Re-Encryption Scheme of Secure Data Sharing for Dynamic Groups in the Cloud

Ajit N. Pawar
Department of Computer Engineering
RMDSSOE, Pune, India

Sonal Fatangare
Department of Computer Engineering
RMDSSOE, Pune, India

ABSTRACT
Continuous changes in the membership of data sharing giving security and privacy preservation are still challenging issues, especially for an untruth cloud due to the collusion attack. It is based on the secure key distribution without assuming any secure communication channel. We propose a secure re encryption scheme of data sharing scheme without assuming secure communication channel for dynamic groups in the cloud .The system provides fine grained access control for any clients who wants to access the information from cloud .It also prevents access of clients after their revocation and protect from collusion attack. Proposed system provide guarantee for secure sharing of data files when they are outsourced with double encryption and particular security key distribution mechanism. Re-encryption of message provides the data security and prevents other security attacks like man in middle attack. If an attacker tries to decrypt the massage using untruth cloud ,it will not possible for them. Users can achieve an effective and economical way for data sharing among group members in the cloud with efficient manner and little management cost.

Keywords
Key Distribution, Re-Encryption, Access Control, Collusion Attack, Fine-Grain Access, User Revocation, Group Membership.

1. INTRODUCTION
Cloud computing provides on demand service and processing resources to the Users. It is dynamic computing style where dynamically scalable and usually virtualization resources are provided as a service over the internet. Fundamental service offered by cloud providers is data storage. Servers of clouds are managed by cloud providers which are not fully secured. Users may store data files on cloud which may be sensitive and confidential, like business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [1]. The most significant difficulties is identity privacy for the wide deployment of cloud computing.

Several security mechanisms for data sharing on untrusted servers have been proposed. In those approaches, data owners store the encrypted data files in entrusted storage and distribute the corresponding decryption. Users may not be willing to join in cloud computing systems without the guarantee of identity privacy, because their real identities could be easily disclosed to cloud providers and attackers. Identity privacy may incur the sabotage of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable [2]. Therefore, traceability, which enables the group manager to track over the real identity of a user, is also highly desirable. Highly recommended for any member in a group should be able to fully access stored data and sharing services provided by the cloud, which could be defined as the multiple-owner manner More broadly, each user in the group is able to not only read data, but also modify their part of data in the entire data file [3]. Finally, groups are normally dynamic in practice. Change in membership makes secure data sharing extremely difficult. On the other side, the various system challenges granted from new users to learn the content of data files stored before their participation, because it is impossible for new approved users to contact with anonymous data owners, and obtain the corresponding decryption keys[4]. An appropriate membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management [5].Here proposed system represents the secure key distribution to the user and access control mechanism on cloud storage without assuming any secure communication channel with certificate authority with proper user revocation. Proposed system prevents cloud storage form collision attack.

2. RELATED WORK
First complete group key management scheme which can supports all functions yet preserves efficiency. That proposed scheme was based on the new concept of access control polynomial (ACP) that efficiently and effectively support full dynamics, flexible access control with fine-tuned granularity, and concealment .New scheme is protected from various attacks from both external and internal malicious parties[2]. RBE scheme allows RBAC policies to be applying for the encrypted data stored in public clouds. RBE-based hybrid cloud storage architecture provides facility of an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud[3].One approach to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as attribute-based encryption, and proxy re-encryption is called broadcast group key management (BGKM), and then give a secure construction of a BGKM scheme called ACVBGKM. Major advantage of the BGKM scheme is that adding users/revoking users can be performed efficiently by updating only some public information. BGKM used for an efficient approach for fine-grained encryption-based access control for documents stored in an untrusted cloud file storage [4].MONA proposed a new secure multi-owner data sharing scheme, for multiple groups in the cloud. They applied the group signature and dynamic broadcast encryption techniques, any cloud user can secretly share data with others. The storage overhead and encryption computation cost of that scheme were independent with the number of revoked users. Also they analyzed the security of scheme with difficult proofs, and demonstrate the efficiency of scheme in experiments [5] .Data distribution in cloud infrastructure provides an effective approach called Secure-Split-Merge (SSM) was introduced for the security of data. That proposed SSM scheme was it uses unique mechanism for performing splitting of data using AES 128 bit encryption key. The chunks of encrypted splits were being maintained on various group servers of different types of cloud zones [7].

Efficient and secure re-encryption scheme was proposed for data sharing in unreliable cloud environment. This scheme is built on top of Cipher text-Policy Attribute-Based Encryption (CPABE), fine-grained access control to share data.

