# Secure Sharing of Data for Dynamic Group in Cloud Storage Application

S.Sathya, Dr. B.Vanathi, K.Shanmugam

**Abstract-**Data sharing is increasingly important for many users and sometimes an essential requirement, especially for industries and society's used to gain proceeds. Sharing group resource among cloud users is a major problem, still the data privacy leak. The existing system Group Key Management method used for sharing Key Generation and distribution in the group member or users. Sometimes change to user one group to another group, the group key to enable authenticated users to access the files securely and efficiently is still a challenging problem. This problem to avoid that sharing data in group using the Time Based Group Key Management (TGKM) techniques for cryptographic cloud storage application , which Conditional Identity Based Broadcast Proxy Re-Encryption (CIBPRE) used to transforming the data's(files) major process in cloud server. To Key Generation method for user a time based dynamic group Key which capably to make stronger in cloud security. Generally, security and performance evaluated that the proposed scheme is highly efficient and satisfies the security requirements for cloud based application.

**Keywords**: Data sharing, Group Key Management, Dynamic Group, security.

## 1. INTRODUCTION

Nowadays, cloud computing is technology to allow the user accessing the data in the internet connection. It can be easily and quickly to sharing the data through the internet which has been pay per use on demand service. Cloud computing mostly used for business and organization, provide the large amount space for the data storing at low cost. Cloud provider have fulfill the mainly need that data storage and high performance computation. Cloud provide by many Cloud computing service provider amazon, Drop box, Google App engine etc... Cloud provider to allow one of the most essential services data storage. Data storing and sharing create the security issues are information leakage and data privacy. Confidential and High sensitive data stored in cloud. So, security and privacy have always been very essential concerns in cloud Computing. Data Encryption is one of the solutions for maintaining data and uploads the encrypted data into the cloud server. By using Data Encryption Techniques are ABE, PRE, KP-ABE, CP-ABE [18][4]etc…

Sahai and Waters [2] was introduced attribute based encryption and provide the data security. In this method used the public Key based one to many encryption that user can be encrypt and decrypt for depend on the user attribute. There are two types of ABE method: Key Policy Attribute Based Encryption (KP-ABE) and cipher text policy Attribute based Encryption (CP-ABE**)**.KP-ABE method a set attribute used the encrypted data and user private key depend upon the access polices created. Cipher text policy Attribute based Encryption (CP-ABE) method allows the data admin to encrypt the data on an access policy, that will be based on the attributes of the user or data. So, the decryption is possible when the secrete key is matching with the access control policy.

Proxy re-encryption[15] is a basic cryptographic method, its converts cipher texts from one encryption key to another encryption key. The re-encryption protocols have to key independent to avoid cooperating the private keys of the sender and the receiver. Proxy re-encryption has many applications in addition to the earlier schemes for forward to email, secure network file storage, and perform the cryptographic operations on storage limited devices.

Group key management is the important method for provide the security in group communication. In this, the security is succeeded by sharing a common key among the group members. The message blocks , those are going to pass on should be encrypted with the shared key. Group key management is generally focusing on the key generation and distribution of key mid the group members. All the group members should contribute in secure distribution, creation and deletion of the keys. To communicate the session group key management is achieved by two entities: Group Controller (GC)[16], important role

for key generation, distribution and resend to key when the change group member and Key Server (KS), important role for maintain the keys and distributing the keys.

In Fig [ 1] the data sharing process mechanisms in the following secure method; the data owner stores data in the cloud storage in an encrypted method. When the data owner encrypts files using asymmetric algorithm a key pair of public and private keys are generated and securely get that key in owner. The Private Key is sent to the users who get the ability to access the files. Large files are encrypted using Public key that results in generation of a cipher-text. Data owner need to send the respected share key to the user.
The user would respected share key and private key can decrypt the file .Figure 1 shows that encryption process between two cloud users and key sharing between them. Proposed cryptosystem would provide a multi encryption in file which is difficult to break and so provide security to sensitive data stored in cloud storage application.

