ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (133-142), Month: April 2015 – September 2015, Available at: www.paperpublications.org

Secure Data Sharing For Dynamic Groups in Multi-Attorney Manner Using Cloud

[1]Vijaya Kumar Patil C, [2]Manjunath H

[1]Dept. Of Computer Science & Engg. Mangalore Institute of Technology and Engineering Mangalore, Karnataka, India.
[2]HOD, Dept.Of Information Science & Engg. Mangalore Institute of Technology and Engineering, Mangalore, Karnataka, India.

***Abstract*: Cloud computing provides an economical and efficient solution for sharing data among the cloud users in the group , users sharing data in a multi-attorney manner preserving data and identity privacy from an untrusted cloud, it is still a challenging issue, due to frequent change of the membership in the group. In this paper, we propose a multi-attorney data sharing scheme for the dynamic groups in the cloud. By combing group signature and Tripple DES encryption techniques, any cloud user anonymously share the data with others. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.**

***Keywords:* cloud computing, data sharing, privacy-preserving, access control, and dynamic groups.**

1. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology [1] due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most important services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following Challenging issues:
First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud service providers and attackers. On the Other hand, unconditional identity privacy may acquire the abuse 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 (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

Second, it is highly recommended that any member in a group should be able to share data and storing data in the dynamic group provided by the cloud service providers, which is defined as the multi-attorney manner. Compared with the single-attorney manner [3], where only the admin of the group can share the data, store and modify data in the cloud, so data sharing in the multiple-attorney manner in dynamic group is more flexible. More concretely, group member can access the data and also modify his / her part of data in the group. Last but not least, groups are dynamic in nature, i.e new member entry into the group and current member revocation from the group. So the changes in group membership make secure data sharing is very difficult in the dynamic group. On one hand, the anonymous system challenges new granted users can access the data files stored in the cloud before their participation into the group, because it is not possible for

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (133-142), Month: April 2015 – September 2015, Available at: www.paperpublications.org

new registered member to contact with anonymous data owners in the cloud, and obtain the corresponding decryption keys. On the other hand, an efficient user revocation mechanism from the group without updating the secret keys of the remaining users is also desired to minimize the complexity of key management. Several security schemes to share data on untrusted servers have been proposed [4], [5], [6]. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized members in the cloud. Thus, unauthorized users as well as storage servers cannot access the file data content because they don't knowledge of the decryption keys However; the complexities of user entry and revocation in these schemes are directly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. [7] proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique [8], which allows any users in a group to share data with other members in group. However, the issue of user revocation is not specified in this scheme. Yu et al. [3] proposed a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique [9]. unluckily, the single-attorney manner hinders the adoption of their scheme into the case, where any granted user to store and share data. To solve the challenges presented above, we propose a secure data sharing scheme for dynamic groups in multi-attorney manner using the cloud. The main contributions of this proposed system include:

1. We propose a secure multi-attorney data sharing scheme. It allows that any user in the group can securely share data with others members in the untrusted cloud.

2. Proposed scheme supports dynamic groups more efficiently. Specifically, new registered users can directly access data files uploaded before their participation without contacting with data owners. User revocation can be easily done through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.

3. This technique provides secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously store and share data in the cloud. Moreover, the real identity of file data owners can be traceable by the group admin when any malicious activity done group member.

4. This technique provide exact security analysis, and perform Extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

2. LITERATURE SURVEY

In [4], Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation. Undesired effort, restoration of blur image is very important in many of the cases [3].

In [5], files stored on the untrusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. Thus, the size of the file metadata is proportional to the number of authorized users. The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated. In their extension version, the NNL construction [10] is used for efficient key revocation. However, when a new user joins the group, the private key of each user in an NNL system needs to be recomputed, which may limit the application for dynamic groups. Another concern is that the computation overhead of encryption linearly increases with the sharing scale.

Ateniese et al. [6] leveraged proxy reencryptions to secure distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly reencrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (133-142), Month: April 2015 – September 2015, Available at: www.paperpublications.org

In [3], Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the KPABE technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a ciphertext if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file reencryption and user secret key update to cloud servers. However, the single-attorney manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

Lu et al. [7] proposed a secure provenance scheme, which is built upon group signatures and ciphertext-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs encrypted data with her group signature key for privacy preserving and traceability. However, user revocation is not supported in their scheme.

