RESEARCH ARTICLE OPEN ACCESS

Integrity Privacy to Public Auditing for Shared Data in Cloud Computing

A.Mahaboob Basha[1], P. Venkata Maheswara[2]
[1]*M.Tech Student, Dept. of CSE, KMMITS, Tirupati*
[2]*Asst. Professor, Dept. of CSE, KMMITS, Tirupati*

ABSTRACT
In cloud computing, 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 .However, public auditing for such shared data— while preserving identity privacy — remains to be an open challenge. Here, 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.
***Keywords*:** Cloud Computing, Data integrity, Public Auditing, Privacy Preserving.

I. INTRODUCTION

Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand. It describes a new supplement, consumption, and delivery model for IT services based on the Internet. It has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its wide range of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

As such services provided by cloud service provider to cloud user, naturally the providers must have and rather can have access to resources which are used by the user. Among the reasons these access are greatly required are for maintenance perspective. As numbers of users are using such service provided by cloud service provider then the infrastructure ought to capable enough to support them and these resources ought to be shared between numbers of users. Data synchronization between number of users, service availability, and availability of data via any devices which includes browser facility make cloud more attractive

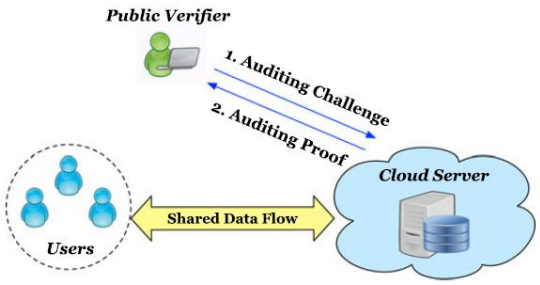


Fig: System architecture

We believe that sharing data among multiple users is perhaps one of the most engaging features that motivates 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 [1]. 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

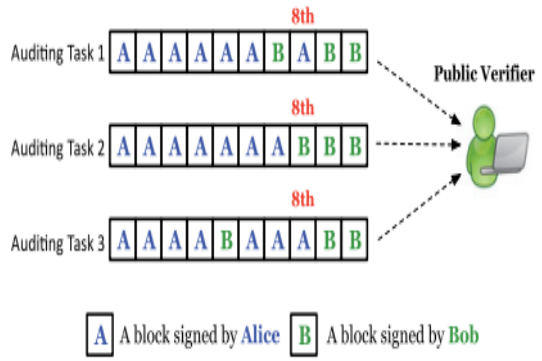


Fig.1. Alice and Bob share a data file in the cloud, and a public verifier audits shared data integrity with existing mechanisms.

II. PROBLEM STATEMENT

In our model, privacy is accomplished by allowing the parties to upload their data in multi clouds and data is split into multiple parts so it gives more protection

Scope: We are going to raise the privacy level of the data owner and the confidentiality of the data in a better way through the multiple cloud environment.

III. PROPOSED WORK

To enable the TPA efficiently and securely verify shared data for a group of users, Oruta should be designed to achieve following properties: (1) **Public Auditing**: The third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data. (2) **Correctness**: The third party auditor is able to correctly detect whether there is any corrupted block in shared data. (3) **Unforgeability**: Only a user in the group can generate valid verification information on shared data. (4) **Identity Privacy**: During auditing, the TPA cannot distinguish the identity of the signer on each block in shared data.

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. These 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 emailid 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 PartyAuditor Registration: In this module , if a third party auditor TPA(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 PartyAuditor 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 revoked during data sharing — while still preserving identity privacy.

IV. PUBLIC AUDITING MECHANISM

Working Methodology:

System Architecture Preserving Storage Data on Cloud using AES, Blowfish, SHA-1 Algorithm.

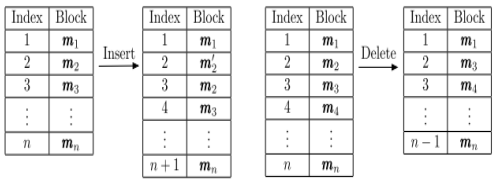
1. In our proposed methodology user store data to cloud. At the time of sending data to cloud it get encrypted by cryptographic algorithms.
2. That encrypted data transfer to the TPA.
3. TPA generates hash of that encrypted data.
4. That generated hash is stored along with TPA.
5. Then that encrypted data TPA will send to cloud.
6. When user wants to check integrity of data then user will send request to the TPA.
7. TPA forward that request to the cloud.
8. Cloud will generate the hash of requested file and send that generated hash to the TPA.
9. TPA fetches stored hash of that requested file and performs comparison in newly generated hash and stored hash.
10. If both the hash are equal then TPA transfer acknowledgement to the user. If both are equal then acknowledgement will be that stored data is as it is. If data get corrupted by cloud then acknowledgement will be that your data is corrupted.
11. Similarly, when user want to download data from cloud then user send request to the TPA to download data from cloud.TPA will transfer request to the cloud. Cloud accepts that request and send data to the user.

