A SURVEY ON ACCESSING CLOUD STORAGE BY GROUP MEMBERS WITH SECURE DYNAMIC USER REGISTRATION AND REVOCATION

[1]V.Dhivya, [2]M.Sivakumar, [3] H.AnandaKumar, [4]B.Anuradha
[1] PG scholar, [2,3] Assistant.Professor, [4]Associate Professor
Department Of Information Technology
SNS College of Engineering - Coimbatore

Abstract—One of the important characteristics of cloud computing is low maintenance which is economically beneficial to the user. All the user in the cloud, provides their resources to the customer (or) a third party by sharing their data in a common area. Group Formation makes it simple, for a group of members share their resources. Group Members in the cloud are identified with a group id or user id. The user has to share or retrieve their data from the cloud using their user id, where user's id is used to authenticate the user. The user id should be secured from third party in a cloud especially in a group by using Revocation list. The Revocation list has to identified an authenticated user. Our work in this paper is to secure the user id, in such a way that a third party will not be able to retrieve any data without the user id. This is applicable even for a dynamic group, by using ring signature algorithm. By using Ring signature any user can securely share the data with others in the group. this reduces the storage overhead and computation cost.

Index Terms—: **Ring Signature, Encryption, Group signature, Group Member, Security.**

I. INTRODUCTION

Cloud computing serves as a model for sharing resource, application, service and release these products with minimum management cost or effect which paves way for the following characteristics of cloud and they are on demand self service, broad network access, resource pooling, rapid elasticity and measured service. The major advantages of cloud services are it has capacity even at peak demands, reduces cost, removing unneeded capacities. Processing network and storage are the cloud system elements from technical point of view. As known to all it consists of three layers they are infrastructure as a structure, Platform as a service and software as a service. Infrastructure as a

service provides service based on unique IP address such as Amazon web services. In Platform as a Service the hardware operating system storage are rented to the user based on their requirement. Software as a service is an outgrowth from platform as a service(Paas). Here the software applications are made available to the user over the internet. It reduces the computation cost [1]. The major drawback found in cloud was security. The following are the security issues in cloud (i) privileged access (ii) Regulatory compliance (iii)Data location (iv) Data segregation (v) Recovery (vi) Long-term viability (vii) Data availability. Cloud transparency entails the cloud provider to disclose the adequate information about their security. The public cloud has high degree of transparency when compare to private cloud or hybrid cloud. The software engineers in the cloud need to decrease the privacy risk and ensure the legal compliance. As these are associated with threads like data storage, remote processing, increased virtualization. This is due to the lack in control and distrust[2].A new security challenges which are introduced in multitendency model and the pooled computing resources involves problem like hacking. The multitendency give raise to two security issues first is the shared resources in the same physical machine involve unexpected malicious resources between the regular resources. Second is the reputation fate sharing, which damages many reputed cloud storages. Another major issue that was noted down is cloud interoperability issue. So the interoperability focuses on the link between different clouds and their connection and local organization systems between them. There are few interoperability levels and the first one is to optimize the IT assets and computing resources. These IT assets are associated with their core competence while outsourcing marginal functions and activities. Second issue outsource the number of marginal functions to cloud service offered by different vendor[3]. Cloud service should be integrity and user privacy. They should enhance the interoperability. Data protection is applied to secure data, resource security and content copyrights. The content copyright is secured for the metadata and the file data's. The metadata consists of encrypted key for providing access control for the data. so, securing the metadata is more important than the data files. Attribute based encryption, Group signature, Elliptic curve cryptography are few mechanisms for protecting metadata. These metadata's are stored as block of files with the key need to deliver and renew gain for user revocation[4].

This paper is further classified into the following sections. Section(II) describes the literature review done for the algorithm selection. Section(III) describes the proposed model. Section(IV) describes the modules and Section(V) ends with the conclusion.

2. LITERATURE REVIEW

2.1 Multiowner cloud

In a multiowner cloud, there are three important roles they are group manager, group member and the cloud where the entry process is done. Group manager has the responsibility to maintain the system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. 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. For authentication purpose the Group manger receives the registration request from all the users, and generates a verification share and forwards to all the requested users[5].

