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

Miss. Rutuja Tuwar
PG Student
Department of Computer Engineering
Pune Institute of Computer Technology

Dr. R. B. Ingle
Faculty
Department of Computer Engineering
Pune Institute of Computer Technology

Abstract:

Continuous changes in the membership of data sharing giving security and privacy preservation are still challenging issues, especially for untruth cloud due to collusion attack. It is based on the secure key distribution without assuming any secure communication channel. Our system proposes a secure re-encryption scheme of data sharing scheme without assuming secure communication channel for dynamic group in cloud. It also prevents access of client after their revocation and protect after collusion attacks. In our system provide guarantee for secure sharing of data files when they are outsourced with double encryption. Our system is able to support the Dynamic groups when user join in the group or user revoked from group, the private key of other user compulsory recomputed and updated.

Keywords – Access control, privacy-preserving, Key Distribution and cloud Computing.

I. INTRODUCTION

Cloud computing provides on demand service and processing resources to the Users or devices. It is dynamic computing style in which dynamically scalable and usually virtualization resources are provided as a service over the internet. Fundamental service offered by cloud providers is data storage. Cloud servers managed by cloud providers which are not fully trusted. 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. One of the most significant difficulties is identity privacy for the wide deployment of cloud computing. Several security schemes for data sharing untrusted servers have been proposed. In these 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. 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. Finally, groups are normally dynamic in practice. Changes 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. An appropriate membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management.

MOTIVATION

In this paper we will improve the access control and data confidentially and efficiency. Access control are work on the two factor first one group member are able to use cloud resources for data operation and user cannot access the data when other user revoke the from particular group. Key distribution requirement securely obtain their private key from group Manger with certificate authorities.

OBJECTIVES

The primary goal of this work is to save the cloud Data from unauthorized user when user revoke from that particular group and that group is dynamically generated by Group Manger.

II. REVIEW OF LITERATURE

On the security of public key protocol Proposes public key encryption protocol, describes the various techniques to encrypt the public key[1].First complete group key management scheme which can supports all these functions yet preserves efficiency. The proposed scheme is 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].Achieving secure role based control on encrypted data in cloud achieved through RBAC. RBE scheme allows RBAC policies to be apply 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 our scheme are independent with the number of revoked users. Also they analyze 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) is introduced for the security of data. The proposed SSM scheme was it uses unique mechanism for performing splitting of data using AES 128 bit encryption key. The chunks of encrypted splits are being maintained on various group servers of different types of cloud zones. The comparative analysis shows that the proposed system gives effective outcomes as compared to various existing and traditional security standards[7].Security achieves against chosen-plaintext attacks using the k-multi linear Decisional Diffie-Hellman assumption[8]. Fine-grained two-factor authentication (2FA) access control system for cloud services. proposed 2FA access control system, it was an attribute based access control mechanism implemented with the necessity of both a user secret key and a lightweight security device[9].Efficient and secure re-encryption scheme has been 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. That scheme can achieve user revocation without whole cipher texts re-encryption and key re-distributions also, re-encryption is not performed until a user requests for that data, which reduces overheads. Further, it does not need any clock synchronization [10].

III. SYSTEM OVERVIEW/ SYSTEM ARCHITECTURE

In this New System Propose a secure data sharing scheme which can achieve through a secure key distribution and data sharing for dynamic group along with secure way non secure communication channel .New re encryption is used for assigning the permission data encryption. The Users can securely obtain there Private key from group Manger with Certificate authorities for verification scheme. The System can achieve the fine grained access control. Hybrid cloud is used for efficient use of cloud. Our System used for data sharing can be protected from collusion attack. The Revoked user not gets the original data access once when they revoked from particular even if they tried with untruth cloud. System supports the dynamic group efficiently when user joins the group or revoked from group their private key are compulsory update and recomputed.

