ORUTA: PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

[1]Ediga Lingappa, [2]Arun Kodirekka, [3]Syed Mohammed Shafi, [4]Patur Ganga
[1,2,3,4]AssistantProfessor, Department of Computer Science and Engineering,
Malla Reddy College of Engineering, Hyderabad.

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.

Key Words: Provable Data Possession, Third party Auditor, Hybrid Cloud

Existing System:

The first provable data possession (PDP) mechanism [2] to perform public auditing is designed to check the correctness of data stored in an un trusted server, without retrieving the entire data. Moving a step forward, Wang et al. [3] (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.

Disadvantage:

Data is not in an encrypted format.

Proposed System:

In this paper, we only consider how to audit the integrity of shared data in the cloud with 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**.**

Advantage:

Here we proposed the secured system and data owner can decide whether the user can access the system or not.

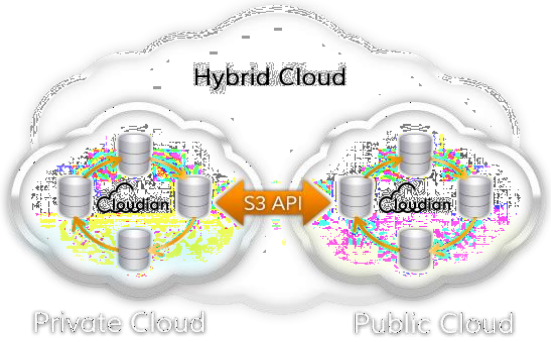
PROBLEM STATEMENT:

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.

Architecture:



ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-11, 2017
DOI: 10.21276/ijcesr.2017.4.11.42

Modules :

1. Owner
2. Third Party Auditor
3. User
4. Data Sharing

Modules Description

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 email id 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 Party Auditor 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 Party Auditor 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.

Proposed System:

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) Enforceability: 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.

System Configuration:-

H/W System Configuration:-

Processor - Pentium–
Speed- 1.1GHz
RAM - 256MB
HardDisk - 20GB
Floppy Drive - 1.44 MB
Key Board - Standard
Windows Keyboard
Mouse - Twoor
Three Button Mouse
Monitor- SVGA

S/W System Configuration:-

- OperatingSystem :Windows95/98/2000/XP
- Front End : Swings &AWT
- Scripts : JavaScript.
- Database : My sql
- Database Connectivity : JDBC.

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-11, 2017
DOI: 10.21276/ijcesr.2017.4.11.42