2.2 Dynamic Broadcast Encryption

In dynamic broadcast encryption techniques, without any hardware support Advanced Encryption Standard can be demonstrated in order to implement the instruction set randomization .This is implemented in a virtual environment using strata. The main aim of strata is to capture the application context and the instruction sets will be translated. These translated instruction sets will be stored in the cache. Storing the data in the caches is insecure. Strata includes variety of application built for code manipulation, compression etc. The user has to use, another third party technique to secure the data from an unauthorized user Dynamic Encryption is used for secure data sharing in the cloud but the major drawback found was the revocation list missing in the multiowner cloud without this the group manager will not be able to identify the existing user in the group[6].

2.3 Member Signature

Group signature also known as Member signature, the main purpose the signature is to provide the data integrity and to authenticate the user in the cloud. The signature is based on the random value (probabilistic value) which easy for third party to access the signature without the knowledge of the authenticated user. The signature verification is done using the Boolean valued algorithm(0's or 1's). [7]. So we propose a ring signature which is more secure and advanced than the group signature that includes the revocation list for identifying the authenticated user in the cloud environment

3. PROPOSED MODEL

In the existing system, a single-owner based cloud method was used, where the single owner is only the group manager who can store and modify the data in the cloud, and rights to share the files with keys. Without the proof of identity privacy, users may be unwilling to join in a group formed in the cloud environment because their real identities could be easily disclosed to cloud providers and attackers. In the literature survey it was found that the data owners store the encrypted data files in an untrusted storage and distribute the corresponding decryption keys only to authorized users. Without the knowledge of decryption key the unauthorized user and the data server will not able to read the data. key management is complex one because the single owner should not be able to maintain the keys and files. Sharing data in a secure manner is very difficult due to the dynamic users in the cloud.

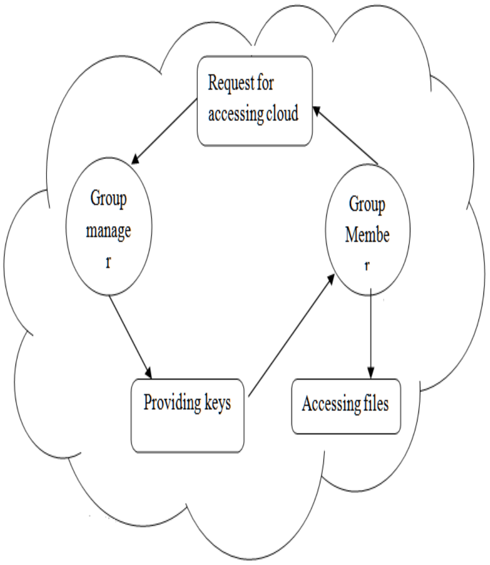


Fig 1 System Architecture

In Multi-owner concept, without the knowledge of other users there is a chance to misuse the key of an authorized user by the group manager. In the Proposed system a secure multi-owner data sharing scheme is developed in such a way the user will be able to share the data in an untrusted cloud. The main advantage of this method is that it supports dynamic group efficiency where a user can decrypt the file and upload without containing the data owner identity. User revocation list is another major advantage that can be achieved without updating the private keys of the remaining users. Ring signature is provided for data security and avoids misuse of key. The below diagram illustrates the following scenario in such a way that the user have to register in the cloud. Now the signature will be generated for the registered user, with the help of the signature the user will be provided a private keys for accessing the files stored in the cloud to the formed groups.

4. DISCUSSION

In group formation, the group is formed by the owner. The data owner have a rights to upload the data into the cloud, the data owner creates the group and give unique id for that group. Each group has one group manager, and there are several members under the group manager. And the manager allocates accessing for the cloud to the formed groups[8]. Group members are a set of registered users, where the user will be able to store their private data into the cloud server and share them with others in the group. Group manager takes in charge of user registration, user revocation and parameter generation. The group manager is fully trusted by the other parties[9].

