International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Secure Multi-Owner Data Sharing for Dynamic Groups through Fine Grained Access Control in Cloud Computing

Pushpa Latha[1]& Harini.Lebaku[2]

[1]Associate Professor,Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana
[2]M.Tech CSE (PG Scholar),Dept of CSE, Marri Laxman Reddy Institute Of Technology & Management, Hyderabad, Telangana

ABSTRACT

A cloud computing paradigm dynamically assigns, configures, relocates and de provisions these computing resources as needed. it also describes applications that are to be extended accessible through the Internet. Data security and availability management is one of the most complex ongoing studies in cloud managing, because of clients outsourcing their sensitive details to cloud service providers. Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users confidential against un trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. One of the biggest concerns with cloud data storage is that of data integrity verification at un trusted servers. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. To resolve this problem recently the best efficient method MONA presented for secured multi owner data sharing in however we identified some limitations in the same approach in terms of reliability and scalability. Hence in this paper we are further extending the basic MONA by adding the reliability as well as improving the scalability by increasing the number of group managers dynamically.

Index Terms— Cloud Computing; dynamic groups; data sharing; reliability; integrity; scalability

I.INTRODUCTION

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. Cloud computing is one of the greatest platform which provides storage of data in very lower cost and available for all time over the internet Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and devices on demand. Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. Cloud Computing means more than simply saving on IT implementation costs. One of the most fundamental services offered by cloud providers is data storage [1].

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

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. Cloud offers enormous opportunity for new innovation, and even disruption of entire industries. Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on demand high-quality applications and services from a shared pool of configurable computing resources. 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 providers and attackers [2]. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Maintaining the integrity of data plays a vital role in the establishment of trust between data subject and service provider. Although envisioned as a promising service platform for the Internet, the new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at un trusted servers. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client [3]. CS2 provides security against the cloud provider, clients are still able not only to efficiently access their data through a search interface but also to add and delete files securely. Several security schemes for data sharing on un trusted servers have been proposed secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second [4], in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. Cloud computing is recognized as an alternative to traditional information technology 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 [5].

One of the most fundamental 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 [6, 7]. 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

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

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 providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable [8]. 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 fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner, where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult [9]. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management [10].

As we know sharing data only by manager in a single owner manner is not flexible so we use multi-owner manner. In our project ,we mainly concerned that the secret key is not generated again and again whenever there is a revocation, We are using a revocation list which the names of the revoked members. It is helpful in a way that whenever a revoked member tries to log in or uploading files, he is not able to do these works. This is helpful in user identity proof. Now we deal with data security, only authorized member can view or upload data and there is group signature key which distributed only to the existing members of the group, it is a combination of private key of member and group key of group and private key is generated each time whenever a new member is added to group. Using group signature key, a member is able to upload or view a uploaded file. Data owners store the encrypted data files in un trusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

II. LITERATURE SURVEY

A. Cryptographic Cloud Storage: S. Kamara et al. 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. HoIver, 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. They have applied the efficient revocation scheme to the cipher text-policy attribute-based encryption based cryptographic cloud storage. The security analysis shows that the scheme is computationally secure.

B. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing : S. Yu et al.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 un trusted 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. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to un trusted cloud servers without disclosing the underlying data contents. They achieve this goal 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 [11].

C. Cipher text-Policy Attribute-Based Encryption: an Expressive, Efficient, and Provably Secure Realization: B. Waters et al.[16] proposed the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an un trusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, they propose a secure multi- owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, they analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

D. Sirius: Securing Remote Un trusted Storage : E. Goh et al.[7] presented a SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. SiRiUS assumes the network storage is un trusted 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. Our implementation of SiRiUS performs Ill relative to the underlying file system despite using cryptographic operations. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Using cryptographic operations implementation of Sirius also possible. It only uses the own read write cryptographic access control. File

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

level sharing are only done by using cryptographic access [12].

E. Broadcast Encryption: A.Fiat et al. proposed a system on multicast communication framework, various types of security threat occurs. As a result construction of secure group communication that protects users from intrusion and eavesdropping are very important. In this paper, they propose an efficient key distribution method for a secure group communication over multicast communication framework. In this method, they use IP multicast mechanism to shortest rekeying time to minimize adverse effect on communication. In addition, they introduce proxy mechanism for replies from group members to the group manager to reduce traffic generated by rekeying. They define a new type of batching technique for rekeying in which new key is generated for both leaving and joining member. The rekeying assumption waits for 30 sec so that number time's key generation will be reduced [9].

