Data Sharing Securely for Administrators of Dynamic Groups in Cloud

Nirali H. Patel[1]
Student of BE Information Technology
BVCOE & RI, Nasik, India
University of Pune
patel.nirali2192@gmail.com

Sajiya S. Patel[2]
Student of BE Information Technology
BVCOE & RI, Nasik, India
University of Pune
sajiyapatel26@gmail.com

Pooja C. Ighe[3]
Student of BE Information Technology, BVCOE & RI, Nasik, India
University of Pune
poojaighe2486@gmail.com

Prof. Madhuri B. Patil[4]
BE Computer Engineering
BVCOE & RI, Nasik, India
University of Pune
Madhur299@gmail.com

***Abstract* -** In recent year's cloud computing is popularly increased day by day in the form of securing, updating, storing, sharing confidential data. Today's condition about data security in cloud computing is very bad thing happens when people work on cloud for confidential company data. System provides scheme for secured data sharing when we use dynamic groups in an un-trusted clouds. In a system, users can share data in other groups without revealing identity privacy to the cloud. Efficient user revocation and new user joining is also supported by the system. Public revocation list is used for efficient user revocation without updating the private keys of the other users. New users before participation can decrypt directly. User within a group is identified by a group signature. Also public revocation list is used. System is a secure data sharing scheme in a multiple group policy.

Keywords- *Cloud Computing, Access controls, Dynamic groups.*

*****

I. INTRODUCTION

In recent years cloud computing become very popular among the users companies and organization. Alternative to traditional information technology is known as cloud computing. It provides intrinsic resource sharing and low maintainance characteristics. CSP's like Cloud service providers delivers various services to their users by providing powerful data center. For example Amazon. High quality services are given to users by migrating local data management systems into cloud servers. Investments on local infrastructure are saved significantly due to this. Data storage is the most crucial service that the cloud provides. If we consider a practical data application where staff of a company is allowed to work in a same group or department so as they can store and share files in the cloud. Staff can completely release from the troublesome local data storage and maintainance by using cloud efficiently. Stored files could lead significant risks sometimes. As data in the cloud is sensitive and confidential such as business plans, organization cannot rely on cloud providers as it is not fully trusted. To design an efficient and secured data sharing scheme we have to face following challenges.

First, One of the obstacle for deployment in cloud computing is identity privacy. Users cannot join in cloud computing system without their accurate identity privacy as real identities could be disclosed to cloud providers and attacker on contradiction. Abuse of privacy could occur due to unconditional identity. For example, untrustworthy staff can forward false files without himself being traceable. It is therefore necessary group manager should provide with

facility of traceability. Second, data storing and sharing services which are provided by cloud should be fully enjoyed by the group members who are part of respective cloud group. This is given by multiple owner manner. In contrast with single owner manner where data in the cloud can be stored and modified so multi-owner manner is always useful and flexible in practical application. Members in the group can modify their part of a data in entire data file which they are sharing with their company.

Third, groups in the cloud are almost always dynamic in nature. For example when new staff participates and current employee revocates in a company. Secured data sharing is extremely difficult when changes to the membership has to be made. New granted user can be allowed to learn the contents it is not possible for granted user to contact with owner of anonymous data. We can revocate membership without updating keys that we have kept secret for remaining users which we have desired to minimize key management for controlling complexity.

Figure 1 shows the basic architecture of cloud computing.It first involve the clouds and then working is done. The data is shared on the cloud. Firstly deploy to a cloud and then manage and interface it. Then migrate to a cloud and interface the clouds.