3. PROPOSED SCHEME

This new system propose a secure data sharing scheme, which can achieve through secure key distribution and data sharing for dynamic group along with secure way non secure communication channels. New re-encryption scheme is used for assigning the permissions data encryption. The users can securely obtain their private keys from group manager with Certificate Authorities for the verification of the public key of the user. The system can achieve fine-grained access control. Hybrid cloud is used for efficient use of cloud. Our system for Secure data sharing can be protected from collusion attack. The revoked users could not get the original data access once when they are revoked even if they tried with the untruth cloud. Proposed scheme achieve secure user revocation with the help of polynomial function .System 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 need to be recomputed and updated. System will provide security analysis to prove the security of our scheme. Data protection is also provided using double encryption mechanism. In proposed system when file is upload to the cloud first that file will be encrypt using AES algorithm, then using horizontal fragmentation that file will fragment in several fragments .After fragmentation again encryption algorithm called RSA will be applied on the that fragmented files and that fragmented files will be stored in multiple available groups. When user want to download their file first fragment of that file will be fetched from various groups and decryption apply on it.

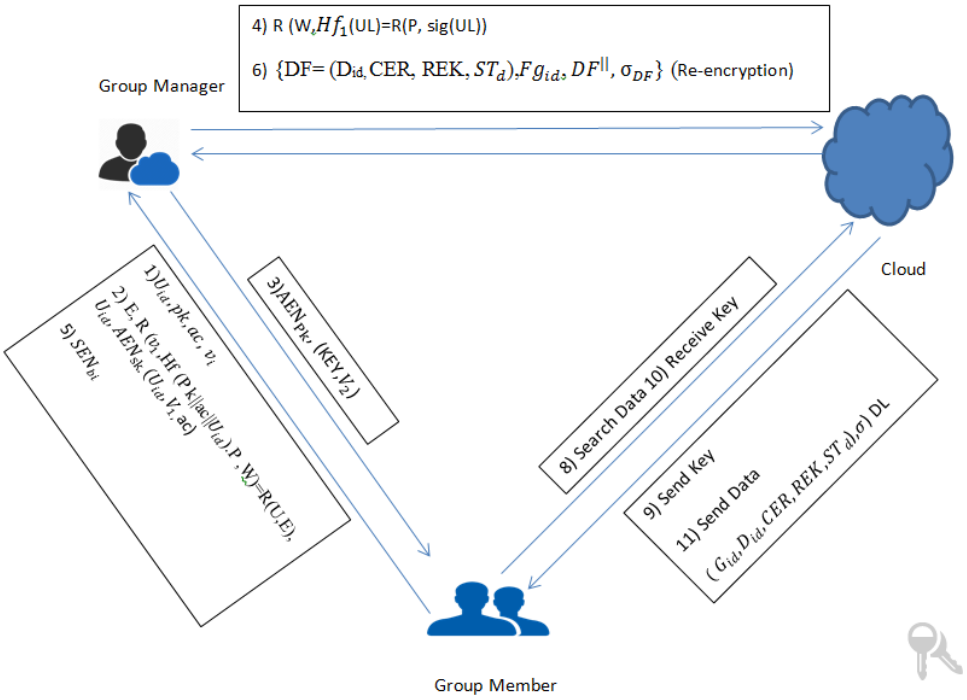

Fig 1. System Communication

Proposed system has three main modules Group manager, group member and cloud. Group manage is responsible for secure key distribution and other important tasks. Group member are the group user. Cloud is where user can store data on it. All these function together and provide data confidentiality, data integrity, access control to system.

3.1 System Module Description

Table 1: Notations

Notation	Description
U_{id}	Identity of user i
D_{id}	Identity of data
SEN_k	Symmetric encryption algorithm used for encryption k
AEN_k	Asymmetric encryption algorithm used for encryption k
DL	Data list
GL	Group user list
ST_d	Time stamp for data
Fr_{id}	Fragment id
ac	Is account of user

3.1.1 System Initialization:

Bilinear map Z=(q,G1,G2,R(_,_)),then sect two random elements let say P,G€G1 a number γ €S_q^* and computes W=γ.P , Y=γ.G , S=R(G,P) and at last , group manager distributes parameters (Z,P,W,Y,Hf,Hf_1, SEN_K()), Hf is hash function: {0,1}* → S_q^* and Hf_1 : {0,1}* → G1. Group manager kept the parameter (γ,G) as master key.

