International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

ACHIEVING SECURE ANTI - COLLUSION FOR SHARING OF DATA BETWEEN DYNAMIC GROUPS IN THE CLOUD

G.Jaccob Britto[1], Arivumalar[2]
[1] Assistant Professor, Yadava College, Madurai.
[2] Professor, Prist University, Tanjore.

Abstract - Cloud computing give more benefits to user for achieving very efficient and cost effective approach to share data between members of group which is created in cloud with very cost effective maintenance and management. In added benefit with this efficient data sharing, it also provides security for data files, because they are outsourced. But the process of preserving security is little bit complicated because of adequate change of members of group and it may lead to collusion attack. The existing systems provide security over communication channel is practically difficult to implement. In this paper, a secure data sharing method for dynamic members is proposed and implement in 4 phases. In first phase, a secure way for key distribution without any secure communication channel is proposed and the members of the group can securely preserve their private keys from group admin. In second phase, our proposed scheme achieves a well-structured access control tool, which protects the cloud by denying the access for the revoked user. In third phase, we achieve a scheme to prevent collusion attack. In this scheme the revoked user cannot get the original data file. In final phase, fine efficiency would be accomplished by preserving the private keys of previous user, which means that there is no need to change their private keys in any scenarios like addition of new user in group and removal of existing user from group.

Keywords: Private key, cloud security, privacy preserving, key distribution.

1. INTRODUCTION

Cloud computing is the wise choice of better utilization of resources and sharing of files with low maintenance cost. In cloud computing, service providers offer an abstraction of infinite storage space for clients to host data. This service reduces the client's data management financial overhead by shifting the local server data to cloud server.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

By shifting the client's data from their server to provider's server, then security becomes main concern and sensitive. To achieve this data security, the conventional Encryption (Plaintext→Cipher text) and Decryption (Cipher text → Plaintext) methodology was used in cloud. Unfortunately it is difficult to design in an efficient manner because of the frequent change of the membership group (dynamic group) in cloud.

In our reference paper [1], the author Kallahalla et al. represent a system which enable data sharing by using the technique of dividing files into file group and encrypting each group with file block key. But still there is a problem of need for updation of such keys and frequent key distribution for a user revocation which creates heavy overhead in key distribution. In [2], [3] some more scheme for secure data sharing are proposed. But the complexity increases when the number of active user and revoked user is increased.

In [4], the key policy attribute based encryption is proposed which still unsucceed in privacy preserving. In [5], the proxy re-encryption and lazy re-encryption is proposed. In [6], the author Yu et al. exploited and combined techniques of [4] and [5] to achieve fine – grained data access control without disclosing data contents. However, the single owner manner may hinder the implementation of application.

In [7], the author Lu et al. proposed a scheme which is used signature for groups and in [8], cipher text policy attribution based encryption technique is exploited. In both systems, each user obtains pair of keys after the registration named as Attribute key – Group signature key where Attribute key is used to decrypt the data which is encrypted by the attribute based encryption and Group signature key is used for privacy preserving and traceability. Here the security is preserved in but revocation is not supported.

In reference paper [9], a secure multi – owner data sharing scheme names Mona is presented by Liu et al. This system can achieve better access control and prevent revoked user to access the data after they are revoked. But this system is still lost its efficiency when collusion attack is occurred by revoked user. The paper [10] also proposed a scheme like this which has the same problem. In these papers the revoked user can use his private key to decrypt the encrypted data file and get the secret data after his revocation by conspiring with the cloud. In the phase of file access, first of all, the revoked user

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

sends his request to the cloud, and then the cloud responds the corresponding encrypted data file and revocation list to the revoked user without verifications. Next, the revoked user can compute the decryption key with the help of the attack algorithm. Finally, this attack can lead to the revoked users getting the sharing data and disclosing other secrets of legitimate members.

Zhou et al. [11] proposed a secure access control scheme for encrypted data by using role based techniques. This technique achieves effective user revocation and secures large data storage. But lag of verification between members this system has lots of chances to affect by attack and may lead to disclosing sensitive data files.

Nabeel et al. [12], presented a privacy preserving policy based content sharing scheme in public cloud. But it is not secure because of the weak protection of commitment in the phase of identity token issuance.

