International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Dynamic Secure Group Sharing in Cloud Computing

Shobha D. Patil[1], Dr. Sulochana B. Sonkamble[2]

[1]P.G Student, Computer Engineering Department, JSPM, NTC, RSSOER, Narhe, Savitribai Phule Pune University Pune, India

[2]Head of Computer Engineering Department, JSPM, NTC, RSSOER, Narhe, Savitribai Phule Pune University Pune, India

Abstract: ***Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data. The basic service provided by the Cloud is Data Storage. However, it is a difficult task for sharing data in multi-owner manner where group admin and all group members can store and modify data while preserving data and identity privacy from an untrusted cloud server, due to the frequent change of the membership. Therefore secure multi-owner data sharing scheme for dynamic groups in the cloud computing have been proposed which involve integration of group signature and broadcast encryption techniques. But this system also identified some limitations in terms of efficiency and security. Because multi-owner data storing and sharing in a dynamic environment dumps huge amount of data files in the cloud, which remains in cloud for indefinite period of time. The sensitive information stored may misused by service providers. To maintain cloud file's security and privacy regular removal of unwanted files is needed. To resolve this drawback we propose new framework for MONA that remove unwanted files automatically when the predefined time period for sharing specified by data owner has been expired which improve performance of the system in terms of security and efficiency. Also this mechanism reduces the overhead during upload and download file in the cloud. Finally proposed method MODOC claims required efficiency and most importantly security. We implement a working prototype of the MODOC methodology and evaluate its performance based on the time consumed during various operations The results show that MODOC has the potential to be effectively used for secure data sharing in the cloud.***

Keywords: Dynamic group, group signature, dynamic broadcast encryption, data sharing, privacy-preserving.

1. Introduction

Cloud computing based solutions are becoming popular and adopted widely because of its low-maintenance and commercial characteristics. With the help of powerful data centers it is possible for cloud service providers (CSP) to convey various services to cloud users on demand. The Cloud server generally store data in very lower cost and makes it available for 24 hour's over the internet Cloud [5]. For e.g. Company permitted its staffs in the same group or department to store and share records in the cloud. Company saves significant investment on their local infrastructure by utilizing the cloud. But these data application in the cloud storage is abstracted by some security issue such as information leakage because cloud service providers are not completely trusted specially, when highly sensitive and confidential data stored in the cloud such as medical records, business plans. Therefore security and privacy have always been very important concerns in cloud Computing. A basic solution provided by existing system to keep sensitive user data confidential against untrusted server is encrypting the data files, before uploading into the cloud server. But unfortunately designing a secure and efficient cloud data sharing scheme for dynamic groups in the cloud is not simple task because of the some difficult issues.

1.1. Identity Privacy

The major problem for the wide adoption of cloud computing is Identity Privacy. Cloud users may be doubtful to join cloud based computing systems without the assurance of identity privacy because if user privacy is not maintained properly then the actual identities of the user can be disclosed easily to the various kinds of intruders and cloud service providers (CSP).

1.2 No Multiple-Owner Manner

Multiple-owner manner is more flexible than single owner manner because multiple owner manners allow every member in the group should be able to alter their own data i.e. Every member able to not only read the data but also modify his part of data in the entire data file, whereas single owner manner allow only Group Admin to store and modify data in the cloud and members can only read the data.

1.3 Effect of Dynamic Groups

The joining of new staff and revocation of current employee makes the group dynamic in nature. The frequent variations of membership make efficient and secure data sharing in Cloud very complicated and hard due to the following two primary reasons: First, new granted users are not allowed to learn the content of data files stored before their participation by the anonymous system, because it impossible for new granted users to directly contact with data owners and get the corresponding decryption keys. Second, to reduce the complexity of key management it is necessary to obtain an efficient membership revocation mechanism without updating the private keys of the remaining users.