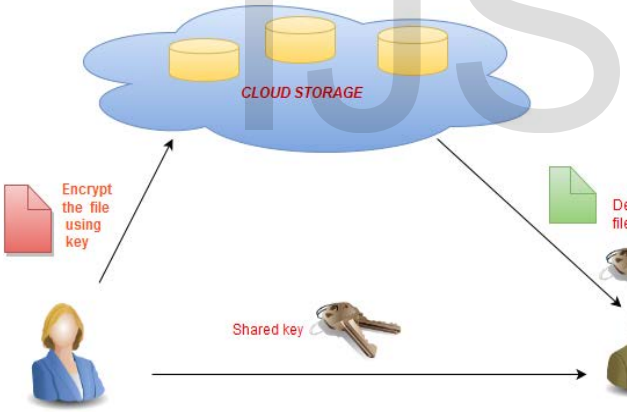


***Fig 1: secure data sharing***

## 2. Related Work:

In[5] To proposed a protection for users to stores and the share their complex data in the cryptographic cloud storage. It offers to basic encryption and decryption for providing the security on cloud application. HoIver, the revocation operation is a definite performance killer in the cryptographic access control system. To improve the revocation procedure, they existent a new efficient user revocation scheme which is efficient, secure, and independently. In this scheme, the unique data are first divided into a number of parts, and then published to the cloud storage. When a revocation happens, the data owner needs only to retrieve one part, and re-encrypt and re-publish it. Thus, the user revocation process is enhanced by affecting only one part instead of the whole data. It must useful the efficient user revocation method the cipher text-policy attribute-based encryption (CP-ABE) based cryptographic cloud storage application. The security analysis shows that the method is computationally secure.

Yu et al. [1] a scalable and fine-grained data access control method access polices based on data attributes element using and KP-ABE technique. To achieve the combination of attribute-based encryption (ABE), proxy re-encryption and lazy re encryption allow the data owner to allocate the computation tasks to untrusted server without revealing the essential contents of data. Data owner encrypt the data files using random key. Using key policy attribute based encryption (KP-ABE) method, random the key is encrypted with a set of attributes. Then the users are given an access structure and corresponding secret key by the group admin. Therefore, only the user with data file attributes that fulfill the access structure can decrypt a cipher text. This system has some control such as multiple-owner manner is not maintained by this system so that those single owner manners make it few flexible access as only group admin are responsible for modifying the data file shared. The user secret key needed to be updated once each revocation.

B. Waters et al. [4] proposed the appeal of low maintenance, cloud computing provides an economical and well-organized solution for sharing group resource between cloud users. Inappropriately, sharing data in a multi- group owner manner while preserving data and characteristics privacy from an untrusted cloud server is still a challenging issue, due to the frequent change of the followers. In this paper, they propose a secure multi- owner data sharing method called Mona, for dynamic groups in the cloud. To improve the group signature and dynamic broadcast encryption (DBE) techniques,

any cloud user can unidentified person share data with others. For this moment, the storage overhead and encryption computation cost of our scheme are self-governing with the number of revoked users. In addition, the security and analysis method with rigorous proofs, and determine the efficiency of scheme in experiments.

E. Goh et al.[2] a SiRiUS, a secure file system considered to be encrusted ended with insecure network and P2P file systems . SiRiUS adopts the network storing is untrusted and offers its own read-write cryptographic access control for file level sharing. Key management and user revocation is simple with minimal out-of-band communication. File system are maintained by SiRiUS using hash tree constructions. SiRiUS contains a new method of performing file random access in a crypto graphical method file without the use of a block server. Extension lead to SiRiUS includes large scale group sharing using the NNL key revocation structure. To implementation of SiRiUS makes the relative to the basic file system despite using cryptographic operations. SiRiUS contains a new method of performance file random access in a cryptographic method by file without the use of a block server. Using crypto graphical operations implementation of Sirius also possible. Private Key share the each group member must be updated but joining of new group user in the group.