In this proposed paper, we propose a secure data sharing scheme which can achieve secure key distribution and data sharing for dynamic group. Here we give importance to some contribution which is listed below.

1. A secure way for key distribution without any secure communication channel is proposed and the members of the group can securely preserve their private keys from group admin without any Certificate Authorities due to the verification for public key of the user.
2. Our proposed scheme achieves a well-structured access control tool, which protects the cloud by denying the access for the revoked user.
3. We achieve a scheme to prevent collusion attack. In this scheme the revoked user cannot get the original data file. This can achieve secure user revocation with the help of polynomial function.
4. Fine efficiency would be accomplished by preserving the private keys of previous user, which means that there is no need to change their private keys in any scenarios like addition of new user in group and removal of existing user from group.
5. It provides security analysis to prove the security and also perform simulation to demonstrate the efficiency of our scheme.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

2. MODEL AND DESIGN

2.1. MODEL

When we considering the model of proposed system, we have to take Threat model and System model are acceptable models.

2.1.1. Threat Model

In this paper we propose Threat model of our scheme from the paper of Delov – Yao [14] Model. In this referred paper, the adversary can overhear, intercept, and synthesis any message at the communication channels. With the Delov-Yao model, the only way to protect the information from attacking by the passive eavesdroppers and active saboteurs is to design the effective security protocols. This means there is not any secure communication channels between the communication entities. Therefore, this kind of threaten model can be more effective and practical to demonstrate the communication and easy to implement.

2.1.2. System model

This model consists of 3 entities as shown in Figure 1. The cloud is maintained by service provider who provides storage space to store data of clients in a payable manner. Since the service providers are untrusted which results the cloud is also untrusted and try to fetch the data which may contain some confidential.

So to make it secure, the cloud allows creating a group by some person called as group admin who take charge foe parameter generation, user registration & revocation. The group admin is trusted by other parties.

Users (group members) are set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

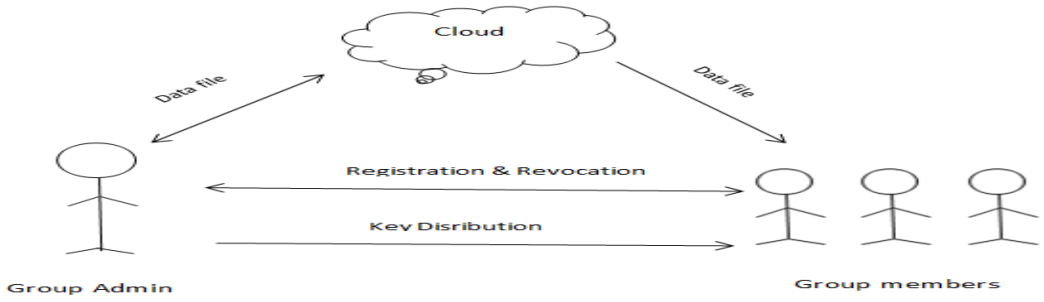

Figure 1

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

2.2. DESIGN

When considering about design we have to describe the design goals for the proposed scheme which includes, Key distribution, Data confidentiality, Access control, Efficiency.

2.2.1. Key Distribution

In existing scheme, the key distribution is achieved through communication channel which assumed that the channel is secure. But in the proposed scheme, the user can securely obtain their private keys from the group admin without any certificate authorities.

2.2.2. Access control

While designing, in aspect of Access control we consider 3 design goals. First, group members are able to use the cloud resources for storing and sharing of data. Second, resources of cloud should not be accessed by unauthorized users. Third, the revoked user cannot use the cloud storage with help of previously distributed keys.

2.2.3. Data confidentiality

To maintain availability of Data confidentiality for dynamic group is still an important and challenging issue. To achieve this, unauthorized users become incapable of learning the content of data stored in cloud. Specifically the revoked users should prevent to decrypt the file after the revocation.

2.2.4. Efficiency

The proposed system has great efficiency by achieve the following goals. Any user can store and share data file in the group. Revocation of user should not affect any other process. Especially, the other authorized user can remain use their previous private key there is no need to update their keys.