There are several security schemes that have been proposed up-to-date for efficient and secure data sharing on untrusted servers. In all of these approaches, the encrypted data files are stored in untrusted storage and distribute the corresponding decryption keys only to authorized users by the data owners. But, the issues of user revocation and multiple-owner manner have not been addressed very efficiently

2. Objective of the Proposed Work

To solve these issues we propose MODOC, a secure multi-owner data sharing over cloud. The main objective of this paper include

- To implement secure multi-owner data shearing scheme which is able to support dynamic group efficiently. It implies that any group member able to store and share data file by untrusted cloud as well as new user joining and user revocation are easily achieved without involving remaining users.
- To provide secure and privacy-preserving access control to users, this guarantees any member in a group to anonymously utilize the cloud resource. That is group members can access the cloud without revealing the real identity.
- To provide a secure way for key distribution.
- To Improve search efficiency and reduce storage overhead.

3. Literature Review

Literature review is the most important step in software development process. Following is the literature review of some existing technique for data sharing in the cloud.

In 2010 Lan Zhou et al. [2] proposed a scalable and fine-grained data access control scheme by defining access polices based on data attributes and KP-ABE technique. The combination of attribute-based encryption (ABE), proxy re-encryption and lazy re encryption permit the data owner to assign the computation tasks to untrusted server without revealing the necessary contents of data. Data files are encrypted using random key by data owner. Using key policy attribute-based encryption (KP-ABE), the random key is further encrypted with a set of attributes. Then the authorized users are assigned an access structure and corresponding secret key by the Group Admin. Thus, only the user with data file attributes that satisfy the access structure can decrypt a cipher text. This system has some limitation such as multiple-owner manner is not supported by this system so that those single owner manners make it less flexible as only Group Admin are responsible for modifying the data file shared. And user secret key needed to be updated after each revocation.

In 2010 Lu et al. [3] proposed secure provenance scheme which records ownerships and process history of data object. This scheme is based on the bilinear pairing techniques which rely upon group signatures and cipher text-policy attribute based encryption (CP-ABE) techniques. The basic feature of this scheme is to offer the anonymous authentication for user accessing the files, information confidentiality on sensitive documents stored in cloud and tracking the provenance on disputed documents for revealing the identity. Mainly, the system consists of a single attribute. After the registration, each user in this scheme obtains two keys: a group signature key and an attribute key. Using attribute-base encryption (ABE) any user can encrypt a data file. For decryption of the encrypted data, an attribute keys is used by other in the group. To accomplish privacy preserving and traceability features, the user signs encrypted data with group signature key. Unfortunately, the disadvantage of this scheme is that user revocation is not supported.

In 2013 Yong CHENG et al [4] proposed a security for customers to store and share their sensitive data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security and data confidentiality. However, the cryptographic cloud storage still has some shortcomings in its performance. Firstly, it is inefficient for data owner to distribute the symmetric keys one by one, especially when there are a large number of files shared online. Secondly, the access policy revocation is expensive, because data owner has to retrieve the data, and re-encrypt and re-publish it. The first problem can be resolved by using cipher text-policy attribute-based encryption (CP-ABE) algorithm. To optimize the revocation procedure, they present a new efficient revocation scheme. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. Thus, the revocation process is affected by only one slice instead of the whole data.

In 2012 B. Wang et al. [6] focused on cloud computing and storage services, data is not only stored in the cloud, but routinely shared among a large number of users in a group. In this paper, they propose Knox, a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group. In particular, the utilize group signatures to construct homomorphic authenticators, so that a third party auditor (TPA) is able to verify the integrity of shared data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA. The original user can efficiently add new users to the group and disclose the identities of signers on all blocks. With Knox, the amount of information used for verification, as well as the time it takes to audit with it, are not affected by the number of users in the group.

In 2007 C. Delerablee [7] introduces new efficient constructions for public-key broadcast which offer stateless receivers, collusion-secure encryption, and high security. in the standard model; new users can join anytime without implying modification of user decryption keys or permanently revoke any group of users. This system achieve the optimal bound of O(1)-size either for cipher texts or decryption keys, also provides a dynamic broadcast encryption system improving all previous efficiency measures (for both execution time and sizes) in the private-key setting.