PROPOSED SYSTEM ARCHITECTURE:

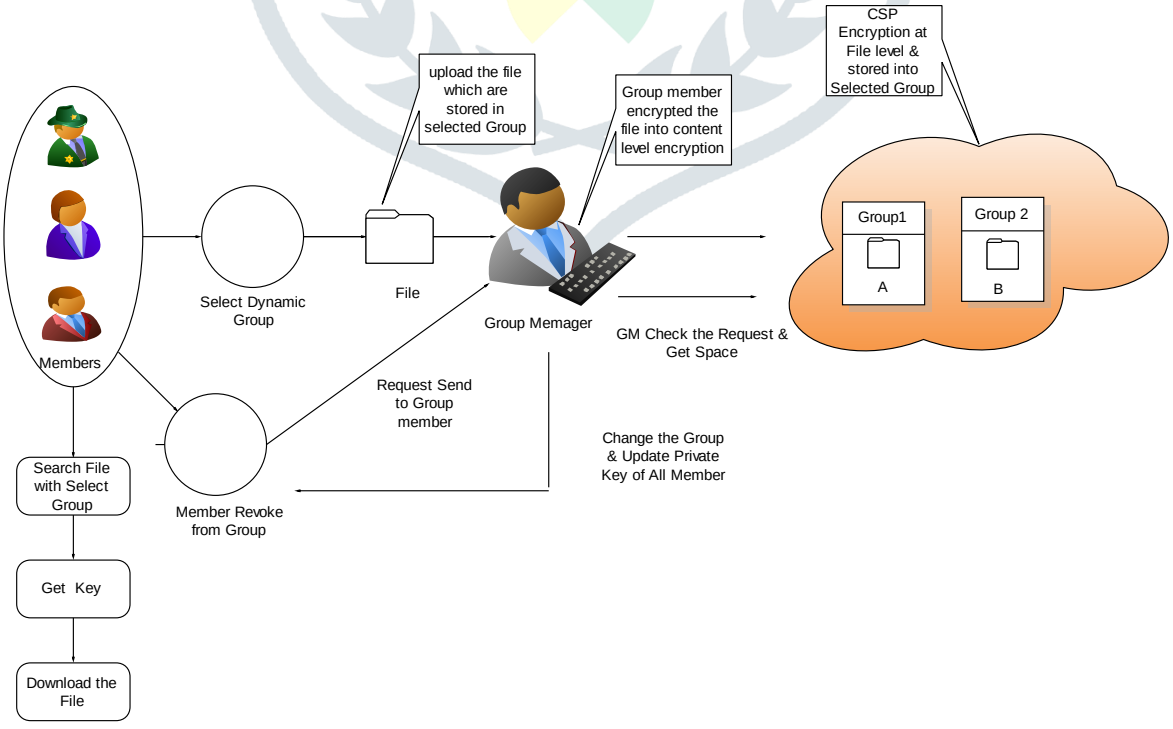

Fig1. Proposed System Architecture

EXPLANATION:

Dynamic Groups:

The Main Concepts of Dynamic Group users select the Particular group when user Register with Group. Groups are created by the Group Manger.

User Revoked or User Join:
When new user joins or revoked from particular group then the Private Key of particular user and other user of same group their private key compulsory update and recomputed.

Group Manger:
Group Manger is created the Groups. And Manger decided space of group and Dynamical efficiently used space.

IV. MATHEMATICAL MODEL

S={s, e, X, Y,Φ}

Where,

s = Start of the program.

1. Log in with webpage.

2. Load Files on cloud.

e = End of the program.

Retrieve the file from cloud storage system.

X = Input of the program.

Input should be File.

Y = Output of the program.

File will be first uploaded then search and send key and download the file

X, Y ∈ U

Let U be the Set of System.

U= {GM,GU, S, G, D}

Where GM,GU , F, S, T, M, D are the elements of the set.

GM=Group Manager

GU=Group User

S=Search keyword

G=Get key from user

D=Download file using key

Bilinear Maps:

Let G1 and G2 be additive cyclic groups of the same prime order q.

