ORUTA: Privacy-Preserving Public Auditing for Shared Data in the Cloud

Puja Dalvi
Student
Department of Information Technology
Sinhgad Institute of Technology, Lonavala

Rohit Kelgandre
Student
Department of Information Technology
Sinhgad Institute of Technology, Lonavala

Varsha Chore
Student
Department of Information Technology
Sinhgad Institute of Technology, Lonavala

Pooja Das
Student
Department of Information Technology
Sinhgad Institute of Technology, Lonavala

Prof. R. S. Badodekar
Professor
Department of Information Technology
Sinhgad Institute of Technology, Lonavala

Abstract

With cloud analysis, it is typical for data to be put away in the cloud, as well as shared over multiple clients. Unfortunately, the integrity of cloud data is liable to suspicion because of the presence of programming disappointments and human blunders. In this paper, we propose a novel privacy-preserving component that discovers open auditing of shared data put away in the cloud. Specifically, we attempt ring marks to process check metadata expected to review the accuracy of data shared with multiple users. With our component, the endorser's character on every piece in shared data is kept private from third party verifiers, who have the capacity to proficiently confirm the shared data integrity without retrieving the whole document. Our trial results show the adequacy and proficiency of our component when auditing shared data integrity.

Keywords: Public auditing, privacy-preserving, shared data, cloud computing

I. INTRODUCTION

Cloud service providers offer users an efficient and scalable data storage service with a lower marginal cost than traditional approaches. It is routine for users to share data in a group, as data sharing becomes a standard feature in most cloud storage included Drop Box, iCloud and Google Drive.

The main reason is the size of data is large. Downloading entire data for verification is a waste, especially when data corrupted in the cloud. Besides, many users need not download the entire data. It is because cloud providers, such as Amazon, can offer users services directly on large-scale data that already existed in the cloud.

II. ARCHITECTURE

As illustrated in Fig.1 the system model, this paper involves three parties: the cloud server, a group of users and a public verifier. There are two users: the original user as Group Owner and The number of users accessing groups. The original user initially uploads data in the form of text file in the cloud, and shares it with group users. Both the original user and group of users are members of the group. Every member is allowed to access and modify shared data. Shared data And Signature is stored in the cloud server. A public verifier, Third Party Auditor sends the file to the admin for verification. Cloud Service Provider (CSP) generates the proof and sends the response to the Third Party Auditor.

When a public verifier wishes to check the integrity of shared data, it sends an auditing challenge to the cloud server. After it receives the auditing challenge, the cloud server responds to the public verifier with an auditing proof.

