International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - I **ISSN (Online): 2454- 1966**

DATA INTEGRITY MAINTENANCE IN CLOUD STORAGE USING HASHING TECHNIQUE

P.Sumathi, P.Kokila,

Assistant professor, PG scholor
Department of Computer Science and Engineering
KSR Institute for Engineering and Technology

E-Mail: harshini.sumathi@gmail.com, pkokila.kokila@gmail.com

March – 2016

www.istpublications.com

International Journal of Future Innovative Science and Engineering Research (IJFISER), Volume - 2, Issue – I,
ISSN (Online): 2454- 1966
www.istpublications.com.

DATA INTEGRITY MAINTENANCE IN CLOUD STORAGE USING HASHING TECHNIQUE

P.Sumathi, P.Kokila,

Assistant professor, PG scholor
Department of Computer Science and Engineering
KSR Institute for Engineering and Technology

E-Mail: harshini.sumathi@gmail.com, pkokila.kokila@gmail.com

ABSTRACT

The cloud data services, it is usual for data to be not only stored in the cloud, but also shared across multiple users. The integrity of cloud data is subject to doubt due to the existence of hardware/software failures and human errors. Some mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without downloading the entire data from the cloud server. The public auditing on the integrity of shared data with these existing mechanisms will predictably expose confidential information, identity privacy to public verifiers. A novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In ring signatures to compute verification metadata needed to audit the correctness of shared data. In this 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. In addition, the mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. To propose the traceability mechanism is perform unbroken record of documentation or an unbroken chain of measurements and associated uncertainties. The experimental results express the competence and efficiency of these mechanisms when auditing shared data integrity.

Key words—Public auditing, preserving, shared data, cloud computing

I. INTRODUCTION

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. Cloud computing is the delivery of computing services over the Internet. Cloud services allow

individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection

is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Cloud computing offers benefits for organizations and individuals. There are also privacy and security concerns. If you are considering a cloud service, you should think about how your personal information, and that of your customers, can best be protected. Carefully review the terms of service or contracts, and challenge the provider to meet your needs

The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures or hash values of the entire data. Certainly, this conventional approach is able to successfully check the correctness of cloud data. However the efficiency of using this traditional approach on cloud data is in doubt.

The main reason is that the size of cloud data is large in general. Downloading the entire cloud data to verify data integrity will cost or even waste user's amounts of computation and communication resources, especially when data have been corrupted in the cloud. It is because cloud providers, such as Amazon, can offer users computation services directly on large-scale data that already existed in the cloud. Recently, many mechanisms have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing.

In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. A public verifier could be a data user (e.g., researcher) who would like to utilize the owner's data via the cloud or a Third-Party Auditor (TPA) who can provide expert integrity checking services. Moving a step forward, Wang et al. designed an advanced auditing mechanism, so that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. Unfortunately, current public auditing solutions mentioned above only focus on personal data in the cloud.

We believe that sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. Therefore, it is also necessary to ensure the integrity of shared data in the cloud is correct. Existing public auditing mechanisms can actually be extended to verify shared data integrity. However, a new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers.

Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information to public verifiers. In this paper, to solve the above privacy issue on shared data. More specifically, we utilize ring signatures to construct homomorphism authenticator's. 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.

II. EXISTING SYSTEM

The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures or hash values of the entire data. Certainly, the conventional approach is able to successfully check the correctness of cloud data. However, the efficiency of using traditional approach on cloud data is in doubt.

Many mechanism have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as a public auditing. A public verifier could be a data user who would like to utilize the data owners via the cloud or third party auditor who can provide expert integrity checking services.

In existing system a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With the 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.

In addition, mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.

A.DISADVANTAGE

These are the problems which are going to overcome in the proposed system failing to preserve identity privacy on shared data during public auditing. Next, protect these confidential information is essential and critical to preserve identity privacy from public verifiers during public auditing.

III. PROPOSED SYSTEM

To propose the traceability mechanism, which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations? Another work is future work is how to prove data freshness (prove the cloud possesses the latest version of shared data) while still preserving identity privacy.

[1] ADVANTAGE

Identify the signature on each block and retrieve the original data to the users.

IV. LITERATURE SURVEY

Wang et al propose cloud computing is widely developed technology, remotely to be temporarily shared across multiple users in flexible manner than products. Users can continuously access service from the remote locations. So cloud creates issues in data security, privacy integrity and dynamic updates. The cloud server stores large amount of data which does not offer guarantee on data integrity and consistency. In user side every time it is not possible to check data consistency of stored data on cloud storage. It is problem is solving by public auditing method which ensure integrity and to reduce online burden on cloud data storage.