In 2013 Xuefeng Liu et al [1] proposed new method "MONA". This method presents the design of secure data sharing scheme for dynamic groups in an untrusted cloud which involve integration of group signature and broadcast encryption techniques. This method support dynamic group i.e. User can be revoked easily through revocation list without updating remaining users as well as new user can decrypt data file without contacting to the data owner. Therefore size and computation costs of encryption are

independent with the number of revoked users. This system identified some limitations in terms of efficiency and security. Also in revocation list the time given for each user is fixed after time expire user cannot access the data until Group Admin update the revocation list and give it to the cloud.

4. Proposed System

The review of literature has revealed that efficient and protective data sharing in cloud computing is still to be a challenging issue.

To solve these issues, we propose a new framework MODOC for secure data sharing in cloud computing by combining group signature and broadcast encryption techniques. In this method we are presenting how to manage risk in securely sharing data among multiple group members. Compared to existing work our proposed system provide some unique features such as

- This system support dynamic group efficiently. It implies that new user joining and user revocation are easily achieved without involving remaining users.
- This system provides rigorous security using encryption technique.
- Provide protection against various attacks at the client side.
- Provide strong security which is necessary to store and maintain confidential data.

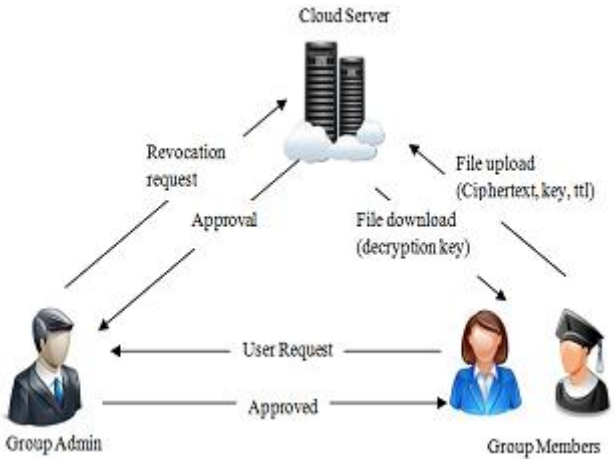

Figure 1: Architecture of cloud data Sharing Scheme

The system model consists of three different entities:

- The cloud server
- A Group Admin (i.e., Admin)
- A large number of group members.

Cloud Server: Cloud is the large repository of resources. Cloud is responsible for storing all user's data and granting access to the file within a group to other group members based on publically available revocation list which is maintained by Group Admin. We assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data, due to the protection of data auditing schemes

Group Admin: The Group Admin is acted by the administrator of the company. Therefore we assume that the Group Admin is fully trusted by the other parties Group Admin perform various operations such as system parameters generation, user registration, group creation, assign group signature, generation of private key using bilinear mapping and assign to the requested user, maintain revocation list and migrate this list into cloud for public use, and traceability.

Group Members: Group members are a collection of registered users that will store their private data into the cloud server and share them with others in the group. Both Group Admin and group member can login using their login details. After successful login, Group Admin activates newly added members of the cloud by generating keys for each member using bilinear mapping and send it to the corresponding group members. He can also check the group details, and assign group signature. After successful login, Group Members signature is verified. After successful verification, the member can upload, download and can modify the files. Group member must be encrypting data files before uploading to the cloud. The Group Members account can be revoked after he leaves the cloud by the Group Admin.

User Registration: After successful creation of cloud setup, users need to get registered with the system through user registration process. While registering, users need to submit their personal details for completion of registration process. User registered with their details such as identity (user name, mobile no and email-id). During registration process, user got unique identity and access structure. This generates secret key for the members. For registered users they will obtain private key, that private key is used file encryption and decryption.

User Authentication: The user can login successfully only if user id and password are entered correctly. The login is a failure if the incorrect user id or wrong password is entered by the user. This helps in preventing unauthorized access.

Key Distribution: Means of distributing secret keys by the Group Admin that is valid only if the group members are not revoked from the group. Key can be updated by generating new key from an old key.