From the above analysis, we can observe that how to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be a challenging issue. In this paper, we propose a novel Mona protocol for secure data sharing in cloud computing. Compared with the existing works, Mona offers unique features as follows:

1. Any user in the group can store and share data files with others by the cloud.

2. The encryption complexity and size of ciphertexts are independent with the number of revoked users in the system.

3. User revocation can be achieved without updating the private keys of the remaining users.

4. A new user can directly decrypt the files stored in the cloud before his participation.

3. PRELIMINARIES

3.1 Bilinear Maps

Let G_1 and G_2 be an additive cyclic group and a multiplicative cyclic group of the same prime order q, respectively [11]. Let e : $G_1 \times G_1 \rightarrow G_2$ denote a bilinear map constructed with the following properties:

1. Bilinear: for all a,b$\in$Zq* and P,Q$\in$ G1,$e(aP,bQ)=e(P,Q)^{ab}$

2. Nondegenerate: There exists a point P such that $E(P,P)\neq 1$.

3. Computable: There is an efficient algorithm to compute e(P,Q) for any P,Q$\in G_1$

3.2 Complexity Assumptions

Definition 1 (q-strong Diffie-Hellman (q-SDH) Assumption [12]). Given (P_1,P2,γP_2,$\gamma 2P2$,….γqqP_2),it is infeasible to compute $1\backslash\gamma + x$

Definition 2 (Decision linear (DL) Assumption [12]). Given P1,P2, P3,aP1, bP2, cP3, it is infeasible to decide whether a+b=c mod q.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent (WBDHE) Assumption [13]). For unknown a Zq* , given

Y,aY,a^2Y ; ::; a^1Y ,P$\in$ G1, it is infeasible to compute $e(Y,P)^{1\backslash a}$

·**Definition 4 ((t,n)-general Diffie-Hellman Exponent**

(GDHE) Assumption [14]). Let f(X)=$\pi^{r}{}_{i=1}$ (X + x_i) and g(X)=$\pi^{n-r}{}_{i=1}$ (X+x_i) be two random univariate polynomials. For unknown k,$\gamma\in$Zq*,given G_0, γG_0,… ,$\gamma t - 1G_0$, $\gamma f(\gamma)$,G_0,P_0,kg(γ)$H_0\in G_1$ and $e(G_0, H_0)^{f2(\gamma)g(\gamma)}\in G_2$.It is infeasible to compute $e(G_0, H_0)^{f2(\gamma)g(\gamma)}\in G_2$.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (133-142), Month: April 2015 – September 2015, Available at: www.paperpublications.org

3.3 Group Signature

Group signature scheme allows group members to sign messages while keeping the identity secret from verifiers. Besides, the designated group admin can reveal the identity of the signature's creator when a malicious activates occurs, which is defined as traceability.

3.4 Tripple DES Encryption Techniques

Triple DES (3DES) is stands for the Triple Data Encryption Algorithm is symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm

The standards define three keying options:

- Keying option 1: All three keys are independent.
- Keying option 2: K_1 and K_2 are independent, and $K_3 = K_1$.
- Keying option 3: All three keys are identical, i.e. $K_1 = K_2 = K_3$.

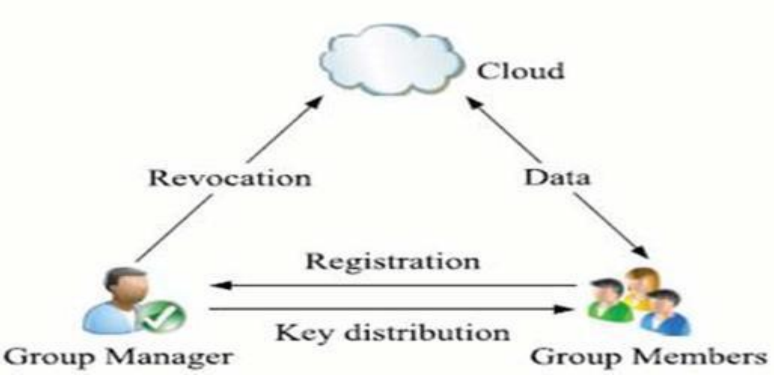
Keying option 1 is the strongest, with 3 × 56 = 168 independent key bits.

Keying option 2 provides less security, with 2 × 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K_1 and K_2, because it protects against meet-in-the-middle attacks.

Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations cancel out.

Each DES key is nominally stored or transmitted as 8 bytes, each of odd parity,[11] so a key bundle requires 24, 16 or 8 bytes, for keying or 3 respectively.

.



Option 1,2

Figure 1: Proposed System Model

4. SYSTEM MODEL AND DESIGN GOALS

4.1 System Model

The system model shown in figure 1 consists three main components of group manager, group member and cloud.

