ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Review on Secure Data Sharing for Frequently Changing Groups in Cloud

Pooja R.Bangad[1], Bapusaheb B.Bhusare[2]

PG Student, Dept. of CSE, MSS'S College of Engineering & Technology, Jalna, India[1]

Assistant Professor, Dept. of CSE, MSS'S College of Engineering & Technology, Jalna, India[2]

Abstract: Cloud computingrelies on sharing of resources to achieve coherence and economies of scale. Cloud resources are shared & owned by multiple users. Security of shared data in multi owner manner is an important and critical aspect due to frequent change of membership. To provide anonymous sharing of data between cloud users group signature & broadcast encryption techniques are used. To provide secure access to accounts one time password technique is used. Security of shared data in multi owner manner is increased by providing authentication at multiple levels. To handle the failure of group admin due to large user requests, it supports to increasing the number of backup group admin, which also improves reliability & scalability.

Keywords: Cloud computing, dynamic groups, reliability, scalability.

I. INTRODUCTION

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing is defined as a type of computing that relies on sharing computing resources rather than having local servers to handle applications. Cloud storage means "the storage of data online in the cloud," wherein a company's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud.

Cloud computing provider can result in significant cost savings and more streamlined, flexible operations, but mixed in with these opportunities are numerous security challenges that need to be considered and addressed prior to committing to a cloud computing strategy. The main cloud computing security challenges are data protection & user authentication. To provide the data protection data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. The Following challenges are there to design a secure data sharing scheme for groups in the cloud.

First Identity privacy, it ensures that the real identities of users will not be disclosed to cloud providers or attackers. Identity privacy should be provided to cloud users. Important thing traceability is also highly desirable, which enables the group manager (e.g., a Company manager) to reveal the real identity of a user.

Second, Challenging issue is multi owner compared with single owner manner where only group manager have data storing & updating access.But in particle applications it is recommended each group member have right to store & share data, called as multi-owner manner.

Another important problem is frequently changing memberships in the group. New members are continuously added to the group & user revocation is also there. This type of dynamic groups is difficult to manage. New granted users should have access to data files stored before their participation, because it is not possible to contact with the multiple owners of the file to obtain decryption Keys. On the other hand, membership revocation should not affect the decryption keys of remaining users.

To solve the challenges presented above, we propose a secure multi-owner data sharing scheme for dynamic groups in the cloud. To provide more security in dynamic groups we use multiple level of authentication. Only text based passwords are not enough to provide higher level of security. To provide higher level of security we are introducing Image based authentication, which provides security at three levels.

Level 1: Security at level 1 has been imposed by simple text -based password.
Level 2: Security is imposed by using image based authentication (IBA) at this level
Level 3: After the successful clearance of the above two levels, the Level 3 Security System will then generate a one-time numeric password (OTP).

As per reliability and scalability concern this method needs to be workout further as if the group manager stop working due to large number of requests coming from different groups of owners, then entire security system failed down. To avoid this failure we are introducing the concept of increasing the number of Group manager i.e. Backup Group Admin.

II. RELATED WORK

A. Broadcast Encryption

A. Fiat A. Fiatet al. [2] proposed a system on multicast communication frame work, various types of security threat occurs.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Broadcast Encryption: In this paradigm, a broadcaster encrypts messages and transmits these to a group of users who are listening to a broadcast channel and use their private keys to decrypt transmissions. The broadcaster may exclude any subset of users from being able to decrypt the contents of the broadcast thanks to a one-time exclusion or revocation mechanism. The subset of revoked users R is chosen at encryption time and may change from one encryption to the next.

B. Cryptographic Cloud Storage

S. Kamara et al. [3] 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. The revocation operation is a sure performance killer in the cryptographic access control system. To optimize the revocation procedure, they present a new efficient revocation scheme which is efficient, secure, and unassisted. 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 accelerated by affecting only one slice instead of the whole data.

C. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data

V. Goyal [4] as more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e. giving another party your private key).They develop a new cryptosystem for Fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

D. Revocation and Tracing Schemes for Stateless Receivers

D. Naor [5] has introduced, now a days there is problem of a sending a message to a group of users such that some subset of the users is considered revoked and should not be able to obtain the content of the message. Here theyconcentrate on the stateless receiver case, where the users do not (necessarily) update their state from session to session. In this paper a framework called the Subset-Cover framework is provided, which abstracts a variety of revocation schemes including some previously known ones. It provides a sufficient condition that guarantees the security of a revocation algorithm in this class. Two explicit Subset-Cover revocation algorithms are introduced; these algorithms are very flexible andwork for any number of revoked users. The main improvements of these methods over previously suggested methods, when adopted to the stateless scenario, are: First reducing the message length to regardless of the coalition size while maintaining a single decryption at the user's end and Second, it provide a seamless integration between the revocation and tracing so that the tracing mechanisms does not require any change to the revocation algorithm [5].