User Revocation: User revocation is the process of removal of user from system user list which is performed by group admin. Group admin can directly revoke multiple users through public revocation list at any time without affecting any non revoked user. If the login credentials of the specified user matches with the details of revocation list then access denied.

File Upload: File upload is the process of storing specified data files into the cloud for sharing in the group. Uploaded files remains in the cloud up to the time specified while uploading the file. Before uploading the file, file has to be encrypted and compressed to ensure security and privacy of the files. Then it is encapsulated with corresponding decryption key and time to live (ttl) value for the file and send it to cloud.

File Download: To access the data that are stored in the cloud, group member will give request as group id, data id. Cloud server will verify their signature, if the group member in the same group then allow to access file. Group member have rights to access data, but not having rights to delete or modify the data that are stored in the cloud.

File Deletion
Since the system itself automatically removes the shared files when time speci fied during upload process will expire. Therefore proposed system does not required explicit deletion mechanisms

5. Mathematical Model

Let S is the main set described below.
MODOC = {S, A, U, F, GH, K, ttl, RL, Ek, SDB }

Where,
S = Start state i.e. Establishing connection between client and cloud server,
A = Group Admin who create group and add members into Group.
U = User called as registered group member.
F = File that user want upload on the cloud server and share within group.
K = Private key of each group members.
GH = Group signature assigned by group admin.
ttl = time to live of the uploaded file.
RL = is the revocation list maintained by group admin.
DE = Encrypted data file.
SDB = is the copy of the server database.
E = End state.i.e User query ran successfully on encrypted database and user get the accurate result in minimum time.

Functionality
A = Create(G, K)
U = Register(uid , password)
RL = RevocationList(GID, MID)
DE = Ek(F)
SDB = StoreData (DE, RL, ttl)

6. Methodology

6.1 Dynamic Broadcast Encryption

The dynamic Broadcast Encryption [7] techniques enabling the group manager to dynamically add new user and at the same time preserves the previously computed information. That is, newly joining users can directly decrypt data files without contacting with data owners. So that there is no need to update user decryption keys.

6.2 Group Signature

Group Signature will be used to achieve privacy of group member against potential verifiers. Group signature scheme allows any group member to issue a signature on behalf of the whole group [10]. Any verifier can publicly check the validity of this group signature using the group public key. The important property of group signatures is that the group manager can open group signatures and identify their signers using the information collected during the admission process when a dispute occurs, which is denoted as traceability. Thus as compare to ordinary digital signatures, group signatures have provide extended security.

7. Result and Discussion

7.1 Security Analysis

Table 1: Security performance comparison

	Secure key distribution	Access control	Secure user revocation	Anti-collusion attack	Data confidentiality
RBAC scheme		√			
Mona	√	√			√
Proposed scheme	√	√	√	√	√

As compared with Mona proposed scheme can achieve secure key distribution, protection from collusion attack and secure user revocation.

7.2 Performance Analysis

We evaluated the MODOC methodology on the basis of the total time consumed to upload and download a file to/from the cloud. The total time is composed of the time from the time of submission of request to the cloud server to the point of time at which the file is uploaded/downloaded to/from the cloud.

Table 2: Comparison of Turnaround Time

File Size (KB)	MONA		MODOC	
	Upload	Download	Upload	Download
148	12.9	11.6	12.4	7.5
520	35.8	40.3	34.3	33.6
876	66.6	68.1	64.6	44.4
1050	80.1	84.6	77.2	50.8
1516	98.8	121.5	81.9	51.5

Table II shows the turnaround times for upload and download. In general, the time to upload and download the data increased with the increase in the file size This table reveal that the MODOC methodology outperforms the existing techniques MONA due to the absence of heavy computations and memory overhead.

