ISSN 2395-1621

# A Secure Group Sharing Framework in Cloud Computing with OTP

[#1]Sandhya D. Chavare, [#2]Prof. D.S.Uplaonkar

[1]sandhya.chavare@gmail.com
[2]uplaonkar@gmail.com

[#12]Department of Computer Engineering

JSPM's RajarshiShahu School ofEngineering & Research,Narhe,
Pune, Maharashtra, India.

**ABSTRACT**

**In public cloud computing, services have appeared for data sharing in group application. The privacy and security are the main issues that arise when sharing group data in public cloud. The semi-trust nature of the third party, therefore the cloud provider cannot be treated as a trusted third party .Therefore security models used traditionally cannot be directly assign to the framework of cloud based group sharing. We propose a novel secure group sharing framework for public cloud. This framework is created by combining Proxy signature, enhanced TGDH and proxy re-encryption together into compact. By adopting proxy signature scheme, the group leader can grant right of group management to chosen a number of group member. By using the enhanced TGDH scheme that enables the group to update and negotiate group key pairs thus all group members need not to be online together. By using proxy re-encryption most of intensive operations which are to be performed computationally can be handed over to the cloud servers without leaking of any private information. Our proposed scheme shows security and performance analysis and also provide the functionality like suppose data owner is unavailable then user send request to data owner mobile and get information through message from admin.**

**Keywords: Secure group sharing, forward secrecy, backward secrecy, public cloud computing, group key agreement, TGDH( Tree-based Group Diffie-Hellman).**

ARTICLE INFO

**Article History**

Received: 27th June 2016

Received in revised form :

28th June 2016

Accepted: 30th June 2016

**Published online :**

**1st July 2016**

## I. INTRODUCTION

With the large organization of networking sites and different cloud services, due to the same concern a community can be easily organized between some populations over Internet, so that group applications with the aid of cloud servers attract greater attentions. Due to its innate sharing of resources and low-maintenance property the Cloud computing is show as an alternative to old information technology. Database and high performance computation are the main needs which have to be fulfilled. Many cloud computing service providers have to provide data storage in cloud. When group data is stored in the cloud , the data owner can share their data with the desired members in the group. The cloud is managed by cloud service provider. Due to semi-trust nature Cloud service provider cannot be behaving as trusted. Finally, traditional security storage model cannot be directly assigned in the public cloud storage application. The cloud providers are managed cloud server. To maintain data privacy, a basic track is to encrypt data files, and then the encrypted data can be uploaded onto the cloud. So valid users can download and decrypt the file. But the session key updating and distribution is a major problem. Another method is the use of Digital Envelope. In these methods, the computing and communication overhead of digital envelopes generation and the computational and communication overhead of session key changing are major problems. Suppose some of the group member leaving then the server launch collision attack, if the cloud server should be trusted then schemes efficiency depend on fact. The group application form can be created in cloud as follows. The group leader in the cloud to form a group application.

## II. RELATED WORK

Our work considers a case study of different security based survey papers as follows below.

**a) Digital Envelope**

K. Ren, C. Wang, and Q. Wangpresents [2], By using given key, authorized member can download the encrypted data

and decrypt them. But in this overview some problem occurs, how to divide and change or update session keys. Digital Envelope is used for this task in : Symmetric encryption is used for data encryption with randomly selecting session key and public-key encryption (public key of specific user) is used for session key encryption.

**b) cryptographic tools**

P. Tysowski and M. Hasan[5] ,authors works based on cryptographic tools like ABE, proxy re-encryption address the privacy preserving data sharing problem for secure mobile application in clouds.

**c) Interest based group sharing**

Yu et al.'s[3] schemes efficiency depends on the users high attribute changeability between them and high attribute variability between different files. But similar interest different group members are in the group application, they have a common attributes among them. In the scenario of interest based group sharing, suppose Yu et al.'s scheme used, the communication and computing overhead of user revocation will be dependent on the size of the group.

**d) proxy-re-encryption keys**

The efficiency of the scheme in[4] that data is maintained by cloud server assumed that it is trusted third party. Here provide the security when user enter and leaving group, therefore data owner need to recalculate his key pair and re-generate N-1 proxy re-encryption key when revoking a group member. Therefore computing overhead increases at high range for data owner because of user joining and leaving frequently in the group.