3. PROPOSED SYSTEM

3.1. PREPROCESSING BASIC

Before implementing this scheme, we need to aware of the some basic preliminary which includes Bilinear Maps and Complexity Assumption. Also the reader should know the rotation used in this paper.

3.1.1. Bilinear Maps

Let G1 and G2 be additive cyclic groups of the same primeorder. Let e: $G_1 \times G_1 \rightarrow G2$ denote a bilinear mapconstructed with the following properties:

i. Bilinear: For all a, b $\in Z^*_q$ and P, Q $\in$ G1,e(aP,bQ) = $e(P, Q)^{ab}$.
ii. Nondegenerate: There exists a point Q such thate(Q, Q) $\neq 1$.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

iii. Computable: There is an efficient algorithm to computee (P, Q) for any P, Q € G1.

iv. Secured : There is very secured algorithms are processed.

3.1.2. Complexity Assumption

Definition 1(Basic Diffie-Hellman Problem (BDHP) Assumption [15]).

Given base point P and a value γ € Z_q^*,it is easy to compute γ. P. However, given P, γ.P, it is infeasibleto compute γ because of the discrete logarithm problem.

Definition 2 (Decisional Diffie-Hellman Problem (DDHP)Assumption [16]).

Similar to definition 1, given base point Pand aP, (a+b)P, it is infeasible to compute bP.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent(WBDHE) Assumption [17]).

For unknown a €Z_q^*, givenY, aY,a^2Y, ……a^lY, P € G1, it is infeasible to compute e(Y, P) $^{1/a}$.

3.1.3. Notation

Each user has a pair of keys (pk,sk), which is used in theasymmetric encryption algorithm, and pk needs to benegotiated with the group manager on the condition thatno Certificate Authorities and security channels areinvolved in. KEY is the private key of the user and isused for data sharing in the scheme. UL is the group userlist which records part of the private keys of the legalgroup users. DL is the data list which records the identityof the sharing data and the time that they are updated.The description of notation used in our scheme is illustratedin Table 1.

NOTATION	DESCRIPTION
ID_i	The identity of user i
ID_{data}	The identity of $data_i$
pk	The public key of the user that needs to be negotiated with group manager.
sk	The corresponding private key to pk.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

Key = (x_i, A_i, B_i)	The private key which is distributed to the user from group manager and used for data sharing.
$Enc_k()$	Symmetric encryption algorithm used key k.
$AENC_k()$	Asymmetric encryption algorithm used key k.
UL	Group user list
DL	Data list

Table 1

3.2. DESCRIPTION OF SCHEME

The implementation of our scheme should include System initialization, Registration, Revocation, File upload, File download.

3.2.1. System initialization

This operation is performed by the group admin. He generates a Bilinear map group system BS = (q, G_1, G_2, e (., .)). After this map generation he selects 2 random variables P, G $\in$ $G_1$and numeric value $\gamma \in Z_q^*$, and then calculate W = γ.P, Y= γ.G and Z= e(G,P). Finally, the group admin publishes the parameters (BS, P, W, Y, Z, f, f1, Enc()). Here f and f1 are hash functions which are defined as below.

$$f : \{0,1\}^* \rightarrow Z_q^*$$

$$f1 : \{0, 1\}^* \rightarrow G1$$

Enc() is an Encryption algorithm. In added with these parameters group admin maintain a secret master key as (γ, G).

3.2.2. Registration

The operation of user registration is illustrated in Figure 2.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