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

C. Delerablee[6] proposed Dynamic broadcast encryption: A basic property very much desired in broad-cast encryption (and other group-based protocols) is that the group should be dynamic in the sense that the group manager can invite new members to join or permanently revoke undesired members in a very efficient way. Although long- term revocation necessarily implies a modification of the keys, there is no such theoretical requirement when a new member joins the group. In this respect, a broadcast system is dynamic when the system setups as well as the cipher text size are fully independent from the expected number of users or an upper bound. A new user can join anytime without implying a modification of preexisting user decryption keys, Hence, by definition; dynamic systems support arbitrarily many users.

F. Ensuring Data Storage Security in Cloud Computing

C.Wang et al. [7] proposed a system to ensure the integrity of data storage in Cloud Computing. In particular, here consideration is the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing.

G. SiRiUS: Securing Remote Untrusted Storage

SiRiUS [8] assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. Here implementation of SiRiUS performs well relative to the underlying file system despite using cryptographic operations.

H. Decentralized Dynamic Broadcast Encryption

Broadcast encryption system [9] generally involves three kinds of entities: the group manager that deals with the membership, the encryptor that encrypts the data to the registered users according to a specific policy (the target set), and the users that decrypt the data if they are authorized by the policy. Public-key broadcast encryption can be seen as removing this special role of encryptor, by allowing anybody to send encrypted data. In this paper, a step further in the decentralization process, by removing

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

the group manager: the initial setup of the group, as well as the addition of further members to the system, does not require any central authority. The construction makes black-box use of well-known primitives and can be considered as an extension to the subset-cover framework.

It allows for efficient concrete instantiations, with parameter sizes that match those of the subset-cover constructions, while at the same time achieving the highest security level in the standard model under the DDH assumption.

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

S. Yu et al .[10] focused on many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users.

The problem of simultaneously achieving fine-graininess, scalability, and data confidentiality of access control actually still remains unresolved. Here goal is achieved by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. They proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability.

III. PROBLEM DEFINITION

To achieve secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the un-trusted cloud. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved without updating thesecret keys of the remaining users.

IV. OBJECTIVES

We define the main objective of the system as follows

- Group Members should be able to fully enjoy the cloud resources & services.
- Unauthorized users should be incapable of using the cloud resources & content of the stored data.
- Any group member can store and share data files with others in the group by the cloud.
- After revocation, revoked user should not have access to cloud resources & content of stored data.
- New users should be able to decrypt the data stored in the cloud before their participation without contacting with the data owner.
- User revocation should not affect the membership of remaining unrevoked users.
- Group members can access the cloud without revealing their real identity.
- To tackle the inside attacks, group manager should have right to reveal the identities of users.

V. PROPOSED MODEL

We combine the following techniques to provide secure multi owner data sharing scheme for dynamic groups.

- Group Signature mechanism
- Dynamic Broadcast Encryption
- Image Based Authentication
- Backup Group Admin

A. Group Signature

To provide security & authenticity the concept of group signature is introduced to the system. After the group creation, to provide security group signature has to be perform by users. A group user can sign the message without revealing their own identities. But whenever dispute occurs group manager can trace the person by revealing the identity of the group member. Even if the user wants to revoke from the group only his identity is disabled in the group, which does not affect the membership of remaining group users.

A new type of signature for a group of persons, called a group signature is described in which states the following properties:

- Only members of the group can sign messages.
- The receiver can verify that it is a valid group signature, but cannot discover which group member made it.
- If necessary, the signature can be "opened"(with or without the help of the group members), so that the person who signed the message is revealed.

B. Dynamic Broadcast Encryption (DBE)

For the security of data, the file is encrypted each time & then stored on the cloud. Broadcast encryption system, where there is broadcaster sends the encrypted data to set of users. This are authenticated users who can decrypt the files. Due to frequent change in membership group manager should be able to include users dynamically which is called as dynamic broadcast encryption system. The size and computation overhead of encryption are constant and independent with the number of revoked users. User decryption keys, size of cipher texts & group encryption keys requires no modification on addition & revocation of users.

