ISSN:0975-9646

Survey Paper On Modoc: Multi Owner Data Sharing Over Cloud.

Shobha D. Patil[1], S. B. Sonkamble [2]

[1] *PG Scholar,* [2] *Professors,*

Department Of Computer Engineering, Savitribai Phule Pune University.
Rajarshi Shahu School of Engineering and Research Narhe, Pune-India.

Abstract— **Now a day's Cloud computing is the developing technology, where data owners can remotely store and modify their data on the premise of pay-as-use manner and enjoy on demand high-quality applications. The fundamental service provided by the Cloud is Data Storage that is increasingly more customers are starting to utilize cloud to online data store and share. But because of the frequent change of the membership sharing data in multi-owner manner become a very difficult task. Therefore we propose secure multi owner data sharing for dynamic groups by combining group signature and dynamic broadcast encryption techniques. We also use AES algorithm to improve performance of the system in terms of security. This guarantee any group member can anonymously share the cloud resources.**

Keywords— **Cloud computing, multi-owner manner, group signature, dynamic broadcast encryption, data sharing, privacy-preserving**

I. 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 enters it is possible for cloud service providers (CSP) to convey various services to cloud users on demand. The Cloud server is store data in very lower cost and makes it available for 24 hour's over the internet Cloud. 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. Therefore security and privacy have always been very important concerns in cloud Computing. A basic solution provided by existing system to ensure data privacy and security 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.

A. *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).

B. *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 manager to store and modify data in the cloud and members can only read the data.

C. *Effect of Dynamic Groups:* The joining of new staff and revocation of current employee makes the group dynamic in nature. The frequent alterations 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 anonymous data owners and get the corresponding decryption keys. Second, to reduce the complexity of key management it is desirable to obtain an efficient membership revocation mechanism without updating the secret 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 in these schemes.

Section II will give a brief review of all the concerned reference papers. It will give a brief discussion of the other contributors and their conclusions. Section III. Discuss the proposed system. Finally, section IV. Concludes this paper by summarizing the key points and other related considerations.

II. LITERATURE SURVEY

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

A. Plutus: Scalable Secure File Sharing on Untrusted Storage.

M. Kallahalla et al. [2] proposed cryptographic storage system which is known as Plutus. Plutus enables secure file sharing on untrusted server by using client based key distribution. Plutus allow client to handle all the key management and distribution operations. As compare to client, Server incurs very little cryptographic overhead because Plutus does not place much trust on server, it eliminate almost all requirement of server trust. Plutus divide files into filegroups and enable data owner to share the filegroups with others by encrypting each filegroup with unique file-block key that can protect data. There are some limitation identified in the Plutus such as a) A heavy key distribution overhead for large-scale file sharing. b) The file block key needs to be updated and distributed again for a user revocation. Thus Plutus provides end-to-end security for group sharing system with lazy revocation

B. Sirius: Securing Remote Untrusted Storage.

E. Goh et al. [3] proposed a SiRiUS, Securing Remote Untrusted Storage**.** A SiRiUS is designed to handle secure multi user file system over insecure network using cryptographic operations. SiRiUS implement cryptographic read-write access control for file sharing without use of a block server. Also it is possible for SiRiUS to implement large scale group sharing using the NNL key revocation construction. Key management and revocation is simple with minimal out-of-band communication. SiRiUS provides secure NFS without changing the file server. SiRiUS has some limitation in case of user revocation and dynamic groups. The user revocation is difficult for large scale sharing. Private key of every group member must be updated while joining of new user in the group.

C. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage.

Ateniese et al. [4] proposed proxy re-encryptions method to add the access control to the secure file system and distributed storage. Blocks of content are encrypted with unique and symmetric content keys by the data owner. The resulting encrypted content keys are further encrypted under a master public key. Additionally, to grant a user's public key, the appropriate content keys from the master public key is directly re-encrypt using proxy cryptography which helps in maintaining the access control and improvement of security. To supervise access to encrypted content stored on distributed untrusted replicas, this scheme makes use of centralized access control server. The main benefits of this scheme are that they are unidirectional and only a limited amount of trust is placed in the proxy. However, a collusion attack can occur between any revoked malicious user and untrusted server allowing them to find out the decryption keys of all the encrypted blocks of content.

D. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing.

Yu et al. [5] offered 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 manager. 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 manager are responsible for modifying the data file shared. And user secret key needed to be updated after each revocation.

E. Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing.

Lu et al. [6] propose 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.

F. Efficient Revocation in CP-ABE Based Cryptographic Cloud Storage.

Yong CHENG [7] proposed a security for customers to store and shares 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.

G. Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud

B. Wang et al. [8] 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.

H. Short Group Signature.

In [9] Dan Boneh, construct a short group signature scheme with length under 200 bytes where the signatures are nearly the standard RSA signature size with the same level of security. Group signature security of this proposed scheme is based on the Strong Diffie-Hellman (SDH) assumption and a new assumption in bilinear groups called the Decision Linear assumption. This system stands on a new Zero-Knowledge Proof of Knowledge (ZKPK) of the solution to an SDH problem where ZKPK is converted to a group signature via the Fiat-Shamir heuristic.

I. Broadcast Encryption.

In [10] Fiat et al. proposed schemes that offers efficient solutions in terms of both transmission length and storage at the user’s end. It introduces new theoretical measures for thoue qualitative and quantitative assessment of encryption schemes designed for broadcasting secure transmissions to an arbitrary set of recipients while minimizing key management related transmissions. The broadcast encryption scheme transmits message securely to all members of the privileged subset. The new parameter added in this scheme represents the number of users that have to collude so as to break the scheme. The scheme is considered broken if a user that does not belong to the privileged class can read the transmission. It also consider another scheme parameter called random-resiliency that refers to the predictable number of users, selected uniformly at random, that have to collide so as to break the scheme.

J. Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Cipher texts or Decryption Keys.

In [11] C. Delerablee 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.

III. Proposed System

Researchers have proposed many methods for protective data sharing in cloud computing, although most methods failed to achieve the efficient as well as secure method for data sharing for groups. 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. Therefore the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively [1].

To overcome these problems, we design secure data sharing scheme for dynamic groups in an untrusted cloud 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 using key regenration techniques. Compared to existing work our proposed system provide some unique features such as

a) Any group member able to store and share data files with others within a group.
b) This system support dynamic group efficiently. It implies that new user joining and user revocation are easily achieved without involving remaining users.
c) This system provides rigorous security using AES encryption technique.

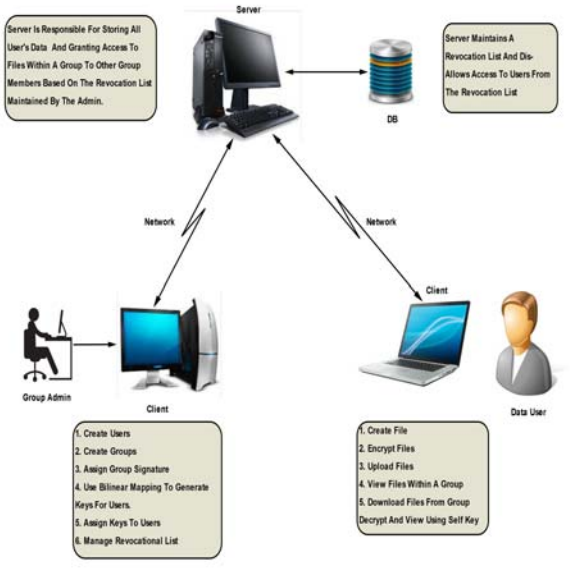
Server Is Responsible For Storing All User's Data And Granting Access To Files Within A Group To Other Group Members Based On The Revocation List Maintained By The Admin.
Server
DB
Server Maintains A Revocation List And Dis-Allows Access To Users From The Revocation List
Network
Network
Client
Group Admin
Client
Data User
1. Create Users
2. Create Groups
3. Assign Group Signature
4. Use Bilinear Mapping To Generate Keys For Users.
5. Assign Keys To Users
6. Manage Revocational List
1. Create File
2. Encrypt Files
3. Upload Files
4. View Files Within A Group
5. Download Files From Group
Decrypt And View Using Self Key

Fig-1 Architecture of cloud data Sharing Scheme.

The system model consists of three different entities:

- The cloud server
- A group manager (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 manager. We assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data, but will try to learn the content of the stored data.

Group Manager: The group manager is acted by the administrator of the company. Therefore we assume that the group manager is fully trusted by the other parties Group manager 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.

IV. CONCLUSION

This paper introduce a cloud data sharing scheme ensuring security for frequent change of membership which involves the integration of group signature and dynamic broadcast encryption techniques. The proposed system is proficient of allowing cloud user in the group to share and store data securely and makes use of resources with others without disclosing real identity and user privacy to the cloud. Moreover, the system proposed in this paper supports dynamic group efficiently, provide features like secure and privacy-preserving access control, anonymity and traceability property for revealing the identity when dispute occurs between the cloud users. The proposed scheme supports multiple read and writes on the content of data stored along with data created by data owner which helps from different malicious attack. Furthermore, the storage overhead and encryption computation cost remains constant with the number of revoked user.

ACKNOWLEDGEMENT

I sincerely thanks to prof. S. 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. M. Kallahalla, E. Riedel, R. Swami Nathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
3. 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
4. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005
5. 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.
6. 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
7. 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 2013.
8. 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
9. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.
10. A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.
11. 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.