ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

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

Alka Taur, Prof. Jyoti Raghatwan,

Department of Computer Engineering, RMD Sinhgad School of Engineering, Pune, India

Assistant Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, Pune, India

ABSTRACT: Collusion attack on untrusted cloud is a challengingas it affects security and privacy due to continuous changesin membership. Without assuming any secure communicationchannel we can do it with secure key distribution. For dynamicgroup in the cloud we proposed a secure re-encryption key of datasharing. Proposed system does not allow any access to the cloudafter revocation of that client and protect cloud after collusionattack. In this system secure sharing of data files can be donewhen they are outsourced with double encryption. This systemsupport the dynamic groups when user join in the group or userswitched from groups, the private key of other user compulsoryrecomputed and updated.

KEYWORDS: Access control, privacy-preserving, Key Distribution and cloud Computing.

I. INTRODUCTION

Cloud computing provides efficient on demand service tothe user or devices by processing resources. Cloud computing provided through internet service which is dynamic computing style. A cloud provider fundamentally offers data storage as a service. Now a days Cloud based server managed by service provider may not be secure. As cloud provides data storage service so that user may store important and confidential documents may be business plans, budgets, audits etc. These data files must be secured as it is important and sensitive for the user. The securing document on the cloud is an importanttask. There are different methods to secure data files by encrypting data as ACP, RBAC, BGKM, MONA, ASSM, 2FAetc.When user upload their data then that data is encrypted and stored on cloud. One of when user access cloud in dynamic groupsit is very difficult to maintain privacy and identity of user, data for untrusted server. Several security schemes for data sharing untrusted servers have been proposed. Any user who uses cloud does not want to join cloud computing system if his identity and privacy may be disclosed to service provider and attackers. If data stored in any cloud is not safe then a user may face problems in future. For example If a person misbehaved or terminated from company he may share confidential files without any traces. Therefore the group manager must know the real identity of user who shares data. Multiple owner concepts is very important in a group, so that any user can able to access all stored data and services as per cloud provider. Every user in a cloud has authority to readdata also modify the data of their own work in the entire data file so that these groups will be dynamic in nature. In thedynamic group can faced different difficulties to share data by maintaining their privacy due to changes in the membership. The encrypted data stored in a cloud before adding any new user can be access through decryption keys. Decryption keys corresponding to the data stored in cloud may be difficult to get for the newly added user. Key management is an important task. In the key management there should be proper membership revocation mechanism with upgradation of secret key to reduce complication in key management. In this project work 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. 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.

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].A modified approach of Access Control Polynomial (ACP), it's very simple to understand, implement, easy flexible key management, Protect internal and external attackers and secure confidential status data in cloudEnvironment[2].With RBAC we can secure role based control on encrypted data in cloud. RBE allows RBAC policies for encrypted data stored in public in cloud. RBE based hybrid cloud storage architecture provide facility of an organization to maintain sensitive information related to organization in public cloud securely[3].Broadcast group key management is a one approach which satisfied different policies to encrypt documents this can be done using different public key such as attribute based encryption and proxy re-encryption. In the Broadcast group key management adding user or removing users can be done by updating only some public information. In this key management we can effectively store document in untrusted cloud[4].Secure multiowner data sharing in cloud for multiple groups can achieved through a system called MONA.In this system group signature, dynamic broadcast encryption is used for secretly sharing data by any user with other. TheEncryption computation and Storage overhead cost of MONA is varying with number of revoked users. The system analyses difficult proofs as security and demonstrate the efficiency with experiments[5].Secure split merge (SSM) is used for security of data effectively. The SSM uses AES128 bit encryption key for splitting of data. The different parts of encrypted splits are maintained on different group servers and cloud zones. The system gives effective outcome in comparison with various existing security standards[7].Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme has strongest form of access control policy. This scheme proven to be secure based on k-multilinear Decisional Diffie-Hellman assumption and assures data confidentiality[8]. Fine grained two factor authentication system was an attribute based access control implemented with necessity of both user lightweight security device and secret key[9].Cipher text policy attribute based encryption CPABE efficiently secure reencryption for data sharing in unreliable cloud environment. The re-encryption is performed only when user request for that data which reduces overhead. In CPABE based system there is no any need of clock synchronization[10].

SYSTEM OVERVIEW/ SYSTEM ARCHITECTURE

In this system we proposed a secure data sharing through asecrete key distribution for dynamic group along with secure communication channel. The new re-encryption is used for assigning the permissions for data encryption. The user can obtain their secrete key from group manager securely with certified verification scheme. In this system fine grained access control and hybrid cloud is used for efficient use of the cloud. The proposed system can be secured from collusion attack. The removed user cannot get the original data access once he removed from particular cloud even if tried with untrusted cloud. The proposed system supports the dynamic group efficiently when user joins or revoked from group, their private keys are updated and recomputed. Software Requirements Speciation:- The Introduction of software requirements speciation provides an overview of all software used in Projects which used the operating system Window 7,8,10. The Language used to implementation is java which required the JDK (Java SE Development kit) JDK have many version such as the 1.2, 1.3 and up to 1.7. Platform which used for JDK is eclipse, eclipse have lost of the version. To run the code in eclipse required the Server as the Apache tomcat 7.Data base used as the MYSQL version 5.