Ateniese et al. [3] proposed method of proxy re-encryptions to use the access control to the secure file system and distributed storage. The data owner encrypted the block of content with symmetric key and unique, that is encrypted all block of content under a master public key. Moreover, to contribution of a user's public key, the suitable block content keys from the master public key is straight re-encrypt using proxy cryptography that helps in keeping the access control and improvement of security. To manage access to encrypted content stored on spread untrusted replicas, this method create used in centralized access control server. The main profits of this method are unidirectional and only a limited volume of trust is set in the proxy. While, a collusion attack can happen between any revoked malicious user and untrusted cloud server permit them to find out the decryption keys of all the encrypted blocks of content.

*Table 1.Different techniques in Cloud computing*

| Title | Techniques | Parameter Achieved |
|---|---|---|
| Achieving secure, scalable and fine-grained data accesscontrol in cloud computing | Attribute based Encryption, Proxy Re Encryption, Lazy Re Encryption | Access Control; Update the secret key in revocation. |
| SiRiUS: Securing Remote Untrusted Storage. | Sirius | P2P File sharing, Access control |
| Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. | Proxy Re Encryption | Unidirectional, Access control, security improvement. |
| Ciphertext-Policy Attribute-Based Encryption | Group signature and Dynamic Broadcast Encryption | Data Sharing, Increasing security, Performance improvement |
| Cryptographic Cloud Storage | CP-ABE | Efficient Revocation, Access Control |

In Fig [2], Cryptographic cloud storage application using the data owner encrypts files before outsourcing to protect the privacy. PRE technique uses the translate major task for cloud application. For the authorized users have the key, they could decrypt the files then downloading. Perceptibly, unauthorized users can't crack user's privacy without authentication. The cloud storage application, data admin need not only store files on the cloud but also shares the files to some group users. Group key management is mainly focusing

on the key generation and distribution of key among the group members.


*Fig 2 Data sharing in groups*

All the group members should participate in secure distribution, creation and revocation of the keys. The existing system method, group key enable authenticated user to access the data. In literature survey we have many methods for secure data sharing in cloud, but most method failed to reach the able as well as secure method for secure data sharing for groups.Limitation of data sharing

- If the Group member and Group admin leaving in the group risk for updating key pairs.
- Leaving that group, revoked user can access the data without security and update key pairs.
- PRE method generates the Private Key randomly.

## 3. PROPOSED SYSTEM:

In Fig [3] Main contribution of this paper is sharing of data in dynamic groups through the cloud computing. To solve these issues, we propose a new framework TKGM for secure data sharing in cloud computing by combining group Key and Conditional identity based broadcast proxy Re encryption (CIBPRE) techniques. In this method we are presenting how to manage risk in securely sharing data among multiple group members.

Compared to existing work our proposed system provide some exclusive features such as

- This system support dynamic group efficiently. It implies that new group user joining and user revocation are easily completed without involving remaining users.
- Provide strong security which is necessary to store and maintain confidential data.
- To implement an able and scalable group key management service for the cloud storage applications.