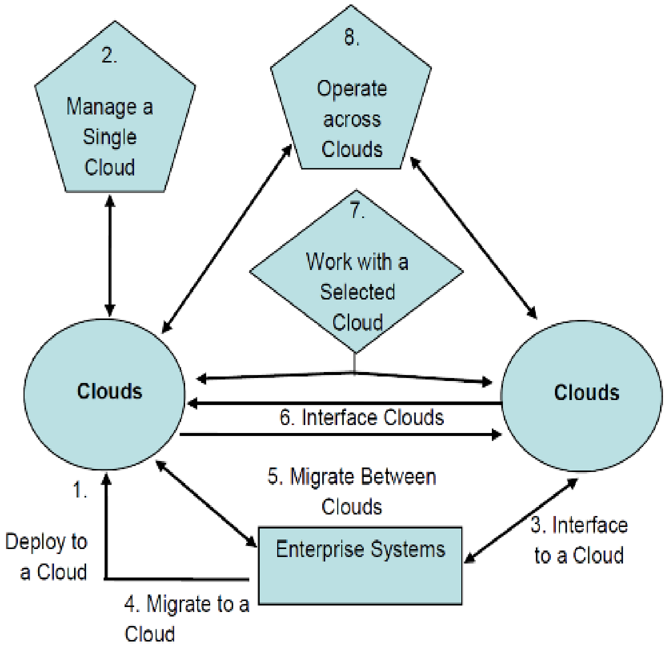

Figure 1: Flow of cloud computing

II. LITERATURE SURVEY

Secured multi-owner data sharing is hot new technology that can be applied in many areas of cloud computing. We found some methods for applying it. Cloud computing refers to both the applications delivered as a service over the internet and hardware and system softwares in data centers that provides those services. The services themselves have long being referred to as software as a service [1]. Security that records owner of data and history of processes data objects is a vital to the success of data in cloud computing [7]. In public cloud infrastructure problem of secured cloud storage is on high risk. Cost of building and maintaining a private storage infrastructure can be reduced by moving data to the cloud. Microsoft's Azure storage service and Amazons S3 are based on storage service of public cloud [2] [8]. Effective solution to make companies trust cloud providers is to encrypt data while working on a cloud on contradiction there are some issues with method like key management issue and solution performance issue, we can solve this by introducing a system which includes key policy attribute based encryption(KP-ABE). There are some other encryption methods are also very useful while achieving secure scalable and fine grained data access, for eg. Proxy encryption(PRE) or lazy re-encryption [3][6][9]. Secure file sharing is possible without placing trust on file servers, this can be achieved by a cryptographic storage system such as p-l-u-t-u-s. Each users can retain direct control over the people who get access to their files which is most crucial feature of p-l-u-t-u-s. It also supports scalable key management. All data is stored encrypted and all keys that has to distributed is efficiently handled in p-l-u-t-u-s as it uses decentralized manner [4]. Revocation scheme is especially used for stateless receiver subset cover algorithms defines a framework. There are two construction schemes are used. This methods are better than earlier known algorithms. By bifurcation property is most useful in this framework which will allow us efficient tracing methods. This will also support functionality of modifying the previously known revocation scheme [10]. The goals of s-i-r-i-u-s are no change to remote file server that implies crypto techniques, Easy for end users to deploy in which minimal client software and no kernel changes are done, it also minimizes trust in file server [5].

III. SYSTEM OVERVIEW

System overview shows how the system works to avoid unwanted situation while working on a cloud. Cloud servers stores all the important data which are uploaded by companies organization and users. Whenever group working on a cloud wants to access their data, they access it through their ids which is provided by group managers to access data.

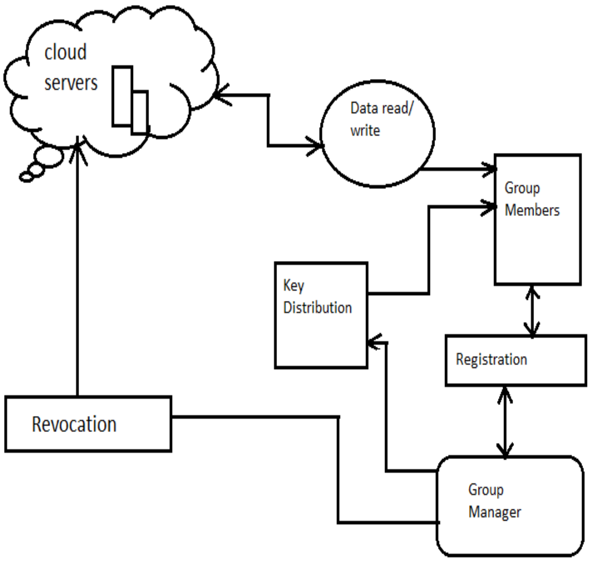

Figure 2: System Overview Diagram

Figure 2 how cloud interaction works when organizations work on a cloud.

Whenever group members want to work on a cloud they have to register their id's to their respective group managers. Registration process is very crucial when secure cloud computing is considered. Group members provide their all personal and official information to group manager. According to provided information group manager authenticate their identity by providing them unique id code. This code will remain consistent throughout the project even if new members to the projects are added in between.