PROPOSED SYSTEM ARCHITECTURE:

The proposed system architecture for securing data sharingin a cloud with private key authentication as shown in figure1. Which contains group manager, group member, cloud, and their first level authentication with the help of text and second level authentication by secure one time password (OTP), which will be updated and recomputed continuously communicatedthrough users authenticated Email-id?

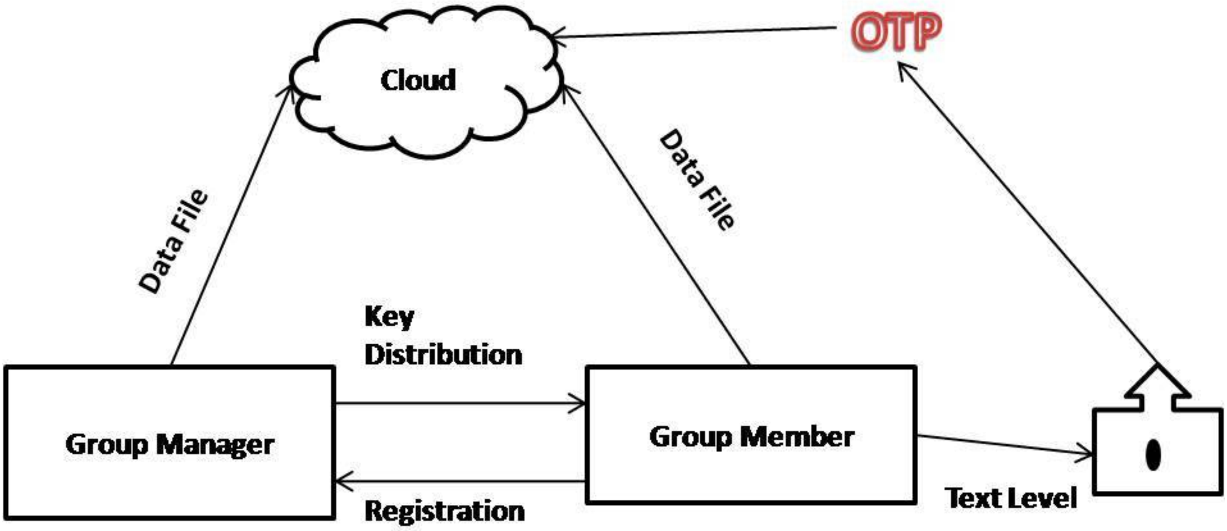


Fig1. Proposed System Architecture

EXPLANATION:

1) Upload MRI scan Image: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.

2) 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.

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

III. 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

DOI: 10.15680/IJIRCCE.2018.0606057

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,$\in$ Z*q and P,Q $\in$ a, b $\forall$
1. Bilinear: $\forall$ a,b $\in$ Z* and P,Q $\in$ G1 , $e(aP,bQ) = e(P,Q)^{ah}$
2. Non generate: There exists a point Q such that $e(Q.Q)\neq 1$.
3. Computable: There is an efficient algorithm to compute e(P,Q) for any P,Q $\in$G1

Mathematical Equations of Notation
ID_i The 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)