Model Description

1. Cloud

Service is provided by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by cloud end users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to [3], [7], we assume that the cloud server is sincere but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes [17], [18], but will try to learn the content data stored in cloud and the identities of cloud users.

2. Group Manager

Performs following operations

1. Group signature generation
2. User registration
3. Traceability
4. User revocation

In the given example, the group manager is an administrator of the company. Therefore, we assume that the group manager is trusted by the all other employers in the company.

3. Group Member

Group members are registered users can share and store the data in the cloud server also member can modify his/her part of data in cloud. Group members can upload the file and download the file within the group.

4. Group Signature

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

5. Tripple DES Encryption

Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block

Triple DES uses a "key bundle" that consists three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The encryption algorithm is:

ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

I.e., DES encrypt with K_1, DES *decrypt* with K_2, then DES encrypt with K_3.Decryption is the reverse:

plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{ciphertext})))$

I.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.Each triple encryption encrypts one block of 64 bits of data.

6. User Revocation

User revocation is performed by the group manager via public available revocation list based on which group members can encrypt their data files and confidentiality against the revoked users.

4.2 Design Goals

- **Access Control:** The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.
- **Data Confidentiality:** Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.
- **Anonymity and Traceability:** Anonymity guarantees that group members can access the cloud without revealing thereal identity. Although anonymity represents an effective protection for user identity, it also poses a potential

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (133-142), Month: April 2015 – September 2015, Available at: www.paperpublications.org

insideattack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

- **Efficiency:** The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or reencryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

5. PROPOSED SCHEMA

5.1 Overview

To achieve secure data sharing for dynamic groups in the cloud, we expect to combine the group signature and Tripple DES encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the Tripple DES encryption technique allows data owners to securely share their data files with others including new joining users. Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the Tripple DES encryption scheme, which results in that both the computation overhead of the encryption and the size of the ciphertext increase with the number of revoked users. Thus, the heavy overhead and large ciphertext size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this challenging issue, we let the group manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the ciphertext size. Specially, the computation overhead of users for encryption operations and the ciphertext size is constant and independent of the revocation users.

5.2 Scheme Description

This section describes the details of Mona including system initializations, user registration, user revocation, file generation, file deletion, file access and traceability.

5.2.1 System Initialization

The group manager takes charge of system initialization

as follows: Generating a bilinear map group system S=(q,G1,G2,e(.,.)).the system parameters include(S,P,H,H0,H 1,H2,U,V,W,Y,Z,f,f1,Enc()), where f is a one way hash function:{0,1}*->Z*q;f1 is hash function:{0,1}*->G1;and Enck() is a secure symmetric encryption algorithm with the secret key k.

5.2.2 User registration

For the registration of user I with identity IDi, the group manager randomly selects a number xi belong to Z*q and computes Ai, Bi as the following equation:

$$\begin{cases} A_i = \dfrac{1}{\gamma + x_i} \cdot P \in G_1 \\ B_i = \dfrac{x_i}{\gamma + x_i} \cdot G \in G_1. \end{cases}$$

Then, the group manager adds (Ai, xi, IDi) into the group user list, which will be used in the traceability phase.
After the registration, user i obtains a private key (xi, Ai, Bi) which will be used for group signature generation and file decryption.

5.2.3 Revocation list

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

Table 1. Revocation list

IDgroup	D1	y1	t1	P1			
	D2	y2	t2	P2			
	.	.	.	.			
	Dr	yr	tr	Pr	Wr	tRL	sig(RL)

The revocation list is characterized by a series of time stamps t1,t2,…tr. In the proposed system once the user time stamp over does not wait for the group manager to update the time stamp or revocation list here once the time over the user immediately send request for extra time for access the data to the cloud. Then the cloud will send that request to the group manager once the see it and give permission then the cloud will time to access the data but if the group manager did not give permission then the cloud will not give permission for access if the data

5.2.4 File Generation

To store and share a data file in the cloud, a group member performs the following operations: Getting the revocation list from the cloud . In this step, the member sends the group identity IDgroup as a request to the cloud. Then, the cloud responds the revocation list RL to the member. Verifying the validity of the received revocation list. First, checking whether the marked date is fresh. Second, verifying the contained signature sig(RL) by the equation e(W, f1 (RL)) = e(P, sig(RL)). If the revocation list is invalid, the data owner stops this scheme. Encrypting the data file M. Selecting a random number T and computing fT. The hash value will be used for data file deletion operation. In addition, the data owner adds (IDdata, T) into his local storage. Constructing the uploaded data file as shown in Table 2, where tdata denotes the current time on the member, and a group signature on (IDdata, C1, C2, C, f(T); tdata) computed by the data owner through private key (A, x).