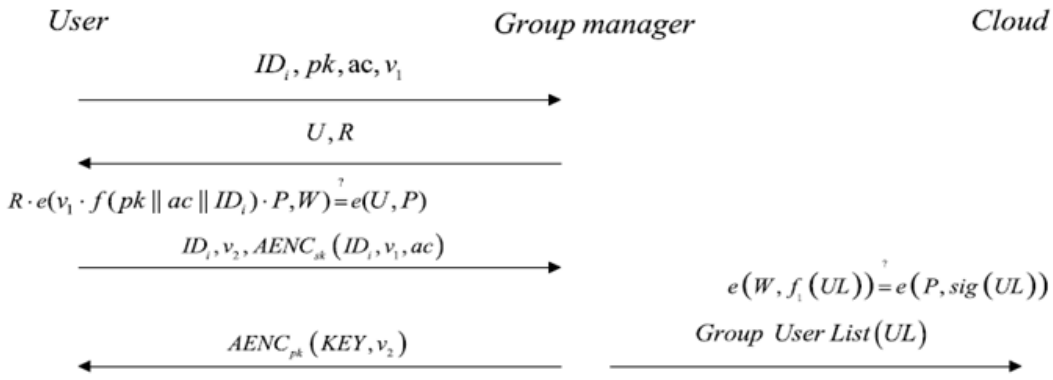

Figure 2

The group members and group admin are involved in this operation. It is initiated by the user who wants to register in the cloud.

Initially, the user create a request message which contains Identity of user, Public key, Account and Random number chosen by user in the format like (ID_i, pk, ac, v_1).

The public key used here is also used in Asymmetric Encryption Algorithm and ac is the account of user used to pay for the registration and v_1 belongs to Z_q^*.

When admin receive this request, he select a random number r which belongs to $Z_q^*$and calculate R and U where they are defined as below,

$R = e(P, P)^r$ and

$U = (r+\gamma.v_1.f(pk||ac||ID_i)).P$

After computing U and R the admin creates a reply message with these terms and forward to user for verification which is performed by user.

For this verification user perform and check the equality with U and R by using the following operation.

$R.\ e(v_1.f(pk||ac||ID_i).P, W) = e(U,P)$.

After the successful verification, the user sends the message of (ID_i, v_2, $AENC_{sk}(ID_i,v_1,ac)$) to the group admin where v_2 is the random number andbelongs to Z_q^*, AENC() is a Symmetric Encryption Algorithm and sk is the private key corresponding to pk.

After this, the admin performs the decryption for $AENC_{sk}(ID_i,v_1,ac)$ and checks the equality comparison for identity ID_i and the decrypted number v_1 with the $ID_i$and $v_1$received in previous message.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

By succeeding all these verification, admin selects another random number x_i belongs to Z_q^* and compute the following equation which are going to use in construction of KEY.

$$A_i = \frac{1}{\gamma + x_i} .P \in G_1$$

$$B_i = \frac{x_i}{\gamma + x_i} . G \in G_1 \quad \rightarrow (1)$$

$$Vi = f(B_i)$$

Then these terms are grouped and create the message KEY (x_i, A_i, B_i) which is going to distributed and used in accessing control.

By successfully generating KEY message, the admin then sends the encrypted message $AENC_{pk}(KEY,v_2)$ to user and stores (x_i, A_i, V_i, ID_i) in the local storage space. In addition, the group admin append (Ai, x_i) to the group user list – UL which makes confirmation to the user.

After adding new user the UL should be refreshed with new Timestamp t_{ul} and update the signature of admin sig(UL) = γf1(UL) and this refreshed UL passed to cloud and make verification by checking the equation e(W,f1(UL)) = e(P, sig(UL)) and store this new updated user list into cloud if the verification is succeed.

At last, the user decrypts the message $AENC_{pk}(KEY,v_2)$ by his private key and obtain his KEY (x_i, A_i, B_i) which is generated by admin. By competing all these, the user becomes a group member and available for data sharing.

3.2.3. File upload

The operation of File upload is illustrated in Figure 3.

