Secure Multi Owner Data Sharing For Dynamic Groups in the Cloud

Priyanka Pujari, Prof. A.S.Shahapurkar

***Abstract*— Cloud computing is a platform that provides an efficient solution for sharing of data. Users can save investments on local storing of data by moving the data onto the cloud. However sharing data while preserving the identity privacy and confidentiality of data in a cloud is a challenging task. Therefore a secure scheme for sharing data among groups is being proposed. To support dynamic groups where new registered clients can access the files uploaded without contacting the owner and preserve the confidentiality of data by encrypting the file and then uploading the encrypted file.**

Index Terms— Cloud computing, data encryption, dynamic groups.

I. INTRODUCTION

In cloud computing various services can be provided to cloud users with aid of datacenters that is powerful. Datacenters provided by cloud companies provide cloud computing, it's hosting and outsourcing solutions via the data centers [1]. Users can appreciate quality services and spare purchases on neighborhood infrastructures by moving neighborhood management systems in cloud servers as it provides storage as a service. Cloud computing is a platform which provides lower cost storage of data and is accessible online.

Valuable information, software's and shared resources are given to personal computers and other gadgets as Cloud processing is Internet based computing. Foundation of trust that is needed between the information subject and company depends upon on how the sincerity of the data is securely maintained. Cloud is one which brings about many issues that have impact and great influence on the security and execution of entire framework.

With cloud information storage in abundance, the verification of information sincerity in an untrusted storage space is one of the primary concerns. To save money and space for storage supplier might fail to keep intact the documents or purposely erase seldom used information that may belong to a common client [1]. The problem can be generalized as to the way the customer can locate effective way to perform periodical confirmation of the information without the duplicate copy of information files stored in the system.

An illustrated application scenario of secure data sharing is shown in Fig. 1 [3]. A simple solution to save information protection is to encode the information, transfer the scrambled data into cloud which is safely utilized by cloud clients. Planning an effective and secure information sharing methods for groups in cloud is not a fairly process due to the accompanying challenging issues:

- Maintaining the identification privacy of clients.
- Single Owner.
- Dynamic characteristics of groups.

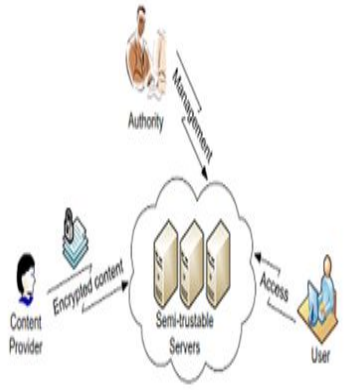

Fig. 1: An example application scenario of data sharing.

To overcome the above referred challenges the scheme secure multi proprietor information sharing for groups that is dynamic is being proposed.

It includes the following:

1) Multi owner information sharing plan that is secured:-Any range of registered clients can securely reveal data with others in group by untrusted cloud.

2) Assist dynamic groups effectively: - New allowed users can specifically decode the documents transferred before their participation without actually informing data owners.

3) Provision of secure and personal data access control as any client in a group can secretly utilize cloud assets. However, identities of information proprietors can be uncovered when disputes occur by the group manager.

II. LITERATURE SURVEY

K.Marimuthu et.al [1] proposed that identity privacy is one of the important challenges in cloud computing. Users may be unwilling to join in cloud computing without the guarantee of their identity privacy because their private information will be easily disclosed to cloud providers and attackers.

Hence anonymity and traceability [9] factors are highly desirable in any system and the authorized group manager should have the ability to reveal the identity of the inside attacker.

Manuscript received June 30, 2016

Priyanka Pujari, Department of Computer Science and Engineering, GIT Belagavi

Prof. A.S.Shahapurkar, Department of Computer Science and Engineering, GIT Belagavi

B.WAN et.al [4] proposed KNOX, an auditing scheme for preserving privacy of shared data with large groups in the cloud. To check the correctness of shared data the KNOX makes use of group signature to check the verification information on the shared data, but they cannot find the identity of the signer on each block of data therefore they will not be reveal the identity of the inside attacker whenever disputes occur as they cannot identify the signer on each block of data.

