International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-01, Apr 2018

Secure & Trusted Information Brokering in Cloud Computing

P Manivannan, Patil Ankita M., Survase Jyoti P., Thakur Latika P., Yadav Shivasare D.

Dept. of Information Technology, Mahatma Gandhi Mission's College of Engineering and Technology, Mumbai, Maharashtra, India.

Pmvannan.mtech@gmail.com, patilankita120@gmail.com, jyotisurvase21@gmail.com, latikapthakur@gmail.com, hiveshyadav45@gmail.com

Abstract - To facilitate extensive collaborations, cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information identity privacy to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. We also propose a secure multi-owner data sharing scheme for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

Keywords: Information Broking System, Automation segmentation, coordinates broker, privacy preserving, Attribute-correlation attack.

I. 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 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. 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.

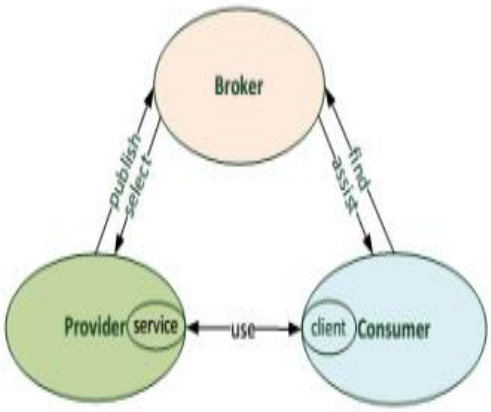

Fig. Relationship between Consumer, Broker & Provider

 DOI : 10.18231/2454-9150.2018.0088

II. PROBLEM STATEMENT

The cloud server, the third party auditor (TPA) and users. There are two types of users in a group: the original user and a number of group users. The original user and group users are both members of the group. Group members are allowed to access and modify shared data created by the original user based on access control polices. Shared data and its verification information (i.e. signatures) are both stored in the cloud server. The third party auditor is able to verify the integrity of shared data in the cloud server on behalf of group members. In this paper, 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 revoked during data sharing, while still preserving identity privacy. We will leave this problem to our future work.

When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing request, the TPA generates an auditing message to the cloud server, and retrieves an auditing proof of shared data from the cloud server. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.

Two kinds of threats related to the integrity of shared data are possible. First, an adversary may try to corrupt the integrity of shared data and prevent users from using data correctly. Second, the cloud service provider may inadvertently corrupt (or even remove) data in its storage due to hardware failures and human errors. Making matters worse, in order to avoid jeopardizing its reputation, the cloud server provider may be reluctant to inform users about such corruption of data. The identity of the signer on each block in shared data is private and confidential to the group. During the process of auditing, a semi-trusted TPA, who is only responsible for auditing the integrity of shared data, may try to reveal the identity of the signer on each block in shared data based on verification information. Once the TPA reveals the identity of the signer on each block, it can easily distinguish a high-value target (a particular user in the group or a special block in shared data).

III. LITERATURE REVIEW

Provable data possession (PDP), first proposed by Ateniese et al , allows a verifier to check the correctness of a client's data stored at an untrusted server. By utilizing RSA-based homomorphic authenticators and sampling strategies, the verifier is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public verifiability or public auditing. Unfortunately, their mechanism is only suitable for auditing the integrity of static data. Juels and Kaliski defined another similar model called proofs of retrievability (POR), which is also able to check the correctness of data on an untrusted server. The original file is added with a set of randomly-valued check blocks called sentinels. The verifier challenges the untrusted server by specifying the positions of a collection of sentinels and asking the untrusted server to return the associated sentinel values. Shacham and Waters designed two improved POR schemes. The first scheme is built from BLS signatures, and the second one is based on pseudorandom functions.

To support dynamic operations on data, Ateniese et al. presented an efficient PDP mechanism based on symmetric keys. This mechanism can support update and delete operations on data, however, insert operations are not available in this mechanism. Because it exploits symmetric keys to verify the integrity of data, it is not public verifiable and only provides a user with a limited number of verification requests. Wang *et al.* utilized Merkle Hash Tree and BLS signatures to support fully dynamic operations in a public auditing mechanism. Erway et al. introduced dynamic provable data possession (DPDP) by using authenticated dictionaries, which are based on rank information. Zhu et al. exploited the fragment structure to reduce the storage of signatures in their public auditing mechanism. In addition, they also used index hash tables to provide dynamic operations for users. The public mechanism proposed by

Wang et al. is able to preserve users' confidential data from the TPA by using random maskings. In addition, to operate multiple auditing tasks from different users efficiently, they extended their mechanism to enable batch auditing by leveraging aggregate signatures.