**e) backward secrecy and forward secrecy**

The paper[6] scheme should explain the claim of privacy of backward secrecy and forward secrecy. The backward secrecy mentions that the leaving member cannot decrypt new cipher texts. The forward secrecy mentions that the newly entering member can also access and decrypt the previously published data. This two security requirements are usually used in this scenarios [6].

## III.SYSTEM ARCHITECTURE

In this approach, we present a secure group sharing Architecture which gives us the basic idea of a system.

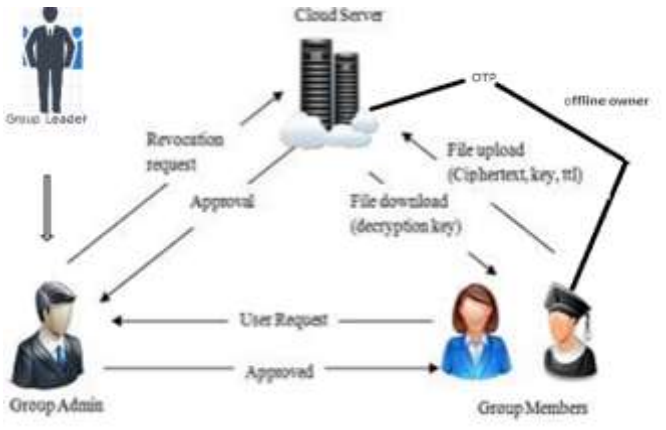



Fig 1: System Architecture

a)Group Leader:

The group leader creates a group using group application in a cloud sharing area. The group leader grants the members permission to implement data management. All the data open to all group members in the group, while they remain private towards the outsiders of the group including the cloud provider. The group leader can give permission to some group member as to management of group, and privilege can also be revoked by the group leader. When a member leaves the group, then he/she cannot download and read any shared data again.

b)Group Admin:

The group leader selects some specific members to management help of group, and this right can also evolve by the group leader. And the Admin can accept the new user request.

- View Members:

Group admin has authority of view group members. He can see how many members are included in group or his/her records.

- Assign Admin

Admin has authority to assign other members as admin. In group one or more admin includes and also change password.

- File Upload and Download

Group admin can upload file on cloud and can also download from cloud. He is a one of the group member of group.

c) Group Member or User:

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. Each group member can have a permission to implement file download and upload operations in the authenticated group. Cloud servers provide some related public information to each group member and the member compute specific set of security parameter, such as group key pair.

- File Upload

To store and share a data file in the cloud, a group member checks the revocation list and verify the group signature. First, checking whether the marked date is fresh. Second, verifying the contained signature. Uploading the data into the cloud server and adding the ID data into the local shared data list maintained by the manager. On receiving the data, the cloud first to check its validity. It returns true, the group signature is valid; otherwise, the cloud stops the data. In addition,if several users have been revoked by the group manager, the cloud also performs.

- File Download

Signature and Key Verification In general, a group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature originator when a dispute occurs, which is denoted as traceability.

d) OTP(One Time Password):

OTPs avoid a number of shortcomings that are associated with traditional passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct

a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. OTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server. In our system OTP is send by system to offline data owner on his mobile no. OTP contain data owner key, mobile number of requested person. OTP send on mobile number of owner.

## IV. ALGORITHM

Step 1: Randomly select a security key.

Step 2: Get the blinded keys of all sibling nodes of every node in the path from his/her associated node to the root node from cloud servers.

Step 3: Compute new security keys and blinded keys of each node in the path from his/her associated node to the root node.

Step 4: Set the versions of his/her associated node and its parent node to child node.

Add 1 to the version of each of the other internal nodes in this path.

Step 5: Send all the blinded keys from his/her associated node to the root node in this path to the GL in an authentication tunnel.

**Mathematical Model:**

Let us consider a set S

where, S= {U, R, SER, D, GM,GL,GA ,FS,BS }

Here, S: System which includes: U: Set of Users Where U= {U1, U2, U3 …, Un, $U_{on}$, $U_{off}$} ,$U_{off}$={$U_{off1}$, $U_{off2}$ ,…….. $U_{offn}$}, $U_{on}$={$U_{on1}$, $U_{on2}$ ,…….. $U_{onn}$}

SER: Server. R: Set of Request.