The original user can efficiently add new users to the group, edit the information of the group data and can disclose the identities of signers on all blocks but with the help of the group manager's private key. The efficiency of KNOX is that it is not affected by the number of users in the group.

Hasan Omar Al Sakran et.al[5] conveyed that the number of businesses using cloud computing has increased dramatically due to attractive features such as low costs, Speedy startup, flexibility, low maintenance cost and scalability. Some of the biggest challenges in the

III. EXISTING SYSTEM

For information sharing on the servers that are untrusted, few secured plans have been proposed. Owners of data store encoded files in a storage that is not actually trusted and then disperse comparing decoding keys to clients who are approved in the existing framework [3]. The renouncement and the user participation complexities in these existing frameworks are expanding linearly though with quantity of blocked clients and the owners of data.

3.1 EXISTING SYSTEM DISADVANTAGES

1) Maintaining essential credentials of clients that are private is a challenging hazard in distributed computing.
2)Single proprietor plan as administrator has capacity to store in information and change information in cloud and others can just access the files without adjusting any information.

3) Groups are usually in practice dynamically changing for Eg, client investment in the group or user revocation from the group. The adjustments in the membership in the group can make secure information sharing to a great degree difficult.

IV. PROPOSED SYSTEM

In this report a protected multi proprietor information sharing plan for dynamic groups is being proposed where a client can share information data within the group without uncovering their credentials to the cloud. The proposed framework enables a client to search for encrypted data at the public cloud while ensuring the security of the information [4].

4.1 ADVANTAGES OF THE PROPOSED SYSTEM

1) Secure information sharing in a multi owner plan suggests that any enrolled client in the group can impart information to others securely and can also modify the data files transferred on the cloud.
2)The proposed framework is able to support gathering of members that are dynamic where enlisted clients can decode the files transferred on the cloud without reaching with the owners of data and revoked cannot reach the information documents once expelled from the group.
3) Any person in allotted group can namelessly use cloud assets, thus providing a privacy enabled access to clients.

4.2 DESIGN GOALS OF THE PROPOSED SYSTEM

The outline goals [6] of the proposed framework are depicted as follows:
1) Access control: Necessities of control access are of two methods. Firstly the enlisted individuals in the group should be able to effectively utilize the cloud assets for information operations. Secondly, blocked clients should be unequipped for utilizing cloud once they are denied.
2) Information secrecy: It needs different clients including the cloud be denied of content learning of substance information.
3) Traceability and Anonymity: Ensures that enlisted members can use the cloud assets by not revealing their credentials. In spite of the fact that it represents an inside danger to frameworks. Eg, an inside assailant in the group may catch hold of critical data as to pick up advantage [4]. During such occasions Administrator should have capacity to follow the credentials of client.
4) **Productivity**: Client can impart records utilizing the cloud and further Clients can be denied of content access without the involvement of remaining clients.

4.3 CHALLENGES OF PROPOSED SYSTEM

The proposed framework has the following challenges:
1) Maintaining the Identity security of the clients as it is effortlessly unveiled to cloud suppliers and hackers.
2) Maintaining confidentiality of the data files stored in the cloud as it may be sensitive.
3) An inside assailant may gather beneficial data or credentials of user to infer considerable advantage. Group administrator should be able to trace the real identities of data owners when an extensive number of clients are accessing the cloud.
4) Preventing unauthorized decoding of the information files stored in cloud by clients.
5) User renouncement accomplishment without involvement of remaining owners of data.

V. SYSTEM ARCHITECTURE

The system architecture of the system is shown in Fig. 2. It shows the working of the system as to how users are registered for using the cloud by the group manager. The data on the cloud can be uploaded, downloaded and edited in a multi owner manner. The group member's account is removed by the group manager. The files are uploaded on the cloud in an encrypted
form for security measures.