Table 2: Message Format

Group ID	Data ID	ciphertext	hash	Time	Signature
ID_{group}	ID_{data}	C_1, C_2, C	$f(\tau)$	t_{data}	σ

Uploading the data shown in Table 2 into the cloud server and adding the IDdata into the local shared data list maintained by the manager. On receiving the data, the cloud first check its validity. If the algorithm returns true, the group signature is valid; otherwise, the cloud abandons the data. In addition, if several users have been revoked by the group manager, the cloud also performs revocation verification. Finally, the data file will be stored in the cloud after successful group signature and revocation verifications.

5.2.5 File Deletion

The file stored in the cloud can be deleted by either the group manager or the data owner .To delete a file ID data, the group manager computes a signature and sends the signature along with ID data to the cloud.

6. PERFORMANCE EVALUTAION

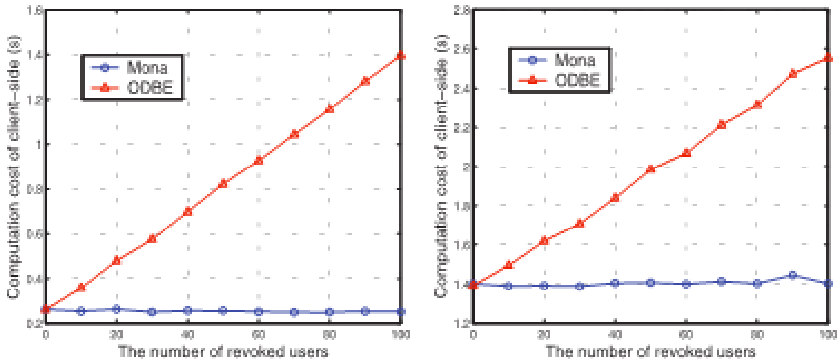
6.1 Storage

Without loss of generality, we set q=160 and the elements in G1 and G2 to be 161 and 1,024 bit, respectively. In addition, we assume the size of the data identity is 16 bits, which yield a group capacity of 216 data files. Similarly, the size of user and group identity are also set as 16 bits.

Group Manager: In Mona, the master private key of the group manager is $(G,\gamma,\varepsilon1,\varepsilon2)\in G1\times Z^{q}_{3}$. Additionally, the user list and the shared data list should be stored at the group manager. Considering an actual system with 200 users and assuming that each user share 50 files in average, the total storage of the group manager is $(80.125+42.125*200+2*10{,}000)*10^{-3}\approx 28.5$ kbytes,which is very acceptable.

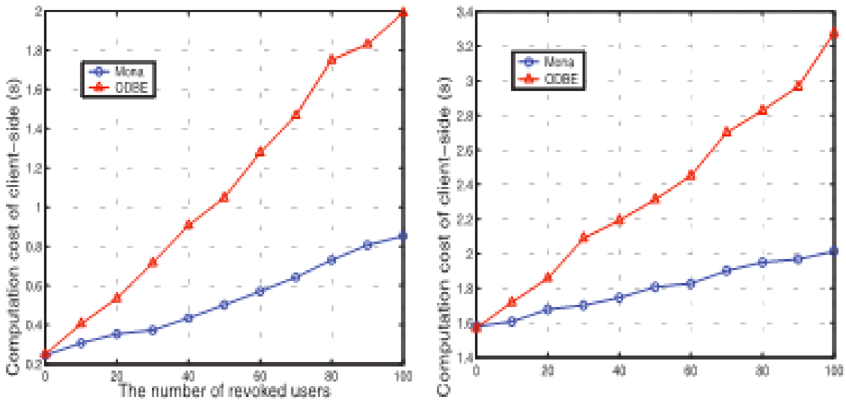
Group Members: Essentially, each user in our scheme only needs to store its private key (A_i , B_i,x_i) is about 60 bytes. It is worth noting that there is a tradeoff between the storage and the computation overhead. For example, the four pairing operations including (e(H,W),e(H,P),e(P,P),e(A_i,P))€$G^4{}_2$ can be precomputed once and stored for the group signature generation and verification. Therefore, the total storage of each users is about 572 bytes.

The extra storage overhead in the cloud: In Mona, the format of files stored in the cloud is shown in Table 2. Since C3 is the ciphertext of the file under the symmetrical encryption, the extra storage overhead to store the file is about 248 bytes, which includes (ID_{group}, ID_{data}, C1, C2, C3, f (τ),d_{ata},σ).