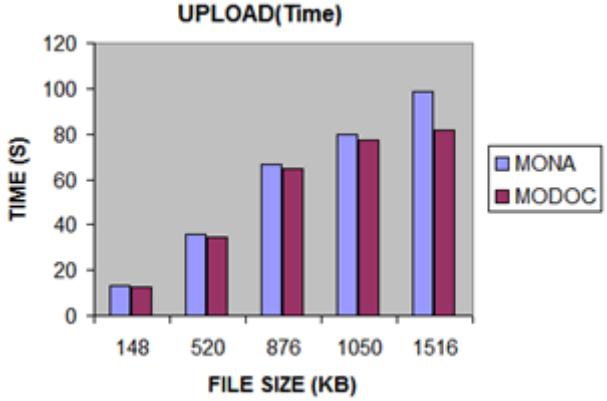

Figure 2: Performance of File Upload.

In Figure 2 show result for upload time. X axis represents the file size Y axis represents the time. In existing system MONA 1.5mb was uploaded in 98.8s, where as in proposed system MODOC it takes 81.9s to upload a 1.5mb file. This graph clearly shows that as compare to the existing system the performance of proposed system is higher.

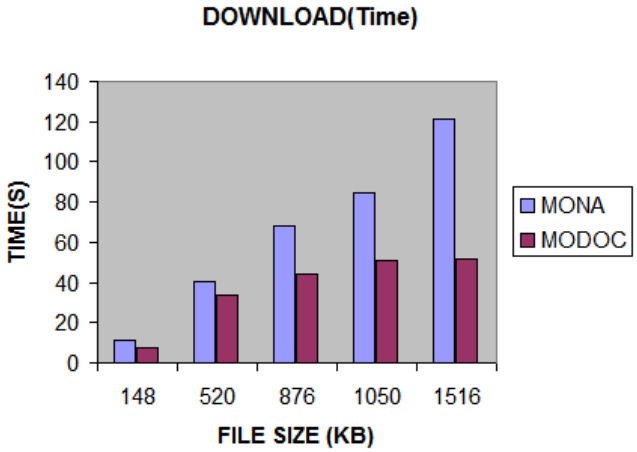

Figure 3: Performance of File Download.

In Figure 3 show result for download time. X axis represents the file size Y axis represents the time. In existing system MONA 1.5mb was downloaded in 121.5s, where as in proposed system MODOC it takes 51.1s to upload a 1.5mb file. This graph clearly shows that as compare to the existing system the performance of proposed system is higher.

8. Conclusion

This paper introduce a cloud data sharing scheme ensuring security for frequent change of membership which involves the combination of group signature and dynamic broadcast encryption techniques. Proposed system supports multiple users to share common data across the members and each member can involve in data dynamics. System introduced in this paper is proficient to provide features like secure and privacy-preserving access control, anonymity and traceability. Also this system provides high security and efficiency by using LFSR technique. Thus proposed system claims required efficiency, scalability and most importantly security.

9. Acknowledgement

I sincerely thanks to Dr. Sulochana. B. Sonkamble for her continuous and constructive support for the work. I would also like to thanks to my friends for their valuable comments.

References

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE Transactions On Parallel and Distributed Systems, Vol.24, No. 6, June 2013.
[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
[3] 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.
[4] Yong CHENG, Jun MA and Zhi-ying "Efficient revocation in cipertext-policy attribute-based encryption based cryptographic cloud storage" Zhejiang University and Springer-Verlag Berlin 2011
[5] 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.
[6] 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.
[7] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.
[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and
[9] Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.
[10] D. Boneh, X. Boyen, and H. Shacham, Short Group Signature, Proc. Intl Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
[11] 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.

Author Profile

Shobha D. Patil received BE degree in computer science and engineering from Shivaji university, Maharashtra, India in 2008. Currently doing ME (Computer Engineering) in JSPM, NTC Savitribai Phule Pune University. Maharashtra, India

Mrs. Sulochana Sonkamble is HOD of Computer Science Department at Rajarshi Shahu College of Engineering and Research, JSPM NTC Pune-India. She obtained Bachelor of Engineering, Masters of Engg. And PhD in Computer Science Shri Guru Gobind Singhji Institute of Engineering and Technology, Swami Ramand Tirth Marathwada University, Vishnupuri, Nanded-India.