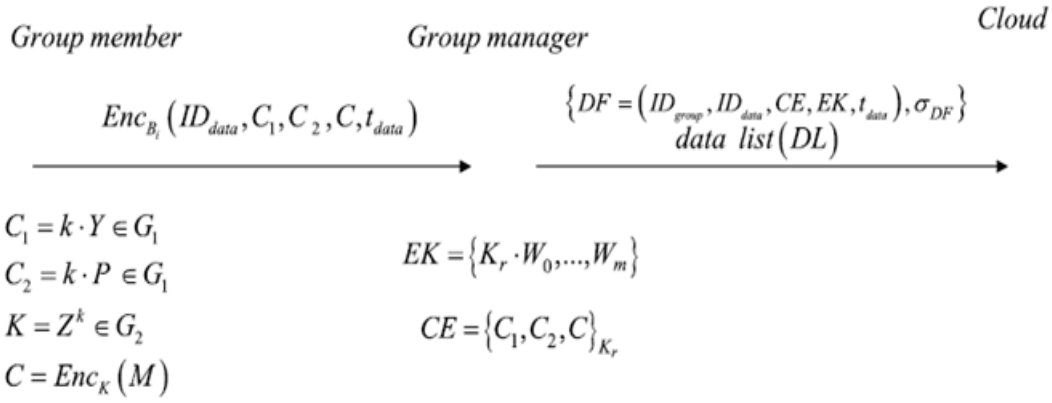

Figure 3

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

To upload a file in a group the member of that group select a unique data file and give name to that file as ID_{data} and choose a random number k € Z_q^*, and then compute the parameters C_1, C_2, K, C which are going to use in upload process. The following are the equation to calculate those parameters.

$$C1 = k.Y \in G_1.$$
$$C2 = k.P \in G_1. \quad \rightarrow (2)$$
$$K = Z^k \in G_2.$$
$$C = Enc_k (M)$$

Then the group member encrypts (ID_{data} , C_1, C_2, C,t_{data}) with his private key B_i, where t_{data} is the real time stamp.At last, the group member sends Enc_{Bi}(ID_{data}, C_1, C_2, C,t_{data})to the group admin.

After getting this message, admin decrypt it and gets (ID_{data} , C_1, C_2, C), then the group admin checks the legal group member in his local storage space if Bi is the private key of a legal user, then the group admin construct the polynomial function, and exponential function as follows, $f_p(x)=\prod_{j=1}^{m}(x - V_j) = \sum_{i=0}^{m} a^i x^i (mod\ q)$

$\{W_0 \ldots W_m\} = \{G^{a0} \ldots G^{am}\}$

After that, a random revers encryption key K_r is selected by group manager and constructs EK = $\{K_r.W_0 \ldots W_m\}$. Finally, an encryption is performed by group admin for the cipher text CE = $\{C_1, C_2, C)$ K_r with a key and create Data File in the format of {DF=(ID_{group},ID_{data}, CE, EK, t_{data}), σ_{DF}}. Then this file is passed to the cloud when t_{data}referred as the time that the Data File is uploaded and σ_{DF}= γ f1(DF) is the signature of the group admin for the Data File.

Besides, the Data List is sends to cloud by the admin. Then this Data File is verified for its freshness by users. This Data File and current time is then appended to the Data List table which is called as DL in the format of (ID_{data}, t_{data}). This Data List is updated every day by admin to guarantee the latest version of Data File. At last, the group admin adds his signature sig(DL) = γ f1(DL) to the Data List in cloud for storage.

Finally, after receiving the message, the file is uploaded to the cloud by verifying the identity of admin by checking the equation e (W, f1(DF)) = e(P,σ_{DF}).

3.2.4. User Revocation

This process is performed by group admin and service provider of cloud and it is illustrated in figure 4.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

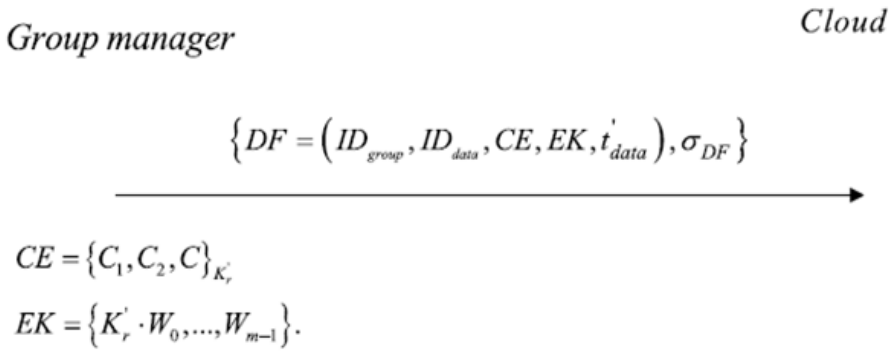

Figure 4

There is a 2 step process when a user is revoked from group. In the first step, the admin sends the revoked message {DF=(ID_{group},ID_{data}, CE, EK, t'_{data}), σ_{DF}} to cloud which contain new data list. Constructing this message includes the following processes.