(a) Generating a 10 MB file (b) Generating a 100 MB file

Figure 3: comparison on computation cost for file generation between Mona and ODBE [14]



(a) Accessing a 10 MB file (b) Accessing a 100 MB file

Figure 4: comparison on computation cost for the file access between Mona and ODBE [14]

6.2 Simulation

The simulation consists of three components: clientside, manager side as well as cloud side. Both client side and manager side process are conducted on laptop with core 2T7250 2.0Ghz processor,DDR2 800 2G,ubuntu 10.04X86.The cloud side process is implemented on machine that equipped with core 2 i3-2350 2.3 GHz,DDR3 1066 2G,Ubuntu 12.04X64.In the simulation ,we choose an elliptic curve with 160 bit group order ,which provides a competitive security level with 1024bit RSA.

6.2.1 Client Computation Cost

In Fig. 3, we list the comparison on computation cost of clients for data generation operations between Mona and the way that directly using the original Tripple DES encryption (ODBE) [14]. It is easily observed that the computation cost in Mona is irrelevant to the number of revoked users. On the contrary, the computation cost increases with the number of revoked users in ODBE. The reason is that the parameters ($P_r Z_r$) can be obtained from the revocation list without sacrificing the security in Mona, while several time-consuming operations including point multiplications in G1 and exponentiations in G2 have to be performed by clients to compute the parameters in ODBE. From Figs. 3a and 3b, we can find out that sharing a 10 Mbyte file and a 100-Mbyte one, cost a client about 0.2 and 1.4 seconds in our scheme, respectively, this implies that the symmetrical encryption operation domains the computation cost when the file is large. The computation cost of clients for file access operation with the size of 10 and 100 Mbytes are illustrated in Fig. 4. The computation cost in Mona increases with the number of revoked users, as clients require to perform Algorithms 3and 4 to compute the parameter Ar,r and check whether the data owner is a revoked user. Besides the above operations, P1, P2, Pr needs to be computed by clients in ODBE. Therefore, Mona is still superior to ODBE in terms of computation cost. Similar to the data generation operation, the total computation cost is mainly determined by the symmetrical decryption operation if the accessed file is large, which can be verified from Figs. 4a and 4b. In addition, the file deletion for clients is about 0.075 seconds, because it only costs a group signature on a message (IDdata,τ)where _ is a 160-bit number in Zq^*.

6.2.2 Cloud Computation Cost

To evaluate the performance of the cloud in Mona, we test its computation cost to respond various client operation requests including file generation, file access, and file deletion. Assuming the sizes of requested files are 100 and 10 MB, the test results are given in Table 3. It can be seen that the computation cost of the cloud is deemed acceptable, even when the number of revoked users is large. This is because the cloud only involves group signature and revocation verifications to ensure the validity of the requestor for all operations. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations, since the size of signed message is constant.

Table 3 computation cost of the cloud (s)

Request	The number of revoked users		
	0	50	100
File generation (100 MB)	0.065	0.154	0.271
File generation (10 MB)	0.045	0.125	0.226
File access (100 MB)	0.045	0.150	0.237
File access (10 MB)	0.045	0.151	0.240
File deletion (100 MB)	0.041	0.153	0.240
File deletion (10 MB)	0.042	0.156	0.238

7. CONCLUSION

In this paper we design a secure data sharing scheme for dynamic groups, Where users can share data anonymously without showing the real identity, so privacy is preserved, And using group signature and Tripple DES encryption it provides access control and security for the data in dynamic group Additionally, this technique supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved 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. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, “Mona: Secure Multi-attorney Data Sharing for Dynamic Groups in the Cloud”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. Int’l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (133-142), Month: April 2015 – September 2015, Available at: www.paperpublications.org

[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131- 145, 2003.

[5] B. 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.

[6] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute- Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[8] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001. [12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[12] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[13] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Tripple DES encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[14] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[15] Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

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

[17] Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[18] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 46- 50, 2008.

[19] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001

Author's Profile:

VIJAYA KUMAR PATIL C completed the bachelor's degree in Computer Science &Engineering from visvesvaraya technological University (VTU). Currently pursuing Masters in Engineering in Computer Network & Engineering at Mangalore Institute of Technology, Mangalore.

MANJNATH H completed bachelors and masters degree in Computer Science and Engineering. Currently working as Associate Professor-I and Head of Information Science and Engg in Mangalore Institute of Technology, Mangalore. Currently he is pursuing his PhD in the area of Cloud Computing. He is also member of BOE of CSE Department of NMAMIT and 20years of experience in Teaching and Industrial experience.