An Efficient Data Sharing Approach for Dynamic Group in Cloud

J.SelvaNithya
Department of Computer Science and Engineering
Dr.Mahalingam College of Engineering and Technology
Pollachi-642001

Mrs.A.Brunda
Assistant Professor (SS)-CSE
Dr.Mahalingam College of Engineering and Technology
Pollachi-642001

Abstract-*Cloud Computing provides an economical and efficient solution for sharing resources among cloud users. Due to the frequent change of membership there is no security and any member in the group can anonymously utilize the cloud resource so the identity privacy from non trusted cloud is still a challenging issue. The user can securely obtain their private keys from the group manager without any secure communication channel. Any user in the group can use the source in the cloud and revoked users cannot access the cloud once they are revoked in the group. A secure data sharing scheme which can be protected from collusion attack and the revoked users cannot get the original data file even if they conspire with the non trusted cloud. In MONA, user is able to share data with others in the group without revealing identity privacy to the cloud. Efficient revocation can be achieved through a public revocation list and it is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group the private keys of the other users do not need to be recomputed and updated. In the scheme MONA, group manager stop working due to large number of requests coming from different groups of owners, then backup manager remains available. This method claims required efficiency, security, scalability and reliability.*

Keywords-*Access Control, Key Distribution, Data Sharing, Dynamic Groups, Privacy Preserving, Revocation and Cloud Computing.*

I. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic sharing resources and the low maintenance [1]. It is a subscription based service where one can obtain network storage space and computer resources. Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic sharing resources and low maintenance characteristics. Data Storage is one of the most fundamental services offered by cloud providers [1]. The cloud provider can use both own and house for hardware and software necessary to run a home or business applications. Cloud users face security threats both from outside and inside the cloud [2]. Most fundamental services offered by cloud providers are data storage such cloud providers cannot be trusted to protect the confidentiality. Cloud poses a significant risk to the confidentiality of the stored files since the cloud server's managed by cloud providers are untrusted.

Cloud systems can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user. It is one of the greatest platforms which provide storage of data in very low cost and available for all time over the internet. In the cloud, data is often shared by the group of users and it is generally hosted by third parties where data can be stored and shared so the security of data is major problem when people use commercial cloud services to store their data [2]. Data owner will provide the decryption keys only to the authorized users and unauthorized user have no rights to access the data once they are revoked.

Cloud systems can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user [3]. It is one of the greatest platforms which provide storage of data in very low cost and available for all time over the internet. In the cloud, data is often shared by the group of users and it is generally hosted by third parties where data can be stored and shared so the security of data is major problem when people use commercial cloud services to store their data.

Data owner will provide the decryption keys only to the authorized users and unauthorized user have no rights to access the data once they are revoked [4]. Several security schemes for data sharing on non trusted servers have been proposed. Data owners store the encrypted data files in non trusted storage and distribute the corresponding decryption keys only to authorized users and the unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys [5]. However the complexity of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. Unfortunately, the single owner manner hinders the adoption of their scheme in to the case where any user is granted to store and share data [6].

II. RELATED WORKS

In 2014, Shani Raj, Varghese paul and Nishana Rahim presented a multi owner information exchange is an model for sharing business data of large organizations which allows owners to create, manage and control their information data in cloud. In policy based data sharing, each user has an access policy for the system and each file has some file access policy. The data may have multiple owners and the owners register into system as a group of users but having individual access keys and passwords. Anyone in the group can store and share the data. The policies of shared files are set by any of the owners and need approval of all the owners. Any change in file policy should need the group permission. File revocation means making file permanently inaccessible for all owners and it is done by deleting the secured decryption key with permission of all the owners along with the file policy. Custom files are shared to a set of selected users by the owners. Public files can be accessed by all users registered in the system and the access permissions are set by owners. Two kinds of users are in the system custom users and public users. For public users a public policy is available for data file access. The keys are sent to users through email and the users who clear all authentication tests are only authorized to access the data file.

