Oruta: Preserving- Privacy Public Auditing For Shared Data in the Cloud

R.HIMABINDU[1], J.VENKATA KRISHNA[2]

[1]Research Scholar, [2]Associate Professor & HOD
Department of Computer Science and Engineering
Sree Vahini Institute of Science and Technology Tiruvuru, Andhra Pradesh

***Abstract*: With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. However, public auditing for such shared data while preserving identity privacy remains to be an open challenge. In this paper, we propose the first privacy-preserving mechanism that allows public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file. Our experimental results demonstrate the effectiveness and efficiency of our proposed mechanism when auditing shared data.**

***Keywords*: Cloud computing, Shared Data, public auditing, identity, privacy**

1. INTRODUCTION

Cloud service providers manage an enterprise-class infrastructure that offers a scalable, secure and reliable environment for users, at a much lower marginal cost due to the sharing nature of resources. It is routine for users to use cloud storage services to share data with others in a team, as data sharing becomes a standard feature in most cloud storage offerings, including Dropbox and Google Docs. The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in an untrusted cloud can easily be lost or corrupted, due to hardware failures and human errors . To protect the integrity of cloud data, it is best to perform public auditing by introducing a third party auditor (TPA), who offers its auditing service with more powerful computation and communication abilities than regular users. The first provable data possession (PDP) mechanism to perform public auditing is designed to check the correctness of data stored in an untrusted server, without retrieving the entire data. Moving a step forward, Wang et al. (referred to as WWRL in this paper) is designed to construct a public auditing mechanism for cloud data, so that during public auditing, the content of private data belonging to a personal user is not disclosed to the third party auditor. We believe that sharing data among multiple users is perhaps one of the most engaging features that motivates cloud storage.

System architecture

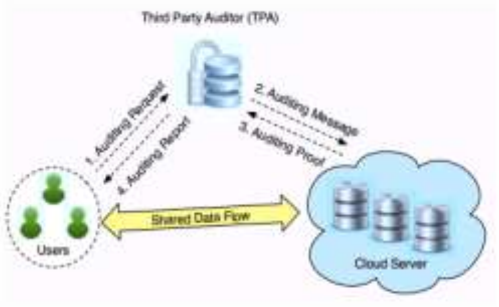

Fig 1.System Architecture

Our Contributions

The main contributions of this paper are the following:
1. Distributed access control of data stored in cloud sothat only authorized users with valid attributes canaccess them.
2. Authentication of users who store and modify theirdata on the cloud.
3. The identity of the user is protected from the cloudduring authentication.
4. The architecture is decentralized, meaning that therecan be several KDCs (Key Distribution center) for key management.
5. The access control and authentication are bothcollusion resistant, meaning that no two users cancollude and access data or authenticate themselves,if they are individually not authorized.
6. Revoked users cannot access data after they havebeen revoked.

7. The proposed scheme is resilient to replay attacks. Awriter whose attributes and keys have been revokedcannot write back stale information.
8. The protocol supports multiple read and write onthe data stored in the cloud.
9. The costs are comparable to the existing centralized approaches, and the expensive operations are mostlydone by the cloud.

2. RELATED WORK

Ateniese *et al.* [2] first proposed provable data possession (PDP), which allows a client to verify the integrity of her data stored in an untrusted server without retrieving the entire file. PDP is the first mechanism that provides public verifiability (also referred to as public auditing). However, it only supports static data. To improve the efficiency of verification, Ateniese *et al.* [10] constructed a scalable and efficient PDP using symmetric keys. This mechanism is able to support partially dynamic data operations. Unfortunately, it cannot support public verifiability and only offers each user a limited number of verification requests.

Juels and Kaliski [11] defined another similar model called proof of retrievability (POR), which is also able to check the correctness of data stored in an untrusted server. The original file is added with a set of randomly-valued blocks called *sentinels*. The user verifies the integrity of data by asking the server to return specific sentinel values. Shacham and Waters [6] designed two improved POR, which are built on pseudo-random functions and BLS signatures [12].

Wang *et al.* [7] leveraged the Merkle Hash Tree to construct a public auditing mechanism, which can support *fully dynamic data*. Erway *et al.* [13] also presented a fully dynamic PDP based on the rank-based authenticated dictionary. Zhu *et al.* [8] exploited index hash tables to support fully dynamic data during the public auditing process.

More recently, Wang *et al.* [3] first considered public auditing for cloud data with data privacy. In this mechanism, the third party auditor is able to check the integrity of cloud data but cannot obtain any private data. In addition, to operate multiple users' auditing tasks simultaneously, they also extended their mechanism to enable batch auditing by leveraging aggregate signatures [5]. Our recent work [14] is able to audit the integrity of shared data in the cloud for large groups. Unfortunately, it cannot support public auditing.

3. PROPOSED METHOD

To solve the above privacy issue on shared data, we propose Oruta, a novel privacy-preserving public auditing mechanism. More specifically, we utilize ring signatures to construct homomorphic authenticators in Oruta, 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.

In addition, we further extend our mechanism to support batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks. Meanwhile, Oruta is compatible with random masking, which has been utilized in WWRL and can preserve data privacy from public verifiers. Moreover, we also leverage index hash tables from a previous public auditing solution to support dynamic data. A high-level comparison among Oruta and existing mechanisms is presented.

4. IMPLEMENTATION

Owner registration:

In this module an owner has to upload its files in a cloud server, he/she should register first then only he/she can be able to do it for that he needs to fill the details in the registration form. he/she details are maintained in a database.

Owner login:

In this module, any of the above mentioned person have to login ,they should login by giving their email id and password .

User registration:

In this module if a user wants to access the data which is stored in a cloud,he/she should register their details first. these details are maintained in a database.

User login:

If the user is an authorized user,he/she can download the file by using file id which has been stored by data owner when it was uploading.

Third Party Auditor Registration

In this module , if a third party auditor (maintainer of clouds) wants to do some cloud offer, they should register first. Here we are doing like, this system allows only three cloud service providers.

Third party auditor login:

After third party auditor gets logged in, He/she can see how many data owners have uploaded their files into the cloud. Here we are providing three tpa for maintaining three different clouds.

Data sharing:

we only consider how to audit the integrity of shared data in the cloud with static groups. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing. The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud. Another interesting problem is how to audit the integrity of shared data in the cloud with dynamic groups a new user can be added into the group and an existing group member can be revokes during data sharing while still preserving identity privacy

5. CONCLUSION

we propose Oruta, the first privacy preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphic authenticators, so the TPA is able to audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy. To improve the efficiency of verification for multiple auditing tasks, we further extend our mechanism to support batch auditing. An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[2] 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.

[3] 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.

[4] R. L. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret,” in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer- Verlag, 2001, pp. 552–565.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” in Proc. In- ternational Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag, 2003, pp. 416–432.

[6] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer- Verlag, 2008, pp. 90–107.

[7] 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.

.

Authors Profiles

R. Himabindu
,M-Tech Dept. of CSE
SreeVahini Institute of Science and Technology
TiruvuruAndhra Pradesh

J.Venkata Krishna
Assoc.Professor &HOD,
SreeVahini Institute of Science and Technology
Tiruvuru Andhra Pradesh
"B.TECH(CSE),M.TECH(CSE),(Ph.D)"
Email id :-hodcsesvist234@gmail.com