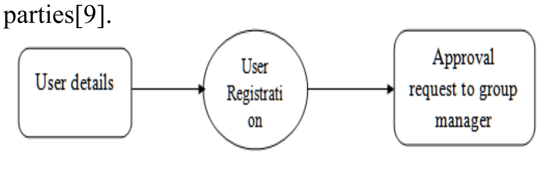


Fig 2 User Registration

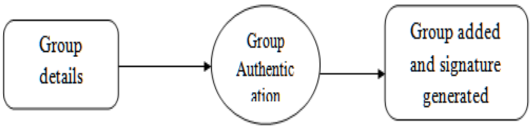
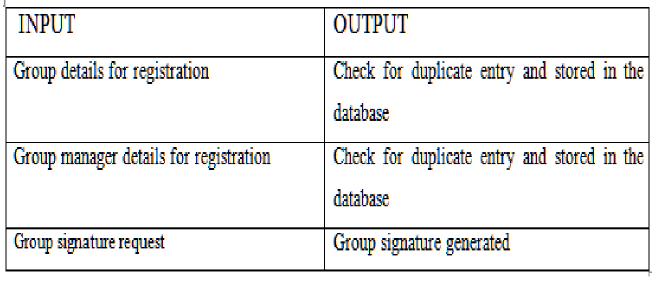


Fig3 Authentication details

Table 1 Group registration and authentication details



INPUT	OUTPUT
Group details for registration	Check for duplicate entry and stored in the database
Group manager details for registration	Check for duplicate entry and stored in the database
Group signature request	Group signature generated

The Group member generation and key allocation is mainly for generation of users. If any new member wants to enter the group, the particular member wants to register into the system. The group manager take over the registration, the group manager allocates individual user id and allow them to access their data files[2]. After the registration, User obtains a private key, which will be used for signature generation and decryption of files. To achieve secure data sharing for dynamic groups in the cloud, ring signature technique is used[10]. One of the security properties of a ring signature is that it should be difficult to determine which of the group member's keys are used to produce the signature. Ring signatures are similar to group signatures but differ in two key ways:

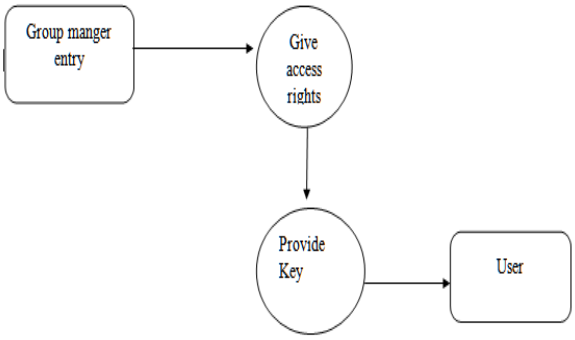
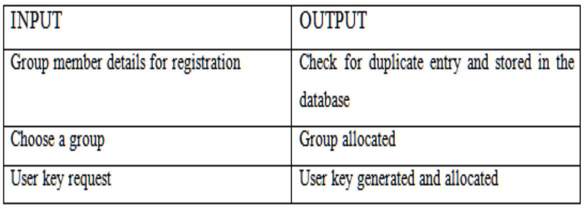


Fig 4 Key Generation

(i) There is no way to revoke the anonymity of an individual signature. (ii) Any group of users can be used as a group without additional setup.

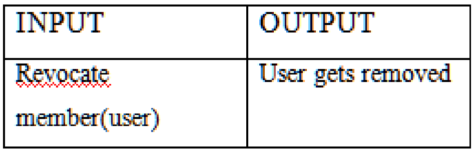
Table 2 Key Allocation table



INPUT	OUTPUT
Group member details for registration	Check for duplicate entry and stored in the database
Choose a group	Group allocated
User key request	User key generated and allocated

In User Revocation, the user is removed from the particular group without disturbing the other users in the group. User Revocation is performed by the group manager with the help of revocation list(RL)[11]. The main purpose of revocation list is to check the user is an authenticated user or not. If the user is not an authenticated user, he is not able to access the data in the cloud.

