Privacy Preserved Public Examining System for Information Sharing In Cloud

[1]PRAKASH J, [2]RAJALEKSHMI J, [3]YATHISH G, [4]SHARADA

[1]UG Student, [2]Assistant Professor, [3]UG Student, [4]UG Student
Computer Science and Engineering,
Rajarajeswari College Of Engineering,Bangalore,India

***Abstract*—-Storage in cloud creates one of the tough managements, since clients without much of a stretch can offer and adjust information with others in cloud. The constancy and security of shared cloud information is ineffective. Specifically, keeping in mind the goal is to reduce the burden on clients, a third party auditor (TPA) is specified to lead the confirmation, which is called public auditing. In any case, the TPA may have pointless access to private data amid during the examining process. With information storage and sharing administrations in the cloud, clients can without much of a stretch adjust and offer information as group. Here for the most part correspondence concentrated on between the gathering of clients and server. Here we propose a security protected public auditing system for shared cloud information by developing a holomorphic verifiable group signature.**

Index Terms-TPA, Holomorphic Verifiable, Public auditing.

I. Introduction

The Cloud computing is a model for permitting administrations, clients universal, advantageous and on-request network access to a mutual pool of configurable computing resources. Cloud is a developing technology to facilitate developments so large scale and flexible computing infrastructure. Cloud computing is a sort of Internet-based figuring that gives shared PC resources and information to PCs and different devices on request. The information rises up out of the cloud where it might be encapsulated, interpreted and transported in bunch routes in the same format as when it entered the cloud. Since cloud servers are helpless to unavoidable equipment defects, software failures or human mistakes, information stored in the cloud might be lost. In the most crucial scenarios, a cloud owner may even conceal information mistake accidents so asto save its reputation. Also, clients who lose direct control over their information don't know whether their cloud-stored information is in place or not. In this way, integrity verification for the shared information in the cloud is important, yet opportune issue for countless clients. To guarantee the integrity of information stored in cloud servers, various systems in view of different strategies have been proposed. Specifically, keeping in mind the goal to reduce the burden on clients, a Third party auditor (TPA) is engaged in to direct the confirmation, which is called public auditing.

II. Related Work

An effective and flexible distribution scheme use two way handshakes based on token management. By operating the holomorphic token with scattered verification of erasure-coded data and achieves the mixing of storage correctness insurance and data error localization to identification of misbehaving server [1]. Architecture would provide to both customers and service providers and give anoverview of recent advances in cryptography motivated specifically by cloud storage. The major technique is information sharing theme to secure multi-owner. User revocation will achieved through a completely unique revocation list will not change the key[2].In cloud storage auditing, to reduce the damage of the client's key exposure in cloud storage auditing, and give the first practical solution for this new problem setting. A protocol employ the binary tree structure and the preorder traversal technique to update the secret keys for the client[3].Author propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind by utilizing the idea of proxy re-signatures and allow the cloud to re-sign blocks on behalf of existing users during user revocation, hence existing users do not need to download and re-sign blocks by themselves[4].The two technologies used for providing security in cloud computing: Multi-tenancy and Virtualization. Multi-tenancy provides multiple residents sharing its resources from physical machine and creates remote environment for each. Virtualization running multiple operating systems on a single device at the same time frame. The quality of service is the responsibility for storage allocating and computing [5].

III. Proposed System

In this paper we propose a privacy preserved public examining system for shared cloud information by developing a holomorphic group signature. We think about a group key agreement with a nearby availability where a client is just aware of his neighbors. In our concern, there is no central authority to introduce clients. A group key agreement for this setting is extremely appropriate for applications, for example, a social network. If the revoked clients plan with the cloud, the private keys of the current clients can be

gotten by the cloud. In this manner, the cloud can mess with the mutual information stored in it arbitral.
To guarantee the integrity of the shared information, a few plans have been intended to permit public verifiers (Third party auditor) to proficiently review information honesty without recovering the whole clients' information from cloud. To guarantee shared information respectability can be checked freely, clients in the gathering need to figure marks on every one of the pieces in shared information.

IV. Problem Definition

Here we are discussing about privacy preserving security based data storage management using group data. Facing more challenges on data transferring mechanism and therefore, the problem of information traceability and also should be considered.
Consequently anybody can challenge the cloud for the examining proofs. This issue will trigger network congestion and misuse of cloud resources. Another issue is that the group clients should have the capacity to progressively enlist and deny the gathering, which will be managed by the group manager.

V. System Architecture

Fig Architecture Diagram

In the above architecture diagram the data owner will choose the file and encrypt it and upload it to the cloud server. When the data user wants to download the file, he has to choose the file from the list and need permission to download the file, where the permission was given by data owner. While uploading the file by data owner will generate a secret key to the file which has to be given to the data user when he need to download the file.

V1.MODULES

1.Profile Generation

Profile generation is one of common security model. Here data owner and data consumer has login to the account with access our personal cloud storage data. Here auditing files with
security mechanism implemented and previous step as profile detail verified with completed authentication process. Every User has Register into the cloud on data storage at beginning level. Cloud is developing technology to be used on security purpose. When the user details as username and password are match.Then only forwarding next process.

2.Group Member Login

This is another security model for implementing types of user as data owner and data consumer. Here all type of user has to be need the login to the access the group files but before they are access to the group member. Here every user to select the grouping to join the group with sharing some particular files between the group of peoples. Then admin is the controller for the group.