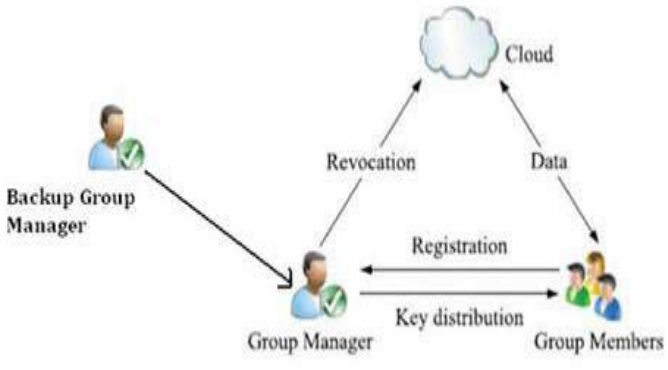
In the existing system, when there is any change in group, we need to circulate new key to every member and encrypt all the files. As if any member is revoked then we need to redistribute the new group key to all the members present in that group,as the revoked user have the key they were using and he/she can misuse the key . Then we have to encrypt all the files with that new key, which is quite a tedious job. Same problem arises when we invoke any new members to the group also. When working in cloud members feel unsafe as their identity is shown to everyone, but if it isn't then the member may misbehave as their identity is not traceable. So we need to keep in mind that this will also not happen. And lastly, one more problem is that there is a single data-owner in which only one can modify the files and others can only read the files [8].

III.PROPOSED SYSTEM

To accomplish the reliable and scalable in MONA, in this cardboard we are presenting the new framework for MONA. In this adjustment we are added presenting how we are managing the risks like abortion of accumulation administrator by accretion the amount of advancement accumulation manager, blind of accumulation administrator in case amount of requests added by administration the workload in assorted accumulation managers. This adjustment claims appropriate efficiency, scalability and a lot of chiefly reliability.

The main models for this project are:

Group Signature: A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Essential to a group signature scheme is a *group manager*, who is in charge of adding group members and has the ability to reveal the original signer in the event of disputes. A group signature scheme must satisfy correctness, which ensures that honestly-generated signatures verify and trace correctly



Data Encryption: Data encryption also allows the group manager to dynamically include new members while preserving previously computed learning the content of the stored data. In this method, they use IP multicast mechanism to shortest rekeying time to

minimize adverse effect on communication. In addition, they introduce proxy mechanism for replies from group members to the group manager to reduce traffic generated by rekeying.

Traceability: 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. When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner there are few lemmas used in our project: Lemma 1: only authenticated user can access the cloud. Lemma 2: Revoked users cannot access the cloud after their revocation. Lemma 3: The revoked user is note able to access the cloud due to in traceability. Now, we explain the system elements:

User Registration: This module is used for registering any member .Here details like name, address, email id, password, phone number, date of birth are filled. If all details about that member are correct then the member is registered. After registration a mail is generated and sent to that member mail id that the member registration is activated or not. It is responsibility of manager to add the member into any group and activation of member.

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

Manager module: This module is for activating member request. When any member try to register and if all details are correct then a request is sent to manager and manager has authority to accept the request .If the request is accepted then a mail is generated and sent to the member Gmail id. In that mail generated key is sent and using that key the member can view any uploaded file. This module is for login purpose of manager. Here manager name and his password is entered and if all details are correct then the manager is logged in successfully.

Member module: Group members are a set of registered users that will store their private data into the cloud server and Share them with others in the group. This module is used by member to upload any file. File is uploaded in encrypted way and if any member wants to view that file then they should me valid member and they have to download that file. Manager has authority to view uploaded file so that any malicious file is not uploaded. Manager has all details about that uploaded file.

Data Flow: The below data flow diagram shows that under the cloud module ,there are two modules Group Manager module Group member module Both can login using their login details. After successful login, Group Manager activates newly added members of the cloud. He can also check the group details, file details of the cloud and he can also delete the files. After successful login, Group Member's signature is verified. After successful verification, the member can upload, download and can modify the files. The Group Member's account can be revoked after he leaves the cloud by the Group Manager. If the login fails, due to the wrong login details, both in Group Member and Group Manager modules, an error is generated. Because of which neither Manager nor Member can login. During group signature verification in the Group

Member module, if the verified result turns out to be false, it is treated as an error and the Member has no access over the group.

IV.CONCLUSION

In this paper, we design a secure data sharing scheme, for dynamic groups in a un trusted cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, it 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, length of the signature and the running time of the signing algorithm are independent with the number of group members.

REFERENCES

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

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

[3] 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.

[4] 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.

[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

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

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

[8] 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.

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

[10] 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.

[11] 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.

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