First the user i who wants to revoke from the group is removed from group user list in the local storage space of cloud and updating is takes place in the clouds storage space. After updating the admin generates new polynomial function and new exponential function by considering there is m legal group members. The functions are described as follows,

$f'_p(x)=\prod_{j\neq ij=1}^{m}(x - V_j) = \sum_{j=0}^{m-1} a^j x^j (mod\ q)$

$\{W_0 \ldots W_{m-1}\} = \{G^a{}_0 \ldots G^a{}_{m-1}\}$

After constructing these functions, a new reverse random encryption key K_r' is chosen and construct EK = $\{K_r'.W_0 \ldots W_{m-1}\}$, by using that key, cipher text CE is computed by the equation CE = $\{C_1, C_2, C\}K_r'$. Then the admin put his signature $\sigma_{DF}$to the constructed message DF=(ID_{group},ID_{data}, CE, EK, t'_{data}) where t'_{data} is the time stamp and finally the revoked message is created and sends to the cloud.

In the second step process, the cloud receives the revoked message which contains modified Data List and verifies the signature by checking the equation e(W,f1(DF)) = e(P,σ_{DF}). After successful verification, thecloud the cloud replaces the old data file with the newdata file.In addition, the group manager updates all the timestamp t'_{data} of the data files in the group for the data list.Then the group manager sends the new data list to thecloud for storage. Finally, the cloud updates the data list.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

3.2.5. File download

This operation is performed by the group member and thecloud, as illustrated in Fig. 6, the group member encryptsID_{data} with his key A_i and sends ID_{group}, ID_i, $Enc_{Ai}(ID_{data})$ as a request to the cloud. On receiving the message, thecloud decrypts it and compares the encryption key A_i withkeys in the group user list, if the encryption key A_i is in thelist, the cloud then sends the corresponding data file {DF=(ID_{group},ID_{data}, CE, EK, t_{data}), σ_{DF}} and the data listto the group member.

Having received the message sent by the cloud, thegroup member verifies the validity of the data file and thelist by checking the equation e(W,f1(DF)) = e(P,σ_{DF}) and e(W,f1(DL)) = e(P, sig(DL)). Then the group memberchecks if the time stamp stored in the DF and the data list isthe same. Finally, the group member starts to decrypt thedata file after successful verification.

In order to decrypt the original data, the group memberneeds to perform two decryptions. For the decryptionof the re-encryption, the group member computesV_i= f(B_i) with his private key, then he computes the re-encryptionkey K_r. W_0. $\prod_{j=1}^{m}(W_j)^{V_i{}^j}$ = K_r. $G^{f_p(V_i)}$ = K_r. Finally, the group member decrypts CE and gets (C_1, C_2,C). For the decryption of the first encryption, thegroup member computes K = e(C_1, A)e(C_2,B), and themember can decrypt the correct cipher text.

Finally, the group member can decrypt the encrypteddata C and get the original data file M by leveraging theencryption key K.

4. PERFORMANCE VALUATION

Our scheme is compared with Mona [9], Original Dynamic Broadcast Encryption (ODBE) [5], and RBAC [11]. For all the schemes mentioned above, we set same values for all common parameters. That is, without loss of generality,we set p = 160 and the elements in G1 and G2 to be 161and 1,024 bits, respectively. In addition, we assume the sizeof the data identity is 16 bits, which yield a group capacityof 2^{16} data files. Similarly, the size of user and group identityare also set 16 bits. After completing this preprocess, the performance is simulated with the network simulator NS2 and the result are monitored. By using these results, we can compute the cost of cloud and member. Also we can make analysis for security which is main concern of our scheme.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

4.1. Cloud computation cost

The costs of the cloud for file upload are computed in all schemes and make comparisons. In general, the cost is acceptable in all schemes. In some scenario the cost would get changed to inacceptable level. For example, In Mona scheme, cost is increases with the number ofrevoked users, as the revocation verification cost increases. But in our scheme the cost should not be affected for increase in number of revoked user. In RBAC scheme the computation cost is very small, because there is no verification between communication entities which results security problem.