Ring Signature Scheme : As we introduce in this sections, we intend to utilize ring signatures to hide the identity of the signer on each block, so that

private and sensitive information of the group is not disclosed to public verifiers. However, traditional ring signatures [1], [2] cannot be directly used into public auditing mechanisms, because these ring signature schemes do not support blockless verifiability. Without blockless verifiability, a public verifier has to download the whole data file to verify the correctness of shared data, which consumes excessive bandwidth and takes very long verification times. Therefore, we design a new homomorphic authenticable ring signature (HARS) scheme, which is extended from a classic ring signature scheme [21]. The ring signatures generated by HARS are not only able to preserve identity privacy but also able to support blockless verifi- ability. We will show how to build the privacy-preserving public auditing mechanism for shared data in the cloud based on this new ring signature scheme in the next section.

HARS contains three algorithms: KeyGen, RingSign and RingVerify. In KeyGen, each user in the group generates his/her public key and private key. In RingSign, a user in the group is able to generate a signature on a block and its block identifier with his/her private key and all the group members' public keys. A verifier is able to check whether a given block is signed by a group member in RingVerify. Details of this scheme are described.

Using HARS and its properties we established in the previous section, we now construct Oruta, a privacy-preserving public auditing mechanism for shared data in the cloud. With Oruta, the public verifier can verify the integrity of shared data without retrieving the entire data. Meanwhile the identity of the signer on each block in shared data is kept private from the public verifier during the auditing.



(a) After inserting block m_2', all the identifiers after block m_2' are changed (b) After deleting block m_2, all the identifiers after block m_1 are changed

Fig. 2. Using indices as identifiers.

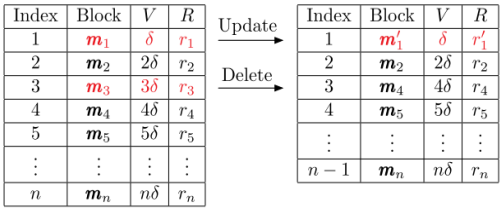


Fig. 3. Update block m1 and delete block m3 in shared data using an index hash table as identifiers.

Supports for data dynamics: As information in Cloud is dynamic, static auditing isn't enough. A dynamic auditing is required to verify the information integrity of the dynamic data. However as information square measure dynamic in cloud, it's dangerous to own associate degree auditing with efficiency. Server will enforce Replay attack and forge attack to fail the auditing method. The dynamic operations embrace modification, insertion and deletion. Whenever dynamic operation is performed, the owner sends the update message to the auditor representing the indicator of that message. The Auditor updates the table. The message m and therefore the tag square measure replaced by the new message and tag in message modification. The new message m and new tag square measure inserted in insertion operation. The message m and tag square measure deleted from the index table and every one the entries below the deleted message move upwards. After performing updates in the table, the auditor conducts the data integrity test for the updated data. Auditor sends the result to the owner and he deletes the local copy of updated data.

V. CONCLUSION

A system of privacy preserving public auditing provides security to data stored in cloud storage. The cloud storage is advantageous than earlier traditional storage system. In cloud storage requirement is to provide security to data stored on cloud. Our system uses encryption of data before storing it on cloud. Therefore data will be secured on cloud storage. The cloud user can check integrity of their data stored on cloud server using TPA. The TPA is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users. 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.

REFERENCE

[1] Boyang Wang, Baochun Li, and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud"IEEE TRANSACTIONS ON CLOUD COMPUTING,VOL. 2,NO. 1,JANUARY-MARCH 2014.

[2] Miss. Pratiksha Meshram, Prof. Roshani Talmale, and Prof. G. Rajesh babu " A System of Privacy Preserving Public Auditing for Secure Cloud Storage System" International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 8, August - 2014

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

[4] 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.