Where R= {R1, R2, R3……., Rn}

D: Database. N: Number of Cluster. (i.e. 2)

GM: Group Members

GL: Group Leader

GA: Group Administrator

U ε S

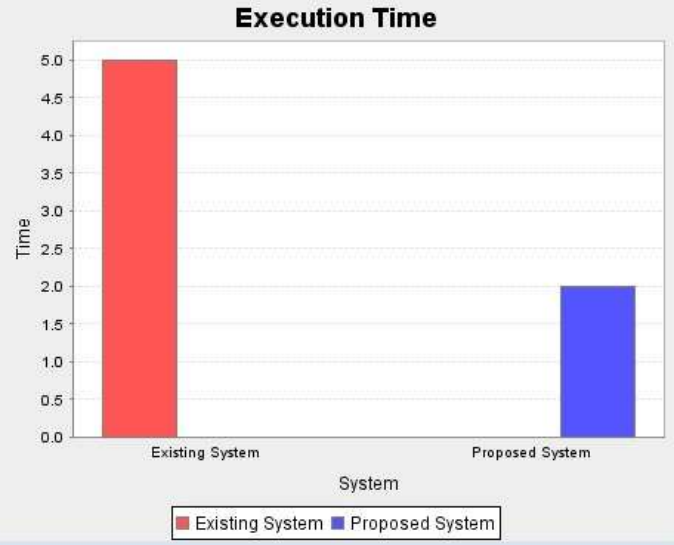
(R)(S(GM)→S(U))
(R)($GM(U_{onn})$↔ GA)
GA→ $GM(U_{off})$ or ⁻GA v $GM(U_{off})$
GA = Group Members+ Group Leaders / Group Leaders

FS:- Forward Secrecy.

BS:- Backward Secrecy.

## V. RESULT

In today's world most of organizations are using cloud for storing data, so there are a large number of users using cloud. There may be a chance of data being viewed by another user so we are giving security to that data by encrypting file which is uploaded. Our System provides sharing functionality to admin by creating group which gives privileges to users for downloading file. Performance graph of prosoed system show below. The execution time of existing system is higher than proposed system.




## VI. CONCLUSION

In this project, a secure data sharing scheme is designed. The management of secure group sharing can be given to various group members. All the data or files to share are securely stored and protected in the cloud servers. TGDH scheme is used for the group members for leaving or joining the group. As all the group members are online at different time still the system works well. It also supports efficient user revocation and new user joining. A new type authentication system, which is highly secure and updating transaction offline. The system provides a secure channel of communication between communicating entities. To achieve the design of the goal the system the security and performance analysis of the system do well, it becomes less complex and communication becomes easy.

## REFRENCES

[1]. Kaiping Xue, Member, IEEE and Peilin Hong, Member, IEEE" A Dynamic Secure Group Sharing Framework in Public Cloud Computing" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 4, OCTOBER-DECEMBER 2014.

[2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,and fine-grained data access control in cloud computing," in Proc.IEEE 29th Conf. Comput. Commun., 2010, pp. 534–542.

[4] W. Jia, H. Zhu, Z. Cao, L. Wei, and X. Lin, "SDSM: A secure data service mechanism in mobile cloud computing," in Proc. IEEE Conf. Comput. Commun. Workshops, 2011, pp. 1060–1065.

[5] P. Tysowski and M. Hasan, "Hybrid attribute-and re-encryptionbased key management for secure and scalable mobile applications in clouds," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172– 186, Jul.–Dec. 2013.

[6] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," ACM Trans. Inf. Syst. Security, vol. 7, no. 1, pp. 60–96, 2004.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in Proc. 10th Int. Conf. Trust, Security Privacy Comput. Commun., 2011, pp. 91–98.

[8]. K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proc.IEEE Conf. Comput. Commun., 2013, pp. 2895–2903.

[9]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[10]. Z. Wan, J. Liu, and R. Deng, "HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.