C. Scheme Description

i. Group Admin or group owner

The group admin is fully trusted person of the group.

The group admin or owner can perform the following operations on group of users, data and cloud:

- Group Creation: Groups are creating by admin.
- User Registration: For the registration of user I with Identity IDi, the group manager randomly selects a number and characters for generate random key. Then, the group
- Revoke User: Theadmin can only have permission for revoke user and remove revocation. The group manger update the revocation list each day even no user has being revoked in the day.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

- File Deletion: File stored in the cloud can be deleted by either the group manager or the data owner (i.e., the member who uploaded the file into the server).

ii. User or Group Member Set of registered users is called as Group users. Who store & share their private data with other members in the group.

- File Generation & Uploading: After verifying with the current revocation list & group signature by group admin, user uses his private key to encrypt data. File is generated & uploaded file on to the cloud. Acknowledgment is provided by cloud upon receiving of encrypted file.

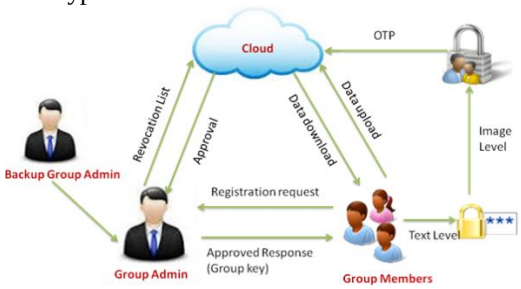

Fig.1 Proposed System Model

- File Download: To learn the content of a shared file, a member sends request to the cloud upon checking the validity of revocation list& verification of group signature Cloud provides the encrypted file. After receiving the file user verifies the validity of the file & decrypt it.
- File Update: Stored file can be updated by any group member. User has to send a signed request to the cloud. After verifying the current time stamp, signature & revocation list cloud provide the file to the respective user. User can make changes to that file & upload it onto the cloud.

D.Image Based Authentication

Different Access control mechanisms are used to secure the resources against unauthorized users. Only text based passwords are not enough to provide the higher security. After Image authentication, user will obtain the one time password (OTP), using the instant messaging services. This OTP then can be used by user to access their personal accounts. In this paper one time password & Image based authentication are used to achieve high level of security in authenticating the user over the Internet.

The main Objective of 3 Level Security system is to provide extremely secured system, employing 3 levels of security.

Level 1: Group member has to first enter the text based password.

Level 2: After text authentication image based authentication (IBA) is performed, in which user has to select three images from the respective grid of images. These images are preselected images by the user.

Level 3: The next level of Security is System will generate a numeric one-time password that would be valid just for one login session. The password will be sent via an email to the authentic users.

Advantage

The image based authentication method relies on the user's ability to recognize pre-chosen categories from a grid of pictures. This helps to eliminate tempest attack, shoulder attack. OTPs are difficult for human beings to memorize. The OTP's are valid for only that session so other people will not be able to use it again.

E. Backup Group admin

The system should be reliable at any type of possible failure. It may happens due to large number of upcoming user requests group admin may get hang, which turns into failure of entire system. Failure of group admin can be handled by sharing the workload in multiple group managers. In this paper idea is to increase the number of group admin. In case of failure of group admin all group members will request to backup group admin. Even if the failure of group admin backup group admin will be there to handle the requests from users. This method claims required efficiency, scalability and most importantly reliability.

REFERENCES

[1]. Xuefeng Liu, Yuqing Zhang, Member, IEEE, 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]. A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

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

[4]. 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.

[5]. 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.

[6]. 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.

[7]. C. 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.

[8]. 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.

[9]. Duong Hieu Phan , David Pointcheval , and Mario Strefler " Decentralized Dynamic Broadcast Encryption" 5 – 7 september 2012, Amalfi, Italy

[10]. 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.

BIOGRAPHIES

Pooja Ban gad received the B.E. degree in Computer Science and Engineering from Dr. Babasaheb Ambedkar Marathwada University. Now doing PG in Computer Science and Engineering

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

from Matsyodari Shikshan Sanstha's College of Engineering and Technology, Jalna, Maharashtra, India

Bapusaheb B. Bhusare received his M.E. degree in Computer Science and Engineering from GovernmentCollege of Engineering, Aurangabad. Working as Assistant Professor in CSE Department. Since last 5 years at MSS's College of Engineering and Technology, Jalna, Maharashtra, India.