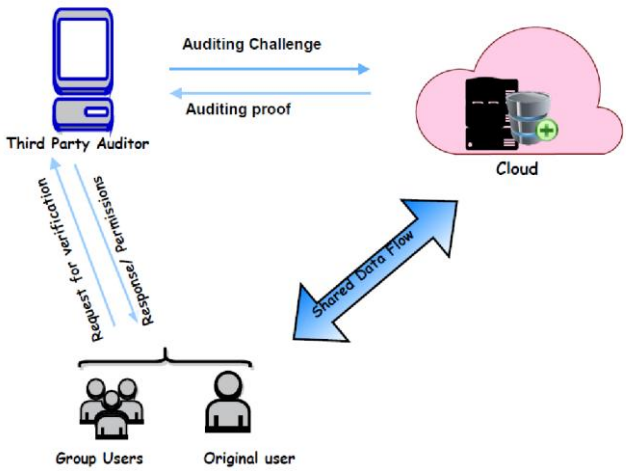
- To provide the system that supports data preserving as well as identity privacy preserving public auditing of shared data in a clouds
- To provide a mechanisms that supports dynamic groups data sharing in the clouds
- To support batch auditing for user's multiple data

5. Proposed Solution

In the proposed system, there are two types of users, the original user who is the data owner and who allows shared data accessibility to other users, and group users who access and make changes to the shared data file in the cloud storage. Before beginning data sharing session, users must be sure of the integrity of the data shared, so they first check for verification from the third party auditor. The auditor receives the request and then TPA generate audit challenges and send them to cloud server to receive audit proof. If the auditor is assured that the shared cloud data is error free, it will give a verification response back to allow the users to proceed with whatever they wishes to do in the shared data. To achieve the objectives of this project, we have proposed to exploit the below techniques:

- Ring signatures will be utilized to construct homomorphic authenticators so that a public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier. We will extend our mechanism to support batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks.
- we will also leverage index hash tables from a previous public auditing solution to support both dynamic data and group

This public auditing mechanism will include KeyGen, SigGen, ProofGen and ProofVerify algorithms which standardized step by step action in public auditing as well Alter. User's own public/private is generated by KeyGen. In SigGen, original user or a group user can calculate ring signatures on the the blocks in shared data. Every Group user is able to delete, update or insert on a block and compute the new ring signature in Alter. ProofGen is run by both the Public Verifier(TPA) and the cloud server to produce a proof of possession of shared data. The proof is verified and and the report is send to user in ProofVerify.



Proposed System Model

6. Conclusion

This review paper proposes a mechanism to perform data integrity check during data sharing on cloud storage that preserve user privacy from a public verifier. It also supports identity privacy preserving on dynamic group.

References

[1] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. of SecureComm'08, 2008.
[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533
[3] Boyang Wang, Baochun Li, Hui Li have presented a new technology "Oruta: Privacy-Preserving Public Auditing for Shared Data in Cloud", IEEE transactions on cloud computing, vol. 2, no. 1, january-march 2014.
[4] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in Proc. ACM Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.
[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–610
[6] H. Shachan and B.Works,"Compact Proofs of Retrievability, in Proc. International Conference on the Theory and application of cryptology and Information security (ASIACRYPT)".SpringerVerlag, 2008, pp,90107.
[7] M. Armbrust et al "A view of cloud computing Communication of ACM",vol. 53 no. 4, pp 5058, April 2010.