In key distribution process, group manager provides unique ID to newly entered group members, group members then take their unique id's from this process. Whenever a group members want to perform read/write operation with cloud then they use their id's to fetch data. Revocation process is carried out by group manager whenever he provides id to group members. In this process group manager refreshes the key list given to cloud servers to allow group members to access company data.

In this way, system overflow takes place through the various processes as shown in system overview diagram. Group manager plays vital role in this all communication process as all security phases goes through managers unique key distribution to all employees.

IV. Algorithmic Strategy

These are the 3 algorithms used in proposed system:

1. Signature Generation Algorithm
2. Signature Verification Algorithm
3. Revocation Verification Algorithm

1. Signature Generation Algorithm:

```
Step 1: Let Private key =(A,x), System parameter=(P,U,V,H,W) and data=M.
Step 2: Generate a valid group signature on M.
Step 3: Select random numbers $\alpha$, $\beta$, $r_{\alpha,}$ $r_{\beta,}$ $r_{x,}$ $r_{\delta 1,}$ $r_{\delta 2} \in Z^*_q$
Step 4: Set $\delta 1 = x\alpha$ and $= x\beta$
Step 5:Compute the values
        $T_1=\alpha.U$
        $T_{2=}\beta.V$
            $T_{3=}A_i+(\alpha+\beta).H$
        $R_{1=}r_{\alpha.}U$
        $R_2=r_\beta.V$
        $R3=e(T_3.P)^{r_x}e(H,W)^{-r_\alpha -r_\beta}e(H,P)e^{-r_{\delta 1} -r_{\delta 2}}$
        $R_4=r_x.T_1-r_{\delta 1}.U$
        $R_5=r_{x.}T_2-r_{\delta 2}.V$
Step 6: Set $C=f(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)$
Step 7: Construct following numbers
        $s_\alpha=r_\alpha+c\alpha$
        $s_\beta=r_\beta+c\beta$
        $s_x=r_x+cx$
        $s_{\delta 1}=r_{\delta 1}+c_{\delta 1}$
        $s_{\delta 2}=r_{\delta 2}+c_{\delta 2}$
Step 8: Return $\sigma=(T_1,T_2,T_3,c, s_{\alpha,}\ s_{\beta,}\ s_{x,}\ s_{\delta 1,}\ s_{\delta 2})$
Step 9: End
```

2. Signature Verification Algorithm

```
Step 1:Let, input system parameter(P,U,V,H,W) and a
        Signature $ɕ=(T_{1,}T_{2,}T_{3,}c,s_{\alpha,}s_{\beta,}s_{I,}s_{\delta 1,}s_{\delta 2})$
Step 2: Now,compute the value
        $\tilde{R}_1=s_\alpha .U- c .T_1$
        $\tilde{R}_2=s_\beta. U - c.T_2$
        $\tilde{R}_3= (e(T_3,W) \diagup e(P,P))^c e(T_3,P)^{8I} e(H,W)^{-8\alpha-8\beta}$
                $e(H,P)^{-8b1-8b2}$
        $\tilde{R}_4=s_I.T_1-s_{\delta 1.}U$
        $\tilde{R}_5=s_I.T_2-s_{\delta 2.}V$
Step3: if $c=(M,T_{1,}T_{2,}T_{3,}R_{1,}R_{2,}R_{3,}R_{4,}R_5)$
Step 4: It returns true
Step 5:Otherwise returns false.
```

3. Revocation Verification Algorithm

```
Step 1: Let System Parameter=$(H_0,H_1,H_2)$, a group signature $\sigma$, and a set of revocation keys $A_{1......}A_r$
Step 2: Check valid or invalid
Step 3: set temp $e(T_1, H_1)e(T_2,H_2)$
        for i= 1 to n
        if$e(T_3-A_i,H_0)$=temp
Step 4: Return valid and end if and end for.
Step 5: Otherwise return invalid.
```

V. Implementation Details

Implementation details contain basic modules included in system. Implementation is the realization of an application or execution of a plan, idea, model, design. Multi-owner data sharing approach includes 2 modules.

A. System based application

System based application is simple application in which system security modules are included.

1. Signature generation module

This module provides ability to group authority to generate unique id's to group members to access confidential cloud storage data in secure manner.

