Integrity Verification of Shared Files on Cloud Computing

Jadhav Ganesh Arun[1] Khan Samim[2] Naikwade Pravin Ramesh[3] Shaikh Shahrukh[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Shatabdi Institute of Engg. & Research, Agaskhind Nashik, Maharashtra, India

Abstract— On cloud we can store and share files. In cloud, there is Third Party Auditor (TPA) which performs auditing of shared files. While auditing, it may happen that some data will be visible to TPA, the TPA may misuse it. In this paper, we proposed a system that will assign rights of TPA to the user who shares the file. This will reduce the significance of TPA form the existing system.

Key words: Signature Generation, Encryption, Signature Generation, Signature Verification

I. INTRODUCTION

This paper is mainly concern about providing security for files on cloud. The recent work in this field inspired us to develop a mechanism that will provide security at the user level.

The Cloud service providers give a centralize access to our files. Sharing feature bring challenges related to security and integrity.

There is a Provable Data Possession (PDP) mechanism that is used to check the correctness of data on untrusted cloud, without accessing the whole data. When we share file, we give access to edit the file content. Any Group user can edit the content of file. This will raise the problem of identity privacy. One way is to allow user to sign the particular block they edit.

In the current system, there is a Third Party Auditor (TPA) that is responsible for performing auditing of the shared file. When a file is shared, you give right to edit and delete the content of the file to the group users. The TPA will keep the record of user who edited or deleted the content of file. For this, the TPA has to look each and every block of file. As in most cloud system the encryption is not provide the content of file are exposed to the TPA. The TPA may misuse the data. In our system, we give the rights of TPA to the user who share file, so that all the auditing will be perform.

II. SCOPE AND OBJECTIVES

A. *Scope*

We are going to increase the degree of security and confidentiality of data at the user level.

B. *Objectives*

- User Level Auditing: The auditing is also provided at the user level.
- Security: File is encrypted uploading on cloud.

III. PRESENT THEORIES AND PRACTICE USED

For identity verification, there is a Provable Data Possession (PDP) that will determine the correctness of data across cloud.

There one more method used in practice, developed by Wang et al. which will not disclose the content of private data belonging to the particular User to TPA.

Oruta is a method in which will keep confidential the identity of each signer of block from TPA. In Oruta they used combination of Ring Signature and Homorphic Authenticators, Called Homomorphic Authenticable Ring Signatures. This method will hide the identity of signer from TPA.

Another method is Preserving cloud computing Privacy (PccP). In this, the privacy is provided using layered approach.

The first layer is the Consumer Layer which form a base for the model, where the request form the user comes. The second is the Network Interface Layer, where the IP Address of the request owner is modified. Next is the top most layer of model which has privacy check mechanism.

The most common approach is to give the auditing work to a Third Party Auditor (TPA). The TPA is used to do the auditing of shared file over the cloud. The TPA check the each and every block of file for its signer. For this the TPA has to access the entire data of file and to check each block identically. As the files on most cloud are not in encrypted format, the content of file are visible to TPA. This is risky if the file contains any confidential data, the TPA may misuse it. So to provide the identity privacy, most of the Cloud service providers are providing encryption for file.

One method is to provide the attributes to User, who shared file, about providing access controls to the user in the group. It is similar to the providing access permissions to the files.

Cloud is also used for backup purpose, one can store the whole backup of its system on cloud. The users are storing the important Backups on untrusted cloud. So security is an important parameter.

IV. EXISTING SYSTEM

In the existing system, TPA perform the auditing task, let's take an example, where a file is shared in two group users, say Steve, John. The shared file is divided into small blocks. Once the file block is shared among users, they modify these blocks. After modification, the user has to sign each and every block they modified using his/her public/private key.

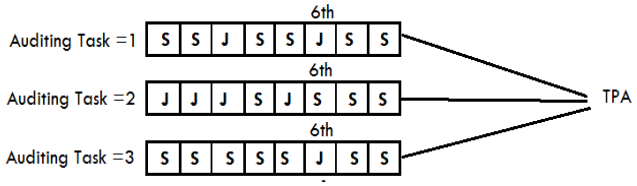

Fig. 1: Existing System

Here S for Steve and J for John. In the Figure 1. There are three blocks which are edited by Steve and John. The blocks they have edited are signed them and they are indicated by their initials in the figure. TPA will access each block and will check for edited blocks and will perform auditing based the signature.

The TPA can also see the data which is signed by the group user.

In the above example, we can see that the 6th element is edited frequently by the user Steve and John. While auditing the TPA will come to that this 6th block is edited frequently. So Based on that, the TPA can draw a conclusion that this block has any important data, may be the final bid from the auction. As the TPA can see the data, it can misuse or change the content of that block. This is because the encryption is not provided on some cloud systems. This is a drawback of existing system. But some cloud are using encryption for the files of user.

V. PROPOSED METHOD

In our approach, we have implemented a system on users system. Instead of encrypting the file on the cloud, our software will encrypt the file before uploading it on cloud.

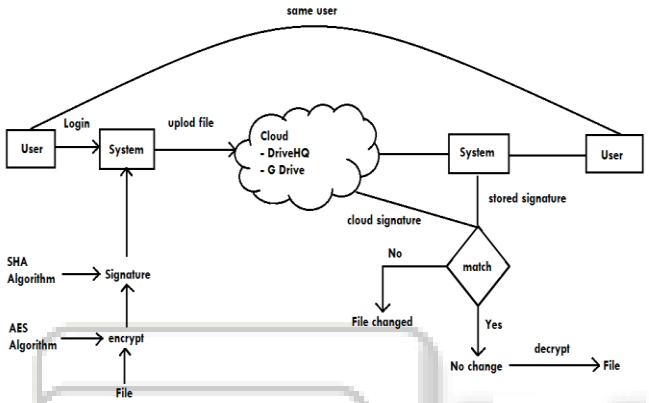

Fig. 2: Block diagram

A. User Login

Using the login and password of cloud account user will login into the system.

B. File Selection

After login the user will select file which is to be uploaded on cloud.

C. Encryption

Now the system will encrypt the file using AES algorithm.

1) Procedure:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (cipher text).

D. Signature Generation

After Encryption, the signature is generated for whole file. Using SHA-1 Algorithm. And the signature will be stored on the users system.

E. Signature Verification

When the user download the file from cloud, the system will calculate the signature of file. Then the calculated signature is compared with the one stored on system. If both signatures matches then user will come to know that the file is not changed and if the signatures does not match then user will come to know that the file is changed.

Our system will provide the security and integrity check at the user side. This will give the rights of TPA will to the user. After the user will come to know that the file is not changed, then the system will decrypt the file. The original and edited content of the file will be shown to user. As the file uploaded on cloud is in encrypted format the TPA will not able to see the content of file, while auditing.

REFERENCES

[1] 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, pp. 525–533.

[2] Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Stroage Sys- tems," in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp. 31–42.

[3] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in Proc. ACM Symposium on Applied Computing (SAC), 2011, pp. 1550–1557.

[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, pp. 552–565.