In 2010, Lan Zhou projected a a scalable and fine-grained data access control scheme by defining access polices based on data attributes and KP-ABE technique. The arrangement of attribute based encryption, proxy re-encryption and lazy re encryption allows the data owners to allocate the calculation tasks to untrusted server without enlightening the necessary contents of data. By using Key Policy Attribute-Based Encryption (KP-ABE), the random key is further encrypted with a set of attributes. Then the approved users are assigned an access formation and matching secret key by the Group admin. Hence only the users with data file attributes that gratify the access structure can decrypt a cipher text. This approach has some drawback such as multiple owner manners. In multiple owner manner it is not maintained by this system so that those single owner manners make it less flexible as only Group Admin are answerable for altering the data file shared. And user secret key needed to be updated after each revocation.

In 2016, Zhihua, Xinhui Wang, Xingming Sun, and Qian Wang proposed a sensitive data should be encrypted before out sourcing for privacy requirements, which obsoletes data utilization like keyword based document retrieval. Cloud data supports dynamic update operations like deletion and insertion of documents. Some dynamic schemes have been proposed to support inserting and deleting operations on document collection. The dynamic schemes support efficient multi-keyword ranked search. The data owner is responsible for the update operation of his documents stored in the cloud server. The data owner generates the update information locally and sends it to the server. Data users are authorized ones to access the documents of data owner. In query keywords only the authorized user can generate a trapdoor TD according to search control mechanisms to fetch encrypted documents from cloud server. Then, the data user can decrypt the documents with the shared secret key.

In 2014, Ning Cao, Cong Wang, Ming Li, Kui Ren and Wenjing Lou data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for greater flexibility and economic savings. Protecting data privacy the sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search which is widely used on the plaintext data, cannot be directly applied on the encrypted data. Downloading all the data from the cloud and decrypt locally and all these multi keyword search schemes retrieve search results based on the existence of keywords, which cannot provide acceptable result ranking functionality.

In 2013, Boyang Wang, Hui Li and Ming Li focus on a public verifier is able to audit the integrity of shared data without retrieving the entire data from the cloud, and also without learning private identity information of the group members. Group dynamics such as user join and user revocation are efficiently handled by outsourcing signature updating operation store the cloud via a secure proxy re-signature scheme. A public verifier is able to efficiently audit the integrity of shared data in the cloud for a group of users without retrieving the entire data from the cloud. The public verifier, who is only a third-party to the group, is not able to reveal confidential information of the group, such as which user in the group or which block in shared data is a higher valuable target than others. The original user is the original owner of data and creates shared data in the cloud in the first place. After shared data has been created in the cloud, not only the original user, but also group users are able to access and modify shared data. The original user also acts as the group manager, who is able to add new users to share data and revoke users from the group. The cloud offers data storage and sharing services to users. Due to the existence of hardware/software failures and internal attacks, users do not fully trust the cloud with the integrity of shared data stored in the cloud. The Third Party Auditor, who is a public verifier, is able to audit the integrity of shared data on behalf of users.

In 2013, Xuefeng Liu, Yuqing Zhang, Boyang Wang and Jingbo Yan secure multi-owner data sharing scheme implies that any user in the group can securely share data with others by the untrusted cloud and new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation

can be easily achieved through a revocation list without updating the secret keys of the remaining users.

III. EXISTING SYSTEM

In Existing System only the group manager can store and modify data in the cloud and identity privacy is not maintained for sharing a file in cloud group also file sharing is not maintained [8].

The requirement of access control is described in two ways of data operation. First the group members are able to use the cloud resources and unauthorized users can't able to use the cloud resource once they are revoked from the group and to avoid unauthorized access data should be encrypted before outsourcing [9].

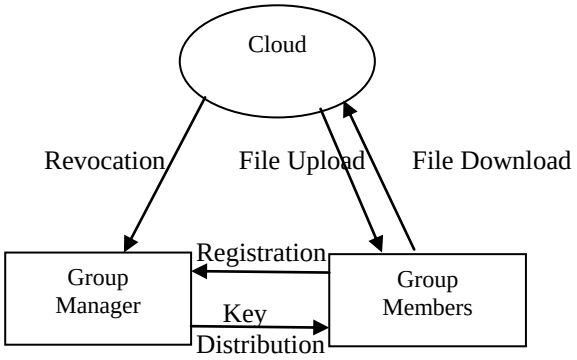

Figure 1.Architecture of Existing Systems

Only the group manager can store and modify the data access in the cloud [9]. The occurrence of traffic level is high to avoid the traffic the process done by the group manager is handled by the backup group manager.

