SECURE DATA SHARING FOR DYNAMIC MULTI OWNER IN CLOUD STORAGE

Ritu A. Rangari
Lecturer, Department of Computer Engineering, Manav School Of Polytechnic, VYALA,
Tal. Balapur Dist. – Akola India

ABSTRACT

The main purpose of this paper is to share the data on cloud. In this paper, we present that how to share data securely, reliably, and flexibly on cloud storage and how to manage their integrity while sharing on cloud. By using group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. To conserve data privacy, the main solution is to encrypt data files, then upload the encrypted data into the cloud. In Secure Sharing of Data for Dynamic Multi Owner in we design a secure data sharing scheme for dynamic group of company in an untrusted cloud.

Keywords: Cloud Computing, Data Sharing, Dynamic Groups, User Revocation, Access Control

I. INTRODUCTION:

Cloud computing is one of the greatest platforms which provide storage of data and available 24 hours over the internet. Cloud computing is Internet-based computing, where shared resources, software and information are provided to computers and devices on demand. Cloud Computing is the hardware and software application offered as a service on a network [1]. Cloud computing gives golden opportunity for new innovation and even disruption of entire industries [2]. So Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. One of the most fundamental services offered by cloud providers is data storage. Designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task because of unconditional identity privacy may incur the abuse of privacy. Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner.

II. LITERATURE SURVEY:

In Existing System Several security schemes for data sharing on untrusted servers have been proposed. In this approach data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. But unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users respectively. By setting a group with a single attribute, proposed a secure providential scheme based on the cipher text policy attribute-based encryption technique that allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme.

Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case, where any user is granted to store and share data [3].

III. PROPOSED WORK:

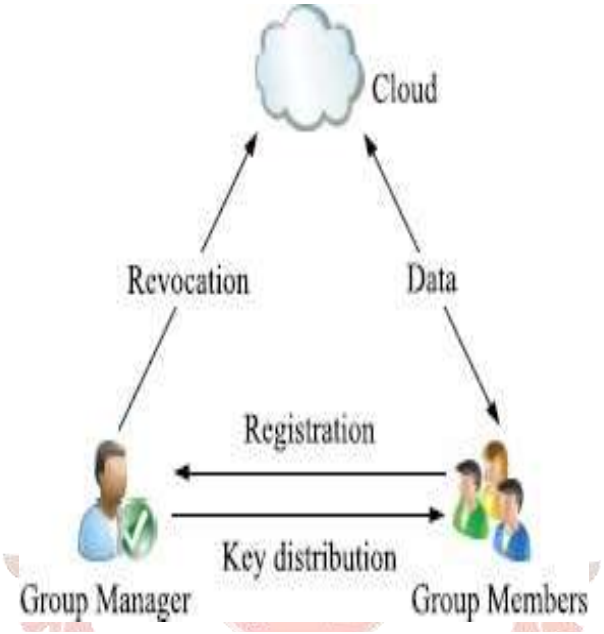
In Proposed work, here we have three parts such as group manager, group members and cloud

Firstly secure multi-owner data sharing scheme which implies that any user in the group can securely share data with others by the untrusted cloud.

This proposed work has ability to support dynamic groups efficiently. Specifically new granted users can directly decrypt data files uploaded before their participation without contacting with data owners.

We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.

IV. SYSTEM MODEL:



Cloud is operated by CSPs and provides storage services. We supposed that the cloud server is honest but *irrelevent.*

That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. The group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our proposed work the staffs play the role of group members. The group membership is dynamically changed, because of the staff resignation and new employee participation in the company.

V. DESIGN GOALS:

In proposed work access control, data confidentiality, anonymity and traceability, and efficiency as follows: Access control: The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked. Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation. Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

Efficiency: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

CONCLUSION

In this paper, we design a secure data sharing scheme, for dynamic groups in an untrusted cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally supports efficient user revocation and new user joining. Efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation.

REFERENCESES

1. Secure Multi Owner Data Sharing For Dynamic Groups In The Cloud S.Seethalakshmi1 , S.Saraswathi2,Dr.V.Raji31,2Deptofcomputerscienceandengineering,SKPEngineeringCollege, Tiruvannamalai 3Assistant Professor, Dept of computer science and engineering , SKP Engineering College, Tiruvannamalai Corresponding author: S.Seethalakshmi1
2. Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud
3. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
4. Dynamic Secure Multi Owner Data Sharing Scheme Over Cloud Computing
5. Secure data sharing for multiple dynamic groups in Cloud