Wang et al gives to preserve the identity of the signer on each block during public auditing, one possible alternative approach is to ask all the users of the group to share a global private key. Every user is able to sign blocks with the global private key. Once one user of the group is compromised or leaving the group a new global private key must be generated and securely shared among the rest of the group, which clearly introduces huge overhead to users in terms of key management and key distribution. While here each user in the rest of the group can still utilize its own private key for computing verification metadata without generating or sharing any new secret keys.

Wang et al describes storing the data in cloud environment becomes natural and also essential. But, security becomes one of the major concerns for all entities in cloud services. Firstly, data owners would worry their data could be misused or accessed by unauthorized users. Secondly, the data owners would worry their data could be lost in the Cloud. Moreover, the cloud service providers (CSP) may be dishonest and they may discard the data which has not been accessed or rarely accessed to save the storage space or keep fewer replicas than promised. As a result data owners need to be convinced that their data are correctly stored in the Cloud. It is desirable to have data storage auditing (DSA) service to assure data are correctly stored in the Cloud.

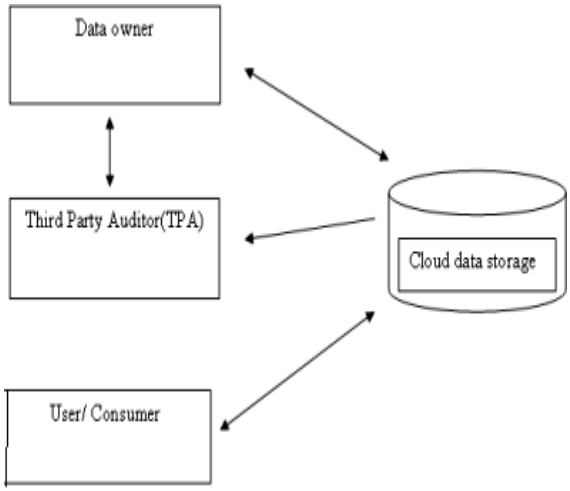
Wang et al gives data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed 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 the revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation. It is inefficient due to the large size of shared data in the cloud.

V.PROBLEM STATEMENT

A. System model

The system model in this paper involves three parties: the cloud server, a group of users and a public verifier as shown in fig. There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. Every member of the group is allowed to access and modify shared data.

Shared data and its verification metadata are both stored in the cloud server. A public verifier, such as a third party auditor providing expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server.



VI.RING SIGNATURES

The ring signatures, a verifier are convinced that a signature is computed using one of group members' private keys, but the verifier is not able to determine which one. More concretely, given a ring signature and a group of d users, a verifier cannot distinguish the signer's identity with a probability more than 1=d. This property can be used to preserve the identity of the signer from a verifier.

VII. HARS

Homomorphic authenticators (also called homomorphic verifiable tags) are basic tools to construct public auditing mechanisms. The unforgeability, a homomorphic authenticable signature scheme, which denotes a homomorphic authenticator based on signatures, should also satisfy the following properties.

A. Block less verifiability

It allows a verifier to audit the correctness of data stored in the cloud server with a special block, which is a linear combination of all the blocks in data. If the integrity of the combined block is correct, then the verifier believes that the integrity of the entire data is correct. In this way, the verifier does not need to download all the blocks to check the integrity of data.

B. Non-malleability

It indicates that an adversary cannot generate valid signatures on arbitrary blocks by linearly combining existing signatures.

VIII. PUBLIC AUDITING

A. Reduce Signature Storage

Another important issue need to take consider in the construction of this scheme is the size of storage used for ring signatures. By the taxonomy of the ring signatures in HARS, a block m is an element of Z and its ring signature

contains d elements of G1, where G1 is a cyclic group with order p. t will be very frustrating for users, because cloud service providers, such as Amazon, will charge users based on the storage space they use.

To reduce the storage of ring signatures on shared data and still allow the public verifier to audit shared data efficiently, it exploit an aggregated approach to expand the size of each block in shared data into k bits.

IX. CONCLUSION AND FUTERE WORK

In this paper a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks.

X. REFERRENCES

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

[2]. ArmbrustM.andZahariaM. (2010), 'A View of Cloud Computing', Comm. ACM,vol. 53, no. 4,pp. 50-58.

[3]. Wang C. and Lou W. (2010), 'Code based for Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing', Proc. IEEE INFOCOM, pp. 525-533.

[4]. 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.