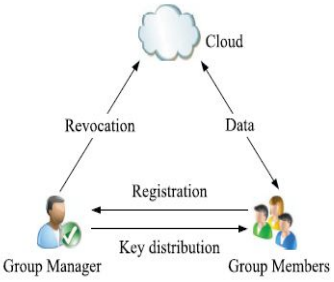

Fig.2: System architecture

VI. SIMULATION WORKS /RESULTS

A. Cloud Module

A nearby cloud that provides no less service is being created. The clients can transfer their data from system onto cloud. But however, the cloud is not in trusted perspective for the clients since the cloud service suppliers are prone to be not so believable to clients.

It is assumed by the cloud users that the cloud is straightforward but is bit interested i.e. cloud will not erase the content of client information but will try to sneak through the credentials of clients this is what is believed. It might misuse the information put away bringing about substantial benefit.

B. Group manager Module

The administrator is assumed as a trusted authority in the gathering of clients known to all. The admin is the chief assigned the reliable task of looking after all operations [8].

Administrator as a supervisor takes sole responsibility of the following:

1. Generation of all essential parameters of system.
2. Enlistment of clients.
3. Creating groups.
4. Allotting R/W permissions of the files to the users.
5. User renouncement.
6. Disclosing the credentials when dispute occurs.

C. File Security Module

1. Encoding the data record transferred on cloud either by supervisor or group member [10].
2. User can download the encrypted file only if given a decryption key and can transfer record file into cloud server using a key which is encoded. File records put away in cloud can be erased either by gathering supervisor or group member.

D. Client denial process Module

Blocking of clients is performed by supervisor based on which the group member cannot perform any data operations using the cloud server or decrypt the data files uploaded on the cloud and guarantee secrecy that is needed against denied clients.

E. Group Member Module

Group members are a bunch of enlisted clients who impart their record files into cloud and impart same them with others in gathering who are also registered in the same groups by the group manager.

The group enrollment is changed because of new participation or members leaving the group. The group members have legacy of changing records. The owners of data can liberally view records which are transferred and can also do some adjustment in the decoded records given the permissions by the group manager.

During accessing the cloud, the user interacts with the cloud server without any external interference and is assigned full authority on its own data [2]

CONCLUSION

In this paper a secure method for access control will be provided to clients. It ensures that any member can anonymously make use of cloud assets. However the credentials of clients will be traced as soon as administration finds some disputes occurring. Data is shared in a multi owner way where the users can not only access the files but can also edit, delete and modify records.

File permissions to the users are allotted by the manager for secure sharing of recorded information. Clients are effortlessly denied by manager without disturbing keys of remaining clients. Enlisted clients can make use of information records once enrolled without actually reaching the information owner and unapproved clients are disallowed to utilize the information records.

FUTURE ENHANCEMENT

In future work, subgroups can be created within the groups. User image can be captured while entering the encryption/decryption key for second level security. Increasing the number of backup group manager so as to share the workload among multiple group managers.

REFERENCES

[1] K.Marimuthu and D.Ganesh Gopal, "Secure DataSharing for Dynamic Groups in Cloud", IEEEInternational Conference Technologies, 2015.

[2] Hong Liu, "Shared Authority Based Privacy–preserving Authentication Protocol in cloud Computing", IEEE transactions, January 2015, pp.243-245.

[3] Xuefeng Liu, Yuqing Zhang, Boyang Wang, andJingbo Yan, "Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IJERA, January 2015.

[4] Boyang Wang, Baochun Li, Hui Li, Member,"Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", January 2015, pp. 94-95.

[5] Hasan Omar, "Accessing secured data in cloud Computing environment", IJNSA, January 2015, pp.23-25.

[6] Xinyi Huang, Joseph K. Liu, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", IEEE transaction, April 2015, pp.971-972.

[7] M.Malarvizhi, J.Angela, T.Revathi, "Secure File Sharing Using Cryptographic Techniques in Cloud", IJNSA Vol.8, No.1, April 2015.

[8] F.Femilshini, V.Ganeshkarthikeyan, S.Janani,"Privacy preserving revocation updates protocol for Group Signature in cloud", ICETECH, 20th March 2015, pp. 3-7.

[9] Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", 2010, pp. 282-292.