3.View User Profile

Here every user has registering to the cloud storage data. User has seen to our profiles automatically and sometimes to be updating user manual details to be updated. View profile status with respective to the results of username and which type of group to be related person and what are the facilities to be configured to send and retrieve the files to be processed. User information are updated and maintained systematically.

4.File Transferring to Server

Here File transformation is one of most crucial part of cloud data storage management system. File Uploaded to server with encryption data or raw data with checking and after the data is certain keys or here using group key based data is stored on cloud server. Data owner or Group owner having unique key to communicate with group users and other group users. Data owner can upload data to its group members and store the files into storage server. View files contents of uploaded files in storage server.

5.Set Access Permission

Access permission is the main model for data processing system. Here when the data consumer or another group user has to go for download the grouping files with get the access permission for certain group admin or group members. So access control mechanism with checking the given files are access with get permission or not to be validated.

6.Retrieve Storage data

File download is data consumer or end user has access the particular data with checking uploading list data views based and get the permission for access the files on cloud server. File downloading with group user information has send to several group of user revocations to the cloud storage management.

V11. RESULTS

1.User login Frame

Fig User Login Frame

The above frame is used to collect the information of user name, password and the group number(group1,group2 or group3) from the user and upon clicking log in button it connects to the database and executes select query to find if a row of a particular user exists ,if row exists go to new frame else display error message. Upon clicking on new user button it takes user to the new frame for registration. Upon clicking close button it dispose the current frame.

2. User Registration Frame

This frame collects user name, password, place and group number from a new user and upon clicking register button it connects to a database and validates inputs given by user and executes insert query to add a new row in to a table, displays message upon successful insertion. Upon clicking go to log in button it takes to user log in frame.

\

Fig User Registration Frame

3.Data Owner File Upload

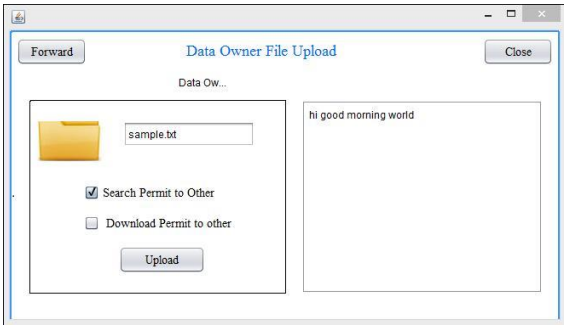

Fig File Uploading Frame

This frame is used to upload a file by the data owner to the cloud. On clicking the folder label in the above frame file browser will be opened for the user to select a file to upload and the contents of the file are displayed in the large text box which is present at the right side of the frame. There are two check boxes which are used to give search and download permit by owner. Upload button is used to prepare for uploading data into the file. And by clicking the close button the current frame will be disposed.

4.Data Consumer Login

Fig. Data consumer Login Frame

The above frame is used to collect the information of consumer name, password and the group number (group1,group2 or group3) from the data consumer and upon clicking log in button it connects to the database and executes select query to find if a row of a particular data consumer exists ,if row exists then go to download page else display error message.

5.File Download

This frame is used to download the file contents by the data consumer. It contains mainly two large text area where one will display the list of files uploaded by the data owners and other text area will display the contents of the file in decrypted format after clicking download button by the end user**.**

6.Auditors Frame

This is a auditors frame where it contains view option on clicking we can see the list of group users , we can view the permission request and list of files.

.

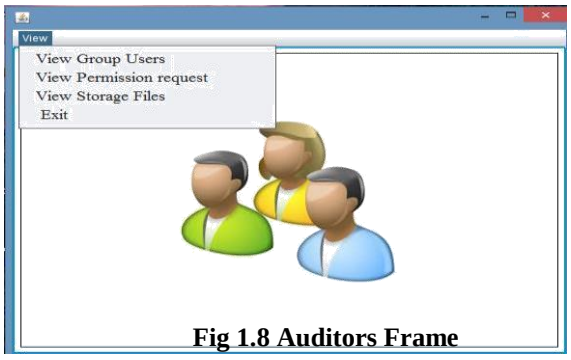

Fig 1.8 Auditors Frame

V111.Conclusion

We propose a novel multi-level security preserving public auditing system for cloud information sharing to various managers. The procedure of examining, the TPA can't acquire the characters of the signers, which guarantees the personal protection of the group clients. Unlike the existing system the proposed system requires t group managers to work together to trace theidentity of the misbehaving user.

References

[1].C. Liu, J. Chen, L. Yang, et al, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates," IEEE Transactions on Parallel and Distributed Systems, 2014.

[2].S.Kamara, and K. Lauter, "Cryptographic cloud storage"(2015).

[3].J. Yu, K. Ren, C. Wang, et al, "Enabling Cloud StorageAuditingwithKey-ExposureResistance,"IEEE Transactions on Information Forensics and Security, vol.10, no.6, pp. 1167-1179, 2015.

[4].B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud, "Proceedings of IEEE INFOCOM, pp. 2904- 2912, 2013.

[5].D. Fernandez, L. Soars, J. Gomes, et al, "Security issues in cloud environments: a survey," International Journal of Information Security, vol. 12, no. 2, pp. 113-170, 2014.