Let e :G1 *G2→G2 denote a bilinear map constructed with the following properties:

G1,∈ Z*q and P,Q∈ a, b ∀

1. Bilinear: ∀a,b∈ Z* and P,Q ∈ G1 , e(aP,bQ) = $e(P,Q)^{ah}$

2. Non generate: There exists a point Q such that e(Q.Q)≠ 1.

3. Computable: There is an efficient algorithm to compute e(P,Q) for any P,Q ∈G1

Mathematical Equations of Notation

ID_iThe Identity of user i

ID_{data}The Identity of data

Pk the public key of user that needs to be negotiated with group manager

Sk the corresponding private key to Pk

KEY=(x_i,A_i,B_i) the Private key which is distributed to the user from the group manager and used for data sharing

Enc_k() Symmetric encryption algorithms used the encryption key k

$AENC_k$() Asymmetric encryption algorithms used the encryption key k

UL group User List

DL Data List

P Public cloud

PP private cloud

M Original content read by GM in File.

Y result of Encryption algorithms

Equations:

ID_i,pk,ac,v_i(1)

U,R (2)

R.e(v_1.F(pk||ac||ID_i).P,W)=e(U,P) (3)

ID_i,V_2,$AENC_{sk}$(ID_i,,V_1,ac) (4)

$AENC_{pk}(KEY,V_2)$ (5)

$e(W,f_1(UL))=e(P,sig(UL))$

$ENC_{B1}(ID_{data},C1,C2,C,t_{data})$ (6)

$\{DF=(ID_{group},ID_{data},CE,EK,t_{data},),\sigma_{DF}\}$

$C_1=K.Y€G_1$ (7)

$C_2=K.P €G_1$ (8)

$K=Z^k€G_2$ (9)

$C=ENC_k(M)$ (10)

$EK=\{K_r,.W_{0,}.....W_m\}$

$CE=\{C_1,C_2,C\}_{Kr}$

$(ID_{group},ID_{data},CE,EK,t_{data},\sigma)DL$

$e(W,f_1(DF))=e(P,\sigma_{DF})$

$e(W,f_1(DF))=e(P,sig(DL))$

V. ALGORITHM

Blowfish Algorithms

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.
2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)
3. Encrypt the all-zero string with the Blowfish algorithm, using the data file described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).
5. Encrypt the output of step (3) using the Blowfish algorithm with the modified data
6. Replace P3 and P4 with the output of step (5).

Key Generation RSA (Ron Rivest, Adi Shamir and Leonard Adelman)

1. Choose p = 3 and q = 11
2. Compute n = p * q = 3 * 11 = 33
3. Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
4. Choose e such that 1 < e <φ(n) and e and n are co-prime. Let e = 7
5. Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
6. Public key is (e, n) => (7, 33)
7. Private key is (d, n) => (3, 33)
8. The encryption of m = 2 is c = 2^7 % 33 = 29
9. The decryption of c = 29 is m = 29^3 % 33 = 2

VI. RESULT

Our System expects the examination of some security parametersODBE, Mona and our plan. It is unmistakably observedthat the computation cost for people in our arrangement isunimportant to the amount of disavowed customers.

Parameter	Exiting System	Proposed System
Cost	High	Low
Security access based	Low	High
ODBE	Yes	No
RBAC	No	Yes
Data Security	No	Yes
Access Control	Yes	Yes
User Revocation	No	Yes
Data Confidentially	No	Yes
Anti-Collision attack	No	Yes