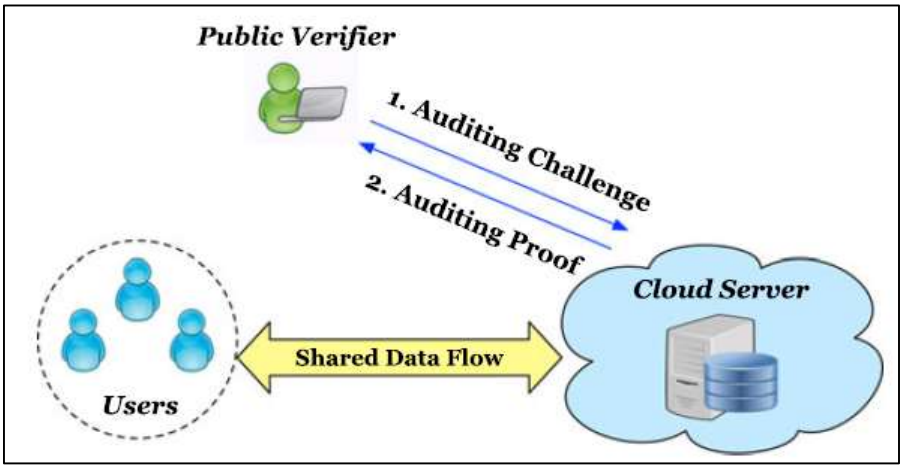

Fig. 1: System architecture

Three Steps
1) Challenge
2) Proof
3) Verify : 0/1 or Yes/No

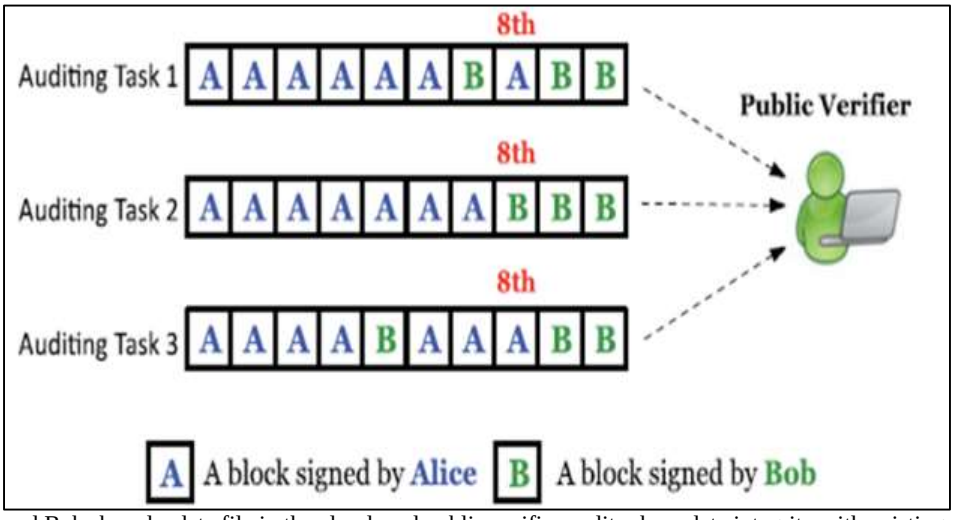

Fig. 2: Alice and Bob shared a data file in the cloud, and public verifier audits share data integrity with existing mechanisms.

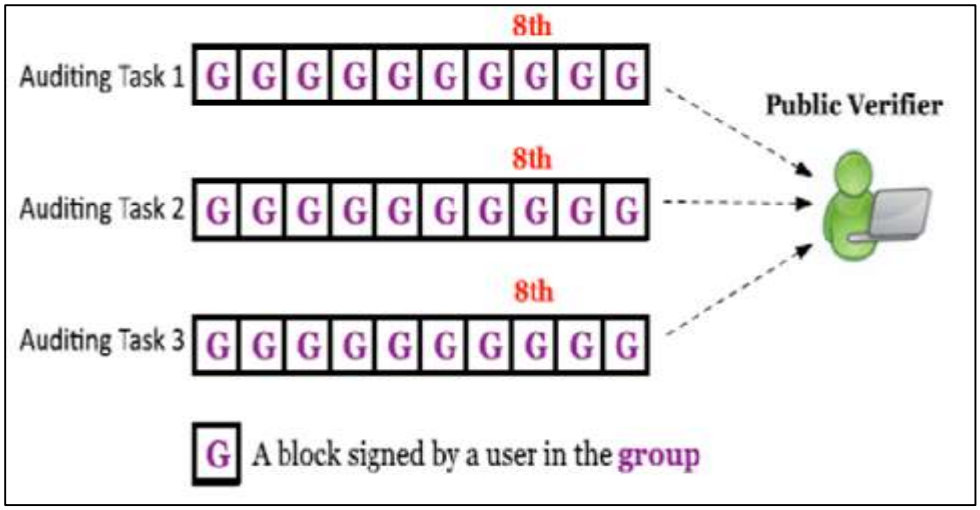

Fig. 3: Alice and Bob shared a data file in the cloud, and public verifier audits share data integrity with ORUTA.

A. Comparison with Existing Systems:

Table – 1
Comparison

	PDP	WWRL	Oruta
Public Auditing	YES	YES	YES
Data Privacy	NO	YES	YES
Identity Privacy	NO	NO	YES

B. Existing System:

The First Provable Data Possession (PDP), the public auditing is done by correcting the data which are stored in entrusted server. It is done by without retrieving the entire data.

Wang ET all has been used WWRL in this paper. It is designed to perform public auditing mechanism; the content of the private data belonging to the personal user is not disclosed to the third party auditor.

1) Disadvantage Of existing System:

Failing to preserve identity, privacy on shared data

C. Proposed System:

In this paper, to overcome the security issues on shared information, we propose Oruta a novel signature we use the ring marks to build homomorphic authenticators in Oruta. Oruta is perfect with arbitrary concealing, which has been used in WWRL.

1) Advantage of Proposed system:

– Public verifier is able to correctly verify the shared data.
– Public verifier cannot distinguish the identity of signer on each block.
– The ring signature generated is not only preserving the identity privacy but also able to support block less verifiability.