IV.SYSTEM ARCHITECTURE

The System Architecture of Proposed system is shown in figure2. In the proposed system MONA is if the group manager stop working due to large number of requests coming from different groups of owners, then backup group manager will remains available. [10]. Here user gets extra time for accessing data after the time out by sending request to the cloud. The Process will handle the risks like failure of group manager then the backup group managers will remains available.

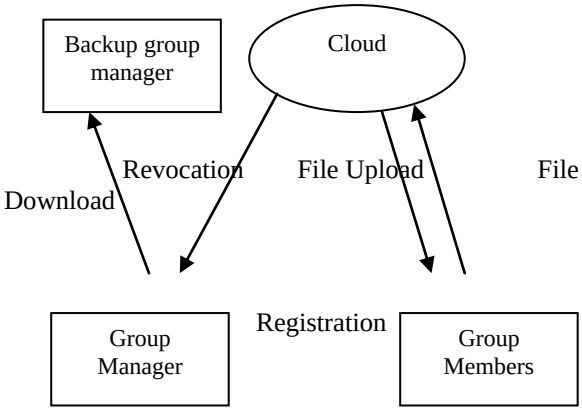

Figure 2.Architecture of Proposed Systems

The original user is the original owner of data, and creates shared data in the cloud. After shared data has been created in the cloud, not only the original user, but also the group users are able to access and modify shared data [12]. The original user also acts as the group manager, who is able to add new users to share data and revoke users from the group.

Diffie-Hellman Key Exchange Algorithm

Diffie Hellman Key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel; also it is a specific method of exchanging keys.

Step 1: Xa < q (user can select any random number less than q)

Step 2: Ya = a Xa mod q (Ya is a public key of sender)

Step 3: K = Yb Xa mod q (where Yb is a public key of receiver and K is a private key)

Step 4: Calculate of Secret Key of Users (User A key generation and User B key generation).

V. MODULES

A. User Registration

The user can login effectively only if user id and password are mention correctly. The login will fail if the incorrect user id or wrong password is entered by the user [13]. This helps in stopping unauthorized access. User registered with their details such as identity (user name, password, email-id, mobile no).For registered users they will obtain private key, the private group key is used for file decryption [13]. The Group manager adds the user identity to the group user list that will be used in traceability phase.

After successful creation of cloud setup users require to get registered with the system through user registration process. While registering, users need to present their personal details for achievement of registration process. During registration process, user got single identity and access structure [14]. This produces secret key for the members. For registered users they will get private key, that private key is used file encryption and decryption.

B. Group Manager

Group Manager is an entity who is going to store, share and manage data files stored in the cloud. Group manager takes charge of user registration, user revocation, system parameters generation and revealing the identity of a dispute information owner.

The group manager is acted by the administrator of the corporate. A Set of registered users who can store their private data in the cloud server and share them with others in the group are referred to as Group manager. Group members are a set of registered users Will store their personal information into the cloud server and share them with others within the group. The Group manager is the admin and has the logs of each and every process in the cloud [15]. The group manager is responsible for user registration and also user revocation too.

C. Group Member

Group members are one or more registered users who are all allowed to store and share their private data in the cloud [10]. Usually the group members are the team members or staffs in the organization.

Group member are a set of registered users that will store the private data into the cloud server. It is a collection of registered users who will store their confidential and personal data into the cloud server and distribute them with others in the group. Both Group Admin and group member can login using their login details [11]. After successful login, Group Admin make active newly added members of the cloud by producing keys for each member using bilinear mapping and throw it to the corresponding group members [12]. They can also check the group particulars, and assign group signature. After successful login, Group Members signature is verified. After successful confirmation, the member can upload, download and can alter the files. Group member must be encrypting data files before uploading to the cloud. The Group Members account can be revoked after he leaves the cloud by the Group Admin.