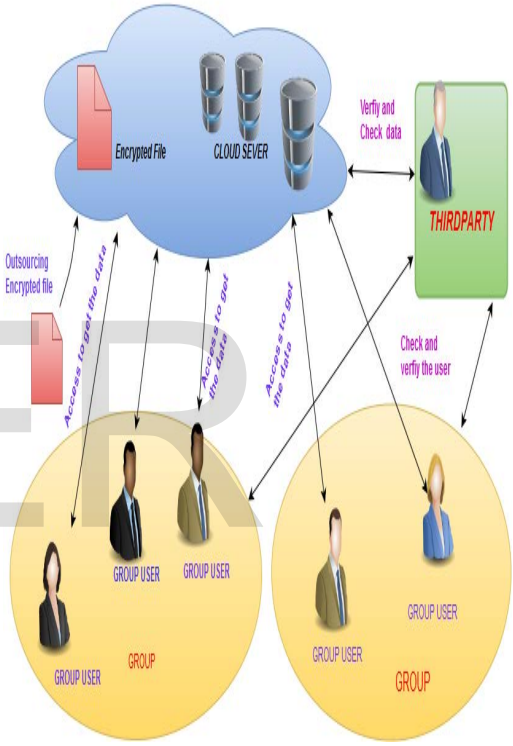


*Fig 3 System Overview Architecture*

**TGKM system model has three parties as follows:**

- **Data Owner or Group Admin**
- **Group Member**
- **Cloud sever**

### 3.1 Group Admin

The Group Admin (GA) is performed by the administrator of the organization. So we accept that the Group Admin is fully trusted by the other parties Group Admin perform different operations such as system parameters generation, user registration, assign group signature, sharing the public key assign the group for each group member using bilinear mapping and assign to the

requested user and maintain revoked user. Group Admin scheme is as shown in Fig [4].

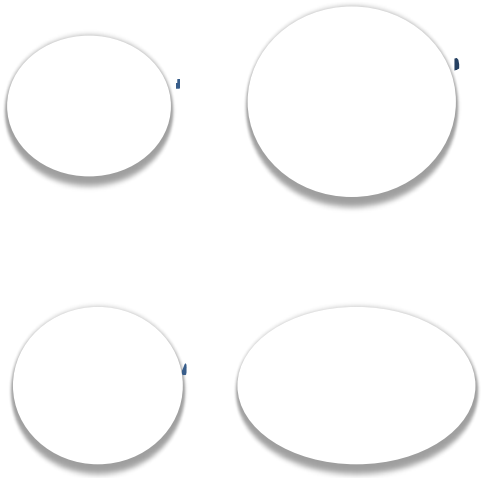

*Fig 4 Group Admin*

3.2 **Key Distribution:**

Distributing secret keys by the Group Admin that is valid only if the group members are not revoked from the group. Key can be updated by generating new key from an old key.

3.3 **Group Members**:

Group Members (GM) are a pool of registered users that will be store their private data into the cloud server and share them using others in the group. Both Group Admin and group member can login using their login details. When a successful login, Group Admin make active newly added members of the cloud by generating keys for each member and sends it to the consistent group members. It can also check the group details and group key. After successful login, Group Members signature is verified. After successful verification, the group member can upload, download and can modify the files. Group Admin must be encrypting data files before uploading to the cloud. Group member encrypt with group key and Group Admin response and shared the public key. After that GM will be decrypt with Public and private key. Group Member scheme is as shown in Fig [5].

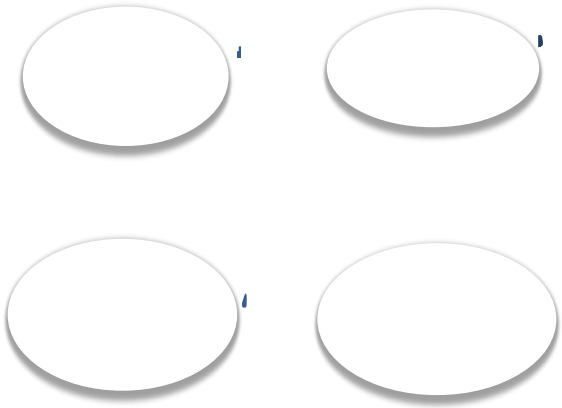

*Fig 5 Group Member*

**3.4 Cloud Server:**

Cloud is the large storage of resources. The cloud suggestions data storage and sharing services to Users. Cloud is important for storing all user's data and permit access to the file within a group to another group members. The cloud server will not delete or modify user data, due to the protection of data auditing method.

**3.5 File Upload:**

File upload is the process of storing identified data files into the cloud for sharing in the group. Uploaded files remain in the cloud up to the time stated but uploading the file. Before uploading the file, file has to be encrypted and compressed to ensure security and privacy of the files. Then it is compressed file with corresponding decryption key and sends it to cloud. File Upload scheme is as shown in Fig [6].