To prevent special attacks exist in remote data storage system with deduplication, Halevi et al. introduced the notation of proofs-of-ownership (POWs), which allows a client to prove to a server that she actually holds a data file, rather than just some hash values of the data file. Zheng et al. further discussed that POW and PDP can co-exist under the same framework.

Recently, Franz et al. proposed an oblivious outsourced storage scheme based on Oblivious RAM techniques, which is able to hide users' access patterns on outsourced data from an untrusted cloud. Vimercati et al. utilize shuffle

 DOI : 10.18231/2454-9150.2018.0088

index structure to protect users access patterns on outsourced data.

S. Kamara et al. proposed a security for customers to store and share their sensitive data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security. HoIver, the revocation operation is a sure performance killer in the cryptographic access control system. To optimize the revocation procedure, they present a new efficient revocation scheme which is efficient, secure, and unassisted. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. Thus, the revocation process is accelerated by affecting only one slice instead of the whole data. They have applied the efficient revocation scheme to the cipher text-policy attribute-based encryption based cryptographic cloud storage. The security analysis shows that the scheme is computationally secure.

E. Goh et al. presented a SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. Our implementation of SiRiUS performs Ill relative to the underlying file system despite using cryptographic operations. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Using cryptographic operations implementation of Sirius also possible. It only uses the own read write cryptographic access control. File level sharing are only done by using cryptographic access.

IV. PROPOSED MODEL

In this paper, to solve the above privacy issue on shared data, we propose, a novel privacy-preserving public auditing mechanism. More specifically, we utilize ring signatures 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. Also user revocation can be done and the new user would be able to access the uploaded data.

The proposed system mainly consists of five modules,
(i) Group member module.
(ii) Ring signature module.
(iii) User revocation module.

ADVANTAGES OF PROPOSED MODELS

- ✓ A public verifier is able to correctly verify shared data integrity.
- ✓ A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing.
- ✓ The ring signatures generated for not only able to preserve identity privacy but also able to support blockless verifiability.
- ✓ The encryption complexity and size of ciphertexts are independent with the number of revoked users in the system.
- ✓ User revocation can be achieved without updating the private keys of the remaining users. A new user can directly decrypt the files stored in the cloud before his participation.

V. ALGORITHMS

*** SECURE HASHING ALGORITHM(SHA).**

*** AES (ADVANCED ENCRYPTION STANDARD) ALGORITHM.**

OVERVIEW ARCHITECTURE MODULE

The proposed middleware architecture consists of a number of core modules, include the trusted resource matchmaking and distributing module, the adaptive trust evaluation module, the agent-based on service operator acquisition module, and the resource management module, among others. This module is core of the trust-aware cloud computing system, and is the major focus of this paper. Using this module, broker can dynamically sort high-performance resources by analyzing the historic resource information in terms of providing highly trusted resources.

- ***Group Member Module :***

Group members are a set of registered users that will store their private data into the cloud server and Share them with others in the group. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it.

- ***Ring Signature Module :***

A ring signature scheme allows member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

- ***User Revocation Module :***

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

 DOI : 10.18231/2454-9150.2018.0088

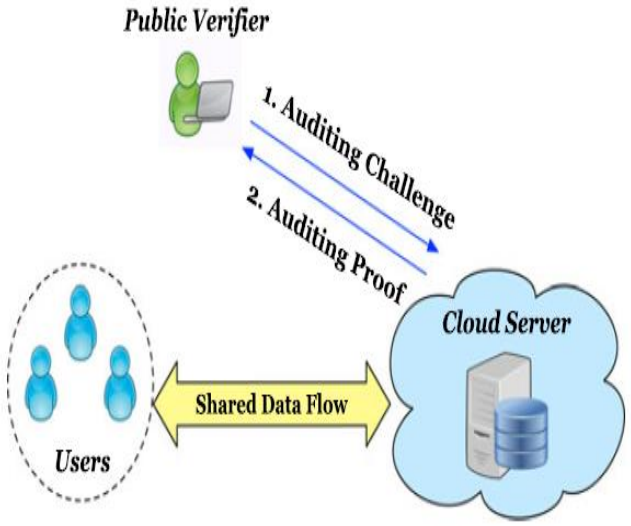

Fig: Architecural diagram

VI. CONCLUSION

We had proposed 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 audi

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 , 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.

[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.

[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.

[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.

[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.

 DOI : 10.18231/2454-9150.2018.0088