III. MATHEMATICAL MODULE

Let S be the whole system S={I,P,O}
I - input
P - procedure
O – output
Input I={GU,PV,CSP,F}
Where,
GU – Group User
PV – Public Verifier
CSP – Cloud Service Provider
F – Files F = {f1, f2…, fn}

1) Step 1 Group User (GU):

There are two types of users in a group: Original user and number of group users. The original user initially creates a shared data in the cloud, and shares it with user. Both are members of the group.

Every member of the group is allowed to access the data and also modify the shared data. Shared data and its verified metadata (i.e. signatures) are both stored in the cloud server.

2) Step 2 Public Verifier (PV):

A public verifier, such as a third party auditor provides expert data auditing services on a shared data.

Publicly verify the integrity of shared data stored in the cloud.

When public verifier wishes to check the data integrity, it first sends the auditing challenge to the cloud server provider.

3) Step 3 Cloud Server Providers (CSP):

After receiving the auditing challenge, the cloud server responds to the public verifier with an auditing proof of the proprietor shared data.

These public verifiers check the correctness of the entire data by verifying the correctness of the auditing proof one by one.

The process of public auditing is a challenge and response a protocol between a public verifier and the cloud server.

IV. METHODOLOGY

A. Ring Signature:

The concept of ring signature is first proposed by Rivest et al. in 2001. By ring signatures, a verifier get convinced that a signature is computed using a private key of one of group members, but the verifier is not able to get which one has uploaded. By this we can preserve the identity of the signer from a third party verifier.

The ring signature scheme is introduced by the Boone et al. is constructed on bilinear maps.

B. Algorithms:

Homomorphic Authentication Ring Signature contains three algorithms: Key Generation, Ring Signature and Ring Verify.
In Key Generation, Each user contains his/her public key and private key.

In Ring Signature, users in the specific group are signature to block calls ring signature. it is distinguished by its own private key.

A verifier checks whether the block is signed by a group member or not and send verification details

C. Construction of ORUTA:

ORUTA means One Ring to Rule them All.

We provide the privacy on shared data by assigning one ring to the group of users so that when a User uploads file Third party auditor never recognize the user identity.

Uploaded file contains its file id .The third party auditor have information only about file id, generated hash value and ring signature.

Now, we present details of our Public Auditing Mechanism as follows:

- It includes five algorithms: Key Generation, Sig Generation, Modify, Proof Generation and Proof, Verify.
- In Key Generation, user generates its own public/private key.
- In Sig Generation, a user is able to computing ring signature blocks in shared data by using its own private key and group member's public keys. Each user is able to perform operation like insert, update or delete on each block, and assigns signature to the block which is modified.
- Proof Generation is operated by both public verifier (Third Party Auditor) and cloud server (admin) together to generate the proof.
- In Proof Verify, The public verifier (third party auditor) audits the integrity of shared data by verifying the proof and sends the response.

D. Modules:

1) Owner Login: In this module, any of the above mentioned people have to login, they should login by giving their email id and password.
2) User Registration: In this module if a user wants to access the data on a cloud, he/she should register their details first. These details are maintained in a Database.
3) User Login: If there is authorized user, he/she can download the file by using its file id which has been stored at the time of uploading.
4) Owner Login: In this module, any of the above mentioned people have to login, they should login by giving their email id and password.
5) Third Party Auditor Login: By login, He/ She can see how many data owners have uploaded their files into the cloud. Here we are providing the Third Party Auditor for maintaining three different clouds.

V. PROPOSED OUTCOMES

We Exert the Ring Signatures to construct homomorphic authentication, so that a public verifier is able to audit shared data integrity without recovering the entire data, yet it cannot distinguish who is the signer.

VI. CONCLUSION

We propose Oruta, a privacy-preserving public auditing mechanism for shared data in the cloud. We exert ring signatures to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without recovering the entire data, yet it cannot distinguish who is the signer on each block.
To increase the efficiency of verifying multiple auditing tasks, we extend our mechanism to support batch auditing.

ACKNOWLEDGEMENT

We would like to thank our guide and Project Coordinator Prof. R.S Badodekar, Our Head of Department Prof. N.A. Dhawas and all the people who support us.

REFERENCES

[1] B. Wang, B. Li and H. Li, "Privacy preserving public auditing for shared data", Proc. IEEE fifth Int'l pp.295-302, 2012 2014.
[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R H. Katz, A. Konwinski, G. Lee, D.A. A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud Computing". Vol. 53 , no. 4, pp. 50-58, Apr. 2010.
[3] K. Ran, C. Wang, and Q. Wang, "Security challenges for the public cloud", IEEE internet computing, vol. 16, no. 1, pp. 69-73, 2012.