Now consider the file download process in which the size of file is 10 to 100 MBs. If we find computation cost of cloud for all schemes described above, the cost is acceptable in general which is similar to the operation of file upload. But in the scheme Mona, the cost increases when the number of revoked user increases, because of the complex revocation verification operation. But in our scheme, the cloud just simply verifies the signature of admin. Hence, the computation cost of the cloud for file download is irrelevant to the number of revoked users. In the scheme RBAC, the cloud performs some algorithm operation to decrypt data file. So if the size of file is increased then the computation cost is increased. But in Mona and our scheme the computation cost is independent with the size of file.

4.2. Member Computation Cost

Here we compare the computation cost of members for the process of file upload for the schemes Mona, RBAC and our scheme. Obviously we can said that the cost in our scheme is irrelevant to the number of revoked user, because we move the operation of user revocation to the admin, so that the legal clients can encrypts the data file alone without involving information of other clients, including both legal and revoked clients. But in RBAC, the cost increases when the number of revoked user increases. The reason is that several operations including multiplication and exponentiation have to be performed by clients to compute the parameters in RBAC.

Now, we consider the file download operation in which the size of file is 10 to 100 Mbytes. For this process the computation cost of member is irrelevant to the number of revoked user in RBAC scheme. Because the operation for members to decrypt the data file almost remain the same. But in Mona scheme, the cost is increased when revoked user increased. The

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

reason is that, the user needs to perform computation for revocation verification and check whether the data owner is revoked user. Besides theabove operations, more parameters need to be computedby members in ODBE. But in our scheme, the computationcost decreases when the number of revoked user is increased, because of the computation for the recovery ofthe secret parameter decreases with the number ofrevoked users.

4.3. Security Comparison

In general our scheme can achieve secure key distribution, fine access control, secure user revocation, anti – collusion attack, data confidentiality. By comparing our scheme with other schemes like Mona, ODBE, and RBAC our scheme alone has secure key distribution. The fine access control is achieved by all schemes. The secure user revocation and anti – collusion attack is achieved alone in ODBE and in our scheme. The data confidentiality is preserved in our scheme alone. By seeing all these, clearly we come to know that our scheme has more advantages than other. This comparison is shown in Table 2.

Performance criteria	**Achieved schemes**			
Access control	Our scheme	ODBE	Mona	RBAC
Anti – Collusion attack	Our scheme		ODBE	
Secure user revocation	Our scheme		ODBE	
Data confidentiality	Our scheme			
Secure key distribution	Our scheme			

Table 2

5. CONCLUSION

In this paper, we design very secure anti – Collusion attack enabling data sharing for dynamic group in cloud.In our scheme, theusers can securely obtain their private keys from group managerCertificate Authorities and secure communicationchannels. Also, our scheme is able to support dynamicgroups efficiently, when a new

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

user joins in the group or auser is revoked from the group, the private keys of the otherusers do not need to be recomputed and updated. In addition to that, in our scheme the revokedusers can not be able to get the original data files once theyare revoked even if they conspire with the untrusted cloud.

REFERENCES

[1] M. Kallahalla, E. Riedel, R.Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[2] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. SecuritySymp., 2003, pp. 131–145.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.

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

[5] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography,2007, pp. 39–59.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc.ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security,2010, pp. 282–292.

[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography,2008, pp. 53–70.

[9] 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. 1182–1191, Jun. 2013.

[10] 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. 185–189.

[11] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-301 PAGE NO: 2004-2019

Forensics Security, vol. 8, no. 12, pp. 1947–1960,Dec. 2013.

[12] 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. 2602–2614, Nov. 2013.

[13] Zhongma Zhu and Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," IEEE Trans. On parallel and distributed system, vol. 27, no. 1, Jan. 2016.

[14] D. Dolev and A. C. Yao, "On the security of public key protocols,"IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[15] B. Den Boer, "Diffie–Hellman is as strong as discrete log for certainprimes," in Proc. Adv. Cryptol., 1988, p. 530.

[16] D. Boneh, X. Boyen, and H. Shacham, "Short group signature,"in Proc. Int. Cryptology Conf. Adv. Cryptology, 2004, pp. 41–55.

[17] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Proc. Annu. Int. Conf.Theory Appl. Cryptographic Techn., 2005, pp. 440–456.