International Journal of Scientific Research in Computer Science, Engineering and Information Technology

© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

Privacy-Preserving Public Auditing for Shared Data on the Cloud

Nitin Jagdale*, Sahil Tamboli, Ashish Kumar, Sonali Kale

KJEI's Trinity Academy of Engineering, Pune, Maharashtra, India

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 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: Public Auditing, Privacy-Preserving, Shared Data, Cloud Computing, Third Party Auditor.

I. INTRODUCTION

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) 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. A unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a higher valuable target than others. For example, Alice and Bob work together as a group and share a file in the cloud. The shared file is divided into a number of small blocks, which are independently signed by users. Once a block in this shared file is modified by a user, this user needs to sign the new block using her public/private key pair. The TPA needs to know the identity of the signer on each block in this shared file, so that it is able to audit the integrity of the whole file based on requests from Alice or Bob.

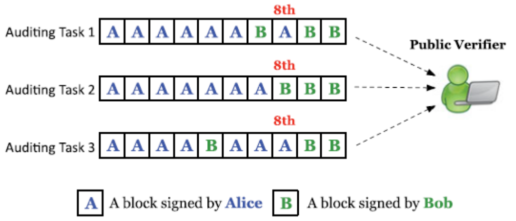


Fig. 1. Alice and Bob share a data file in the cloud, and a public verifier audits shared data integrity with existing mechanisms.

II. LITERATURE SURVEY

S No	Year	Title	Author	Description
01)	2016	Preserving Privacy in	Anjali R. S.	Cloud technology helps the authenticated

CSEIT17241 | Received : 16 Oct 2017 | Accepted : 31 Oct 2017 | September-October-2017 [(2)5: 1032-1034]

		Public Auditing for Shared Cloud Data	Department of Computer Science and Engineering	cloud users to access plenty of resources that are transferred and accumulated in cloud. To preserve the data security and un-authorized users from accessing the users confidential data a auditing mechanism can be performed with the help of a third party auditor.
02)	2016	Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud	Ms.Priya Kharmate Department of Computer Engineering	To mitigate the risks of privacy of data stored on cloud with objective of minimum computational overhead and the fact that the data owner cannot always stay online hence the data privacy maintained through auditing process.
03)	2016	Public Auditing Services in Cloud Networks for Data Sharing Including Privacy Preserving	Sonal Shukla Computer Science, Maharishi Ar vind College of Engg. and Reaserch Center, Jaipur, India	This system development demonstrating incorporates three interesting substances: Users that has a great deal of information to be secured in cloud and have the approvals to get to and control set away information. Cloud Service Providers who cording ate to give data stockpiling organizations have sufficient stockpiles and calculation assets
04)	2013	Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics	Boyang Wang State Key Laboratory of Integrated Service Network	In this Project, we propose a privacy-preserving public auditing mechanism in the cloud for dynamic groups. By sharing a common group private key with users in the group, each user is able to compute valid signatures on shared data, so that the TPA is able to audit the integrity of shared data for the group but cannot reveal the identity of the signer on each block
05)	2015	Identity-Preserving Public Auditing for Shared Cloud Data	Kai He Computer School, Wuhan University, Wuhan, China	We proposed an identity-preserving public auditing scheme for shared data in cloud storage. By utilizing the idea of proxy re-signatures and the technique of bilinear pairing, our scheme achieves identity preserving against the TPA and the auditing cost is very low.

III. METHODS AND MATERIAL

MODULES

1. Admin

Admin get notification when where user try to change settings then admin will be asked one security question if that answer matches with the database values then admin will allowed change settings.

2. 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.

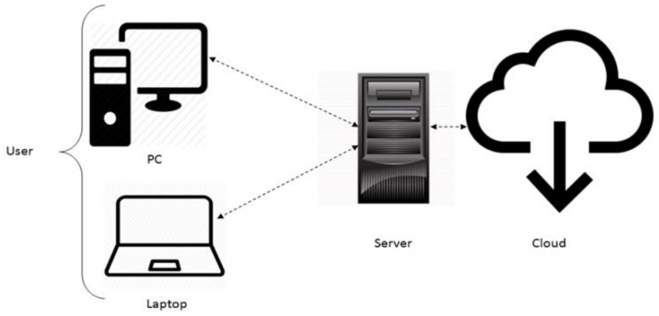
3. User Login:

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.

4. Data Sharing:

We only consider how to audit the integrity of shared data in the cloud with static groups. It means the group is predefined 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 revoked during data sharing while still preserving identity privacy.

IV. SYSTEM ARCHITECTURE



V. SYSTEM FEATURES

We believe that sharing data among multiple users is perhaps one of the most engaging features that motivates cloud storage.

We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless i ntegration of these two salient features in our protocol design. It implies that the data are stored in one or more servers in the network and that there is some software locking mechanism that prevents the same set of data from being changed by two people at the same time. Data sharing is a primary feature of a database management system (DBMS) They appended the current time period to the ciphertext, and OTP.

VI. CONCLUSION

We propose, 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.

VII. FUTURE SCOPE

- ✓ Providing a better user interface to view shared files.
- ✓ Providing better authentication and allow total group access to shared accounts.
- ✓ Extending our app so that it can be used on multiplatform such a iOS, Blackberry OS.

VIII. REFERENCES

[1]. B. Wang, B. Li, and H. Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,” Proc. IEEE Fifth Conf. Cloud Computing, pp. 295-302, 2012.

[2]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, “A View of Cloud Computing,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3]. K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4]. D. Song, E. Shi, I. Fischer, and U. Shankar, “Cloud Data Protection for the Masses,” Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5]. 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.