2. Signature detection module

In this section system provides a control to detect whether authorized person is accessing cloud storage data. In this it checks whether id provided by group member is valid to access company's confidential data.

B. Cloud based application

This module is based on cloud technology hence the manager of the group can check group members authority anytime when he wants to check security level of cloud based company's data. It provides reliability to company's authority that their data is in a safe manner.

Figure 3. Shows how to decide a message good or bad for filtration. If the known/unknown person is already in blacklist then gives the notification to that person or block that person due to this setting messages of that person is not

posted on user's wall. Messages are check according to filtering strategies whether message is good or bad then and then it will be posted on user's wall of OSN.

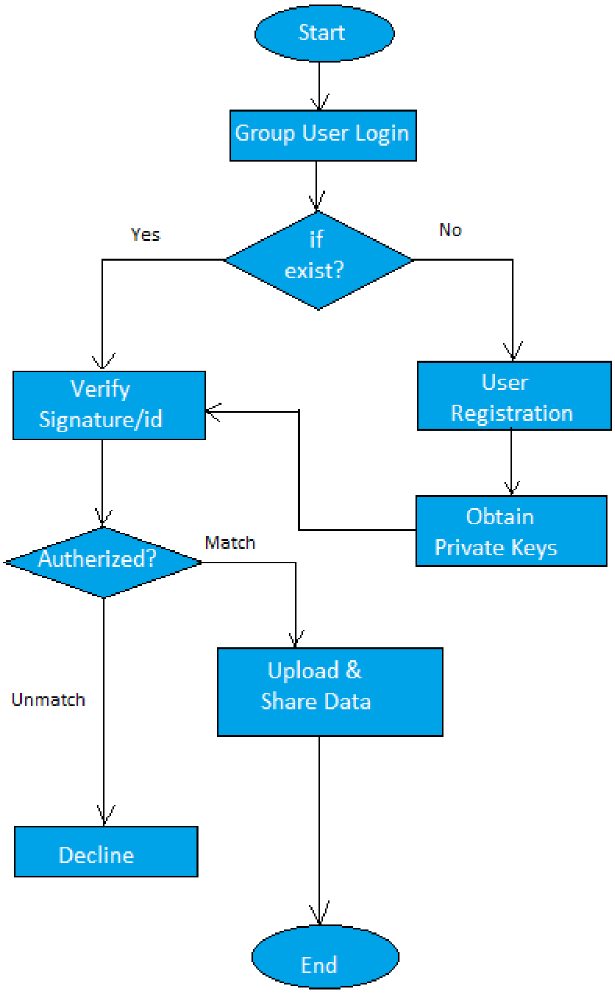

Figure 3. Filtering Approaches

VI. CONCLUSION

Hence M-O-N-A is security system provided to multi-owner data members for exchanging their data while working on a cloud, so even if cloud is not safe users can securely communicate and exchange their data. Only the head of group is able to keep and change the data in the cloud. The group can securely share data with others by unsecured cloud. In our system manager of group is the only person who can change the data. The difficulty of encryption and text length of cipher text is not depending on revoked users that we have called. Keys that are private to other users are needed not to be update while calling them.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.

[2] Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing,"Comm. ACM,vol. 53,no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage,"Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[4] 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.

[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage,"Proc. USENIX Conf. File and Storage Technologies,pp. 29-42, 2003.

[6] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage,"Proc. Network and Distributed Systems Security Symp. (NDSS),pp. 131-145, 2003.

[7] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,"Proc. Network and Distributed Systems Security Symp. (NDSS),pp. 29-43, 2005

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud

[9] Computing,"Proc. ACM Symp. Information, Computer and Comm. Security,pp. 282-292, 2010

[10] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,"Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography,http://eprint.iacr.org/2008/290.pdf, 2008

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[12] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers,"Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-62, 2001.

Nirali H. Patel she is Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest is in the field of testing and cloud computing.

Sajiya S. Patel she is student of Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of Pune. Her interest in the field of security and cloud computing.

Pooja C. Ighe she is student of Engineering student of Information Technology at Brahma Valley College of Engineering And Research Institute, Nasik under University of pune. Her interest in the field of coding and cloud computing.

M. B. Patil, BE Computer Engg. Was educated at Pune University. Presently she is a master student in the department of Computer Science and Engineering, RTU Kota University. Her interests include Data Mining.