D. Cloud Server

A cloud server is a logical server that is built, hosted and delivered through a cloud computing platform over the Internet [12]. Cloud servers possess and exhibit similar capabilities and functionality to a typical server but are accessed remotely from a cloud service provider. Cloud Server will not able to modify or delete user data due to the protection of data auditing schemes.

D. Backup Group Manager

If the group manager stop working due to large number of requests coming from different group of owners, then backup group manager will remains available. Here user gets extra time for accessing data after the time out by sending request to the cloud [15].

VI. ANALYSIS

It is expected that the computational cost decreases with the number of revoked users because of the computation for the recovery of the secret parameter decreases and the number of revoked users also decreases [15]. In the proposed system, it is expected to the cost is irrelevant to the number directly uses the original dynamic broadcast encryption. It is able to support the dynamic groups efficiently and user revocation can be achieved through a public revocation list without updating the private keys of remaining users [15]. Data owners store the encrypted data file only to the authorized users.

VII.CONCLUSION AND FUTURE WORK

The group manager takes charge of the operation. Data owners distribute the secret keys only to authorized users and unauthorized user have no rights to access the data. Due to the occurrence of heavy traffic the process handle by the group manager is handled by the backup group manager. It is expected to support dynamic group efficiently and user revocation can be achieved through a public revocation list without updating the private keys of remaining users.

References

[1] Zhingma Zhu and Rui Jiang," A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud" IEEE Transactions on Parallel and Distributed Systems, Vol. 27, no. 1, January 2016.

[2] M. kavitha Margret, "Secure Policy Based Data Sharing For Dynamic Groups in the Cloud", International Journal of Advanced Research in Computer Science Engineering and Technology, Volume 2, Issue 6, June 2013.

[3] Aswathy v, J.M Gnanasekar "A Novel Methodology for Secure Multi Owner Data Sharing For Dynamic Groups in Cloud" International Journal of Engineering Research and Technology, Vol 3, Issue 5,May 2014.

[4] Sunita R. Patil and Yogesh Sayaji "A Survey Paper on RS-MONA: Reliable and Scalable Approach for Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 12, December – 2013.

[5] Divya N, Jyothi K S, "Data Sharing in Multi Owner Access Control for Dynamic Groups in the Cloud", International Journal of Engineering, Research and Technology,Vol 3, Issue 4, April 2014

[6] Mr.Parjanya C.A, Mr. Prasanna Kumar, " International Journal Of Advanced Resesarch in Computer Science and Software Engineering", Volume 4,Issue 3, March 2014.

[7] Shani Raj1, Dr. Varghese Paul2, Nishana Rahim3, "Multi-Owner Data Sharing in Cloud Storage Using Policy Based Encryption", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 5, May 2014.

[8] Nutakki Prasad,K.Kiran Kumar, "A Dynamic Secure Multi Owner Data Sharing Over Cloud Computing", International Journal of Computer Engineering in Research Trends, Volume 2,Issue 10,October 2015.

[9] Boyang Wang, Hui Li and Ming Li, "Privacy Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics", IEEE Communication and Information Systems Security 2013.

[10] XuefengLiu,Yuqing Zhang,Boyang Wang and Jingbo Yan, "Mona: Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transaction on Parallel and Distributed Systems, Vol 24, No.6, June 2013.

[11] S.L.Sowjanya, D.Ravikiran, "Secure Data Sharing For Dynamic Groups in the Public Cloud" International Journal

of Computer Engineering In Research Trends, Volume 1,Issue 6, December 2014.

[12] C.Delerablee,P. Paillier, and D. Point cheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Cipher texts or Decryption Keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.

[13] Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing", 31st International Conference on Distributed Computing Systems 2011.

[14] M.R Kalai Selvi, "Secure Data Sharing For Dynamic and Large Groups in the Cloud" International Journal of Innovative Research in Computer and Communication Engineering, Vol 2, Issue 1,March 2014.

[15] Sandeep kadam, Sunitha R.Patil, "Reliable and Scalable Approach to Store and Share Sensitive Data for Dynamic Groups in the Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5,May 2014.

[16] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans.Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.