3.1.2 Registration for Existing user:

At the beginning user sends U_{id} ,Pk, V_1 as request parameter to the manager. Pk is the public key used in RSA algorithm which is asymmetric in nature, ac is account for user related to user identity and v_1€S_q^* is the random number which is

selected by the user. After receiving the request from user group manger choose random number r €S_q^* and then computes E=R$(P,P)^r$ .Group manager then verify U,E by checking equation E,R(v_1,Hf(Pk‖ac‖ U_{id}).P,W)=R(U,E),then user sends the message with AEN_{sK} the group manager by successful verification. AEN_{sK} is private key in RSA algorithm. Then group manger compares U_{id} message with identity U_{id} decrypting using AEN_{sK}(U_{id} , v_1,ac).group manager also generates the KEY (x_i, a_i, b_i).Then group manager sends encrypted message AEN_{PK}(KEY, v_2) to user and placed $(x_i, a_i, b_i,$ U_{id}) in local space. Keys are added by group manger to group user list GL along with the time stamp and its signature ST_{gl} and sig(GL). cloud verifies the signature and time stamp. At finally by decrypting massege using private key in RSA algorithm and user can obtain its private key (x_i, a_i, b_i).After this procedure user become a group member.

3.1.3 File upload:

Group member choose a unique data file D_{id} and random number k € S_q^* and the computes the parameter as follows,

F_1=*k.Y€G1*,F_2=*k.P€G1*,K=S^k*€G2*,F=AEN_K *(M)*

Then group member decrypts then ($D_{id,}$ F_1, F_2, ST_d) using it's private key b_i, ST_d is real time stamp and then group member sends the SEN_{b_i} ($D_{id,}$ F_1, F_2, ST_d) to group manager. After receiving this message group manger decrypts and gets the ($D_{id,}$ F_1, F_2, ST_d) and check the all legal group member list and its private key b_i. And also perform encryption of actual data file and the fragments that encrypted file and again perform re-encryption on that fragmented data file. Then group manger select random re-encryption key K_r and construct the equation REK ={$K_r.W_0$…….W_m} and finally re-encrypt the cipher text CER ={F_1, F_2,F } with re-encryption key and sends {DF=($D_{id,}$ CER, REK , ST_d),Fg_{id}, $DF^{||}$, σDF} where Fg_{id} is fragment id of data file, σDF is group manager signature to data file. And at last cloud verifies and identifies the group manager and store successful message or data file on it.

3.1.4 File Download:

In this phase group member encrypts D_{id} Its key a_i and sends request to cloud .After getting request cloud decrypt it and compare $a_i$with group user list GL. if it found in GL then cloud sends data file to user {DF=G_{id} , D_{id} ,RCE ,REK, σDF} along with data list. After getting message from cloud user verifies the validity of data file and then group member start the decrypt the data file. Here two decryptions are required one for keys and other for data file. For re-encrypted key decryption group member computes V_i=Hf(b_i) and then group manager decrypts RCE and gets {F_1, F_2, F}.and for decryption of first encryption group member computes the equation $\widehat{K}$=R(F_1,a)R(F_2,b) and get original file. In this way user gets original data file M by encrypting $\widehat{K}$ from encrypted data F.

3.1.5 User Revocation:

Removing user U with its U_{id} group manager blocks revoked users access and update the keys of remaining group members. User revocation is performed by the group manager and the cloud, When a user i with identity U_{id} is revoked, the group manager performs the following operations:

1) Removing user i from the group user list in the local storage space and updating the group user list which is stored in the cloud.
2) Checking the new group user list, suppose that there are m legal group members in the list. According to the list.
3) Selecting a new random re-encryption key K_r^i and constructing REK= { $K_r^i.W_0, \ldots\ldots W_{m-1}$}
4) Computing cipher-text CE = { F_1, F_2, F} with the new re-encryption key K_r^i
5) Signing his signature σ (DF) to the modified message (G_{id} ,$D_{id,}$ RCE, EK, $ST_{d,}$) where σ is the time stamp.
6) Sending the message {DF=G_{id} , D_{id} ,RCE ,REK,ST_d^l σDF}to the cloud. After that modification message cloud verify it and perform replacement operation and update all time stamp to the data file in the group.

4. RESULTS

We compare some of security parameters ODBE, Mona and our scheme. It is obviously observed that the computation cost for members in our scheme is irrelevant to the number of revoked users.

Table 2. Security Performance Comparison

	Secure Key distribution	Access control	Secure user revocation	Anti-collusion attack	Data confidentiality
Mona[11]		√			
RBAC[11]		√			
ODBE[11]		√	√	√	
Re-encryption (proposed system)	√	√	√	√	√

We list the comparison on computation cost of members for file upload and File downloading and user revoke. It is obviously observed that the computation cost for members in our scheme is irrelevant to the number of revoked users. Group manager so that the legal clients can encrypt the data files alone without involving information of other clients, including both legal and revoked clients.