Table 3 - User Revocation



INPUT	OUTPUT
Revocate member(user)	User gets removed

Accessing control consists of file deletion and file updation. For Updation and deletion of data's in the cloud, first the user sends the id to the revocation list. The revocation list checks whether the id is valid or not. If it is valid encryption should be done and then the group member can securely share their data's in the cloud. If it is not valid the particular user may be removed from the group. In case if the user wants to delete a file the user id should match with the id that is stored by the group manager[12].

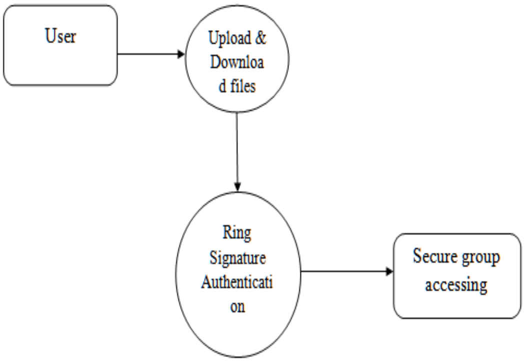
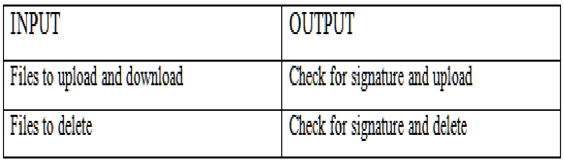


Fig 5 File updation and Deletion

Table 4 Updation and Deletion



INPUT	OUTPUT
Files to upload and download	Check for signature and upload
Files to delete	Check for signature and delete

5. CONCLUSION

Now a day all social networks include the multiowner group formation, where the user will be able to share the data in a secured way. But the user authentication is a difficult process, to overcome this step we use ring signature which is more secure than the group signature. And additionally we use revocation list for validation the user. Thus we conclude that the valid user will be able to access the data in the cloud.

REFERENCES

[1] George Pallis gpallis@cs.ucy.ac.cy "Cloud Computing The New Frontier of Internet Computing" Published by the IEEE Computer Society 1089-7801/10/$26.00 © 2010 IEEE

[2] Ramgovind S, Eloff MM, SmithE"The Management of Security in Cloud Computing" 978-1-4244-5495-2/10/$26.00 ©2010 IEEE

[3] Tharam Dillon Chen Wu and Elizabeth Chang "Cloud Computing: Issues and Challenges" 2010 24th IEEE International Conference on Advanced Information Networking and Applications

[4] Cong Wang, Qian Wang, and Kui Ren Wenjing Lou "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing" IEEE INFOCOM 2010

[5] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud" IEEE transactions on parallel and distributed systems, VOL. 24, NO. 6, JUNE 2013

[6] Wei Hu, Jason Hiser, Dan Williams, AdrianFilipi, JackW. Davidson, David Evans,John C. Knight, Anh Nguyen-Tuong, Jonathan Rowanhill " Secure and practical defense against code injection attacks using software dynamic translation" VEE '06 June 14–16, 2006

[7] V.Padmavathi, M.Madhavi, N. Nagalakshmi "An Approach to Secure Authentication Protocol with Group Signature based Quantum Cryptography" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-2, January 2013

[8] Giuseppe Ateniese, KevinFu, Matthew Green, Susan Hohenberger, " Improved Proxy Re-Encryption schemes with application to secure distributed storage" ACM transactions in Information and Security Systems, vol-9,No.1,feb 2006

[9] Rongxing LuXiaodong LinXiaohui Liang, and Xuemin (Sherman) Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing" IEEE 13-16 2010

[10] Eu-Jin GohHovav Shacham Nagendra Modadugu Dan Boneh "SiRiUS: Securing Remote Untrusted Storage" 2007

[11] DalitNaor, MoniNaor, Jeff Lotspiech"Revocation and tracing schemes for stateless receivers" IEEE 2009

[12] Zhiqian Xu, Hai Jiang "HASS: Highly Available Scalable and secure Distributed Data Storage.