Table 1 Compassion of Exiting System and Proposed System

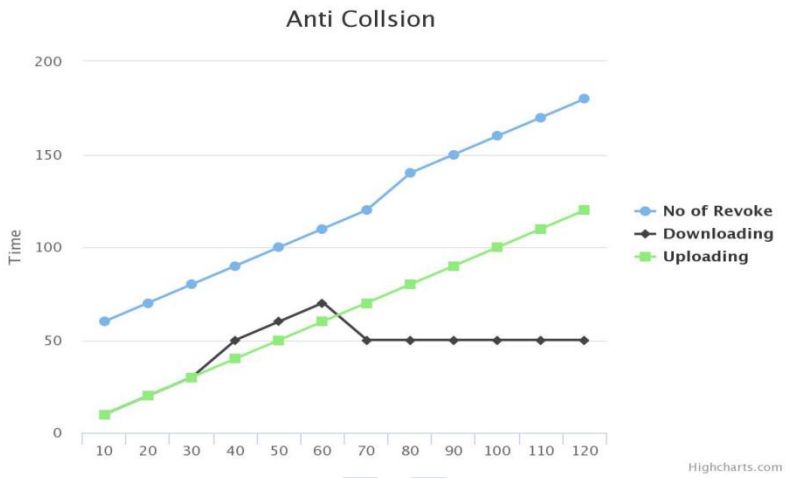

Fig 2 Graph between Uploading & Downloading and Number of Revoke

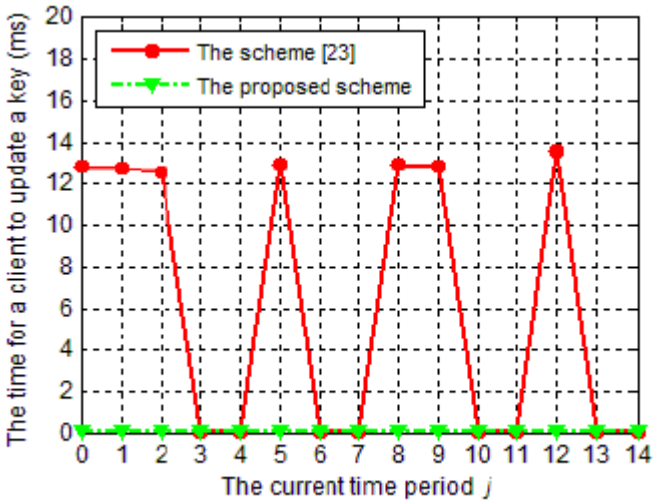

Fig 2 Graph between Current Times of Updating Private Key

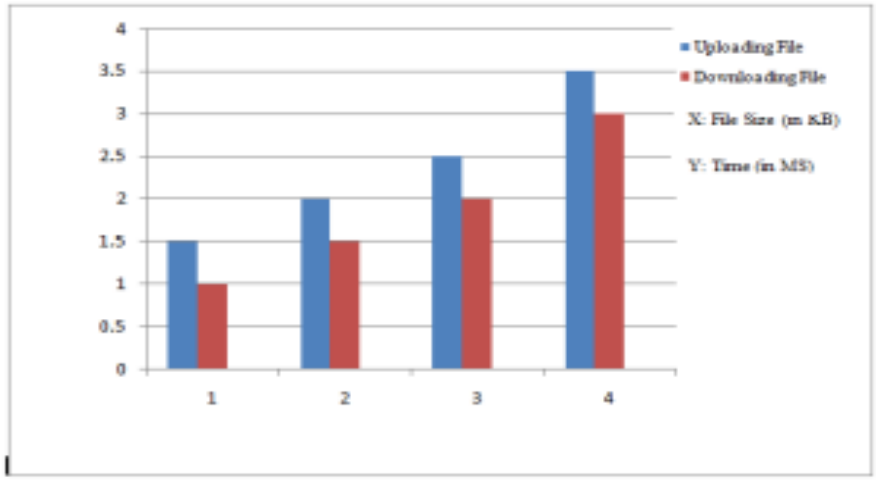

Fig 3 Graph between Uploading & Downloading Time of Different Size of Data

VII. 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 without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. System also provides the new double encryption technique for data security. New re-encryption provides tight authentication.

REFERENCES

[1] D. Dole 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. Zoo, Y.-S. Dai, and E. Bettino, A practical and flexible key management mechanism for trusted collaborative computing, in Proc. IEEE Conf. Compute. Common.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 multi owner 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 multi owner data sharing for dynamic groups in the cloud, in Proc. Int. Conf. Inf. Sci. Cloud Compute., Dec. 7, 2013, pp. 185189

[7] BurhanUl 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] JieXu, Qiaoyan Wen, Wenmin Li, and Zhengping Jin, Circuit Ciphertext- Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 11821191, Jun. 2013.

[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 Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 11821191, March 2013.
.

[10] NazatulHaque 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.