$EK=\{K_{r,}.W_{0,}................W_m\}$

$CE=\{C_{1,}C_{2,}C\}_{Kr}$

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

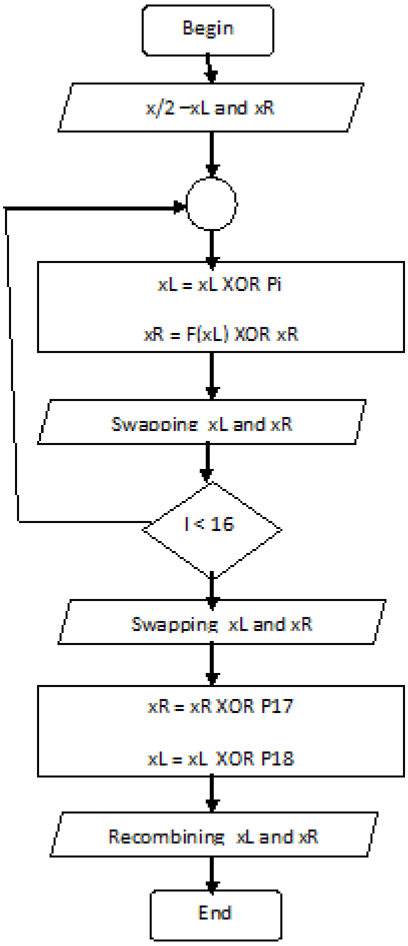
$e(W,f_1(DF))=e(P,\sigma_{DF})$

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

IV. ALGORITHM

Blowfish Algorithms

In this system we are using Blowfish algorithm along with DES. Our algorithm has 32 to 448 bit key. These key used to generate 18 32bit sub keys which is in p-array and 4 8*32s-boxes. This algorithm have 2 primitives i.e. addition and XOR operation.following figure shows this algorithm:



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

V. RESULT

We Expect the comparison of some Security parameter OBBE,Mona and Our Scheme. It is obviously observed that computation cost for members in our scheme is irrelevant to number of revoked users.

Fig. 1 Comparison with different Scheme

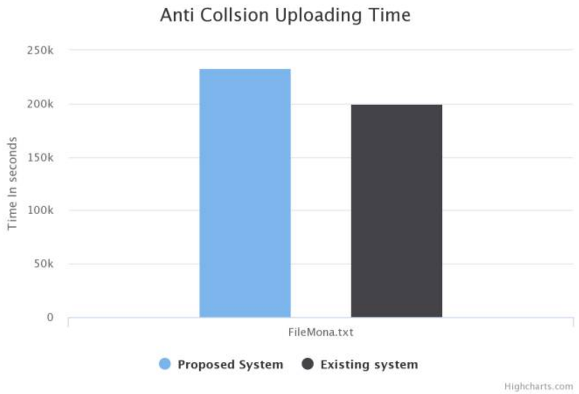


Fig 2 Comparison Uploading Time with Proposed System and Exiting System

User uploads the Data in Anti Collusion while uploading how much time to get the uploading and encryption the Data internally with previous system.

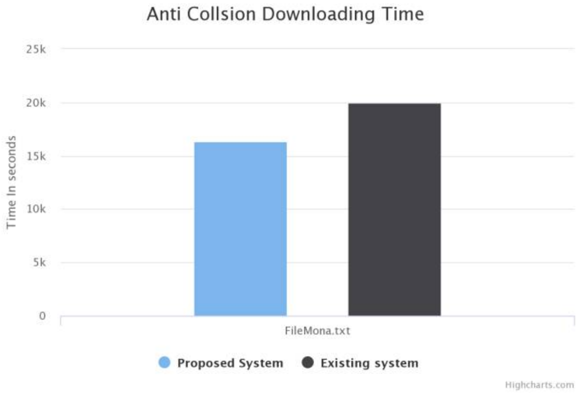


Fig 3 Comparison Downloading Time with Proposed System and Exiting System

User Search the Data From particular Group when while downloading the data or file from cloud when data is internally decryption is possible.

When user join or revoke from particular group then after searching the particular file then according to anti collusion rule if user join or revoke from the any particular group then private key of user is compulsory update and again stored in the cloud.

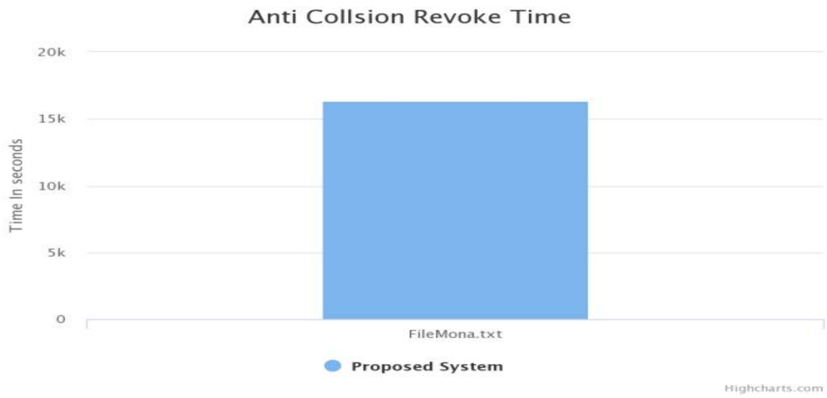


Fig 4 Anti collusion Revoke.

VI. CONCLUSION

The proposed system share data securely in untruth cloud for dynamic groups. We proposed authentication system, which includes text level authentication and OTP which is highly secure. In this proposed system user can shared information to other users in a group without disclosing identity to the cloud. In proposed system joining of new user and revocation efficiently. Without updating private keys of users we can revoked User through a public revocation list. Which will not affect existing users, a newly added user can decodes the files stored in the cloud before their participation. The proposed system provides new double encryption technique for data security with 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-basedaccess 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] 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 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] 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