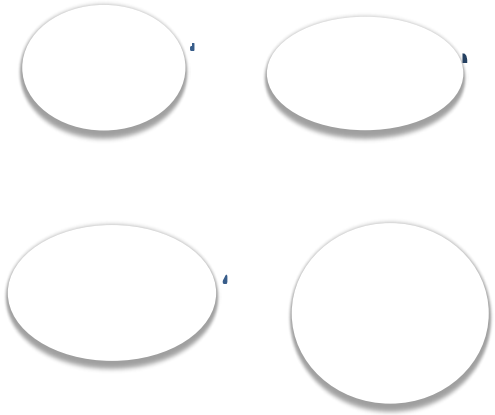

*Fig 6 File upload*

## 4. CONCLUSION

In this paper, a secure data sharing for dynamic groups in a cloud environment. In TKGM scheme, when the group users are enable to the dynamic groups, which will be key management transfer the generated key in the cloud. Generally, user can be data sharing the other group without updating the private keys, decrypting file and stored the more computation cost. More ever, the storage overhead and the computation and communication cost reduced. Our scheme efficient and effective data sharing in cloud application.

## 5. Reference

[1] Yu, S., Wang, C., Ren, K., Lou, W.: Achieving secure, scalable and fine-grained data accesscontrol in cloud computing. In: Proceedings of IEEE INFOCOM 2010, pp. 15–19 (2010).

[2] Goh, E.-J., Shacham, H., Modadugu, N., Boneh, D.: SiRiUS: Securing Remote Untrusted Storage. In: NDSS 2003 (2003).

[3] Ateniese, G., Fu, K., Green, M., Hohenberger, S.: Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. In: NDSS 2005 (2005)

[4] Bethencourt, J., Sahai, A., Waters, B.: CiphertextPolicy Attribute-Based Encryption. In: 28th IEEE Symposium on Security and Privacy 2007, pp. 321–334 (2007)

[5] Kamara, S., Lauter, K.: Cryptographic Cloud Storage. In: Sion, R., Curtmola, R., Dietrich, S., 2010 Workshops. LNCS, vol. 6054, pp. 136–149. Springer, Heidelberg (2010).

[6] Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. IEEE Trans. Parallel Distrib. Syst. 25(1), 222–233 (2014).

[7] Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFO-COM 2010, 2010, pp. 525–533.

[9] B. Wang, B. Li, and H. Li, "Panda: Public Auditing For Shared Data with Efficient User Revocation in The Cloud" IEEE Trans. Services Computing, Dec.2013.

[10] Kim, Y., Perrig, A., Tsudik, G.: Tree based group key agreement. ACM Trans. Inf. Syst.Secur. 7(1), 60–96 (2004).

[11] Wang, Q., Wang, C., Ren, K., Lou, W., Li, J.:Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. IEEE Trans. Parallel Distrib. Syst. 22(5),847–859 (2011).

[12] Hong, C., lv, Z., Zhang, M., Feng, D.: A Secure and Efficient Role-Based Access Policy towards Cryptographic Cloud Storage. In: Wang, H., Li, S., Oyama, S., Hu, X., Qian, T.(eds.) WAIM 2011. LNCS, vol. 6897, pp. 264–276. Springer, Heidelberg (2011).

[13] Jian Weng, Robert H. Deng, Xuhua Ding, Cheng-Kang Chu, and Junzuo Lai," Conditional proxy reencryption secure against chosen ciphertext attack", In ASIACCS,2009,pp. 322–332.

[14] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma,"Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", IEEE Transactions on Computers 2015.

[15] Kaiping Xue, Peilin Hong," A Dynamic Secure Group Sharing Framework In Public Cloud Computing" Ieee Transactions On Cloud Computing, Vol. 2, No. 4, October-December 2014 459.

[16] Kim, Y., Perrig, A., Tsudik, G.: Tree-based group key agreement. ACM Trans. Inf. Syst. Secur. 7(1), 60–96 (2004).

[17] Yanjiang Yang, Haiyan Zhu, Haibing Lu, Jian Weng, "Cloud based data sharing with fine-grained proxy re-encryption" Pervasive and Mobile computing 2015.

[18] V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute based encryption for fine grained access control of encrypted data," in Proceedings of the13th ACM conference on Computer and communications security , pp. 89{98, 2006} .