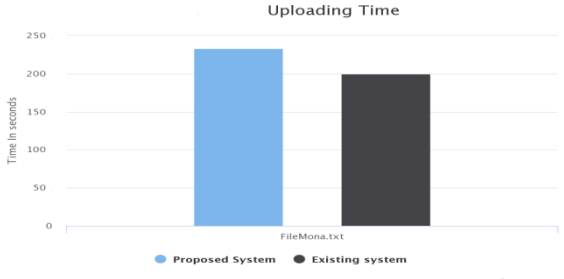

Fig 2.Uploading file

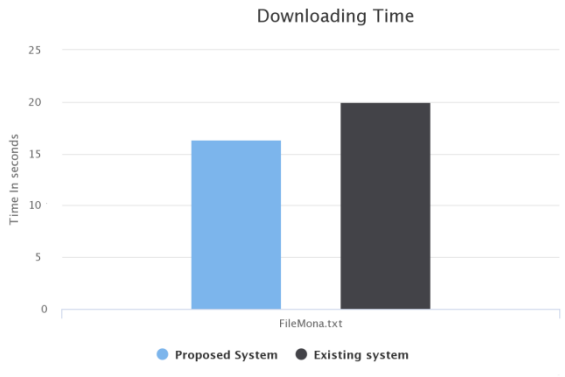

Fig 3. Downloading

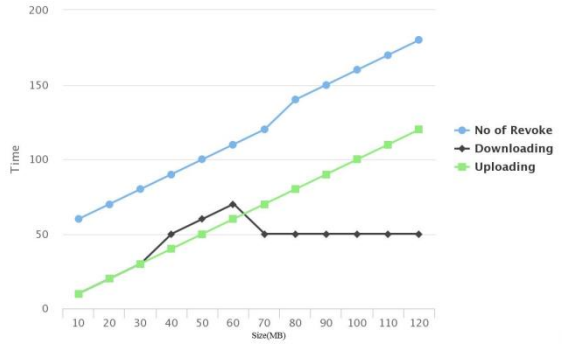

Fig 4. Comparison of various schemes

5. CONCLUSION

This system is design for secure data sharing scheme, for dynamic groups in an untruth cloud. A new type authentication system, which is highly secure, has been proposed in this system. User is able to share data with others in the group without disclose identity privacy to the cloud. It also supports efficient user revocation and new user joining. User revocation can be done through a public revocation list with updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Proposed system has efficient use of dynamic groups in cloud. System also provides the new double encryption technique for data security.

6. ACKNOWLEDGMENT

I take this chance to express my appreciation to my guide Mrs.Sonal fatangare and head of department, Prof. V. M. Lomte, Department of Computer Engineering, RMDSSOE, for their kind cooperation and guidance during the entire research work.I would also like to thank our, Principal and Management for providing lab and other facilities.

7. REFERENCES

[1] D. Dolev and A. C. Yao, "On the security of public key protocols,"IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198208, Mar. 1983.

[2] X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing,"in Proc. IEEE Conf. Comput. Commun., 2008, pp. 12111219.

[3] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 19471960, Dec. 2013.

[4] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 26022614, Nov. 2013.

[5] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 11821191, Jun. 2013.

[6] Z. Zhu, Z. Jiang, and R. Jiang, The attack on "mona: Secure multiowner data sharing for dynamic groups in the cloud," in Proc. Int.Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185189.

[7] Burhan Ul Islam Khan, Rashidah F. Olanrewaju "SSM: Secure-Split-Merge Data Distribution in Cloud Infrastructure," in 2015 IEEE Conference on Open Systems (ICOS), August 24-26, 2015, Melaka, Malaysia

[8] Jie Xu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin, "Circuit Ciphertext- Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 27, NO. 1, JANUARY 2016.

[9] Joseph K. Liu, Member, IEEE, Man Ho Au, Member, IEEE, Xinyi Huang, Rongxing Lu, Senior Member, IEEE, and Jin Li, Fine-Grained "Two-Factor Access Control for Web-Based Cloud Computing Services," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,VOL. 11, NO. 3, MARCH 2016.

[10] Nazatul Haque Sultan Ferdous Ahmed Barbhuiya, "A Secure Re-Encryption Scheme for Data Sharing in Unreliable Cloud Environment," 978-1-5090-2616-6/16 2016 IEEE DOI 10.1109/SERVICES.2016.16.

[11] Zhongma 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