ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Prof. Jyoti Raghatwan, Alka Taur,

RMD Sinhgad School of Engineering, Pune, India

Student, RMD Sinhgad School of Engineering, Pune, India

ABSTRACT: In this review users can achieve an effective and economical approach for data sharing among group members in the cloud with characters of low maintenance and little management cost. Proposed system must provide security guarantees for the sharing data files since they are outsourced. Due to the continuous change of the membership sharing data while providing while giving security protecting is still challenging, especially for an untruth cloud due to the collusion attack. In existing system the secure key distribution is based on the secure communication channel, however to have such a channel is strong assumption and is difficult for practice. In this system we propose a secure data sharing scheme for dynamic members. In proposed system first propose is secure way for key distribution without using any secure communication channels, and user can securely obtain their private keys from group managers. The system can accomplishes fine grained access control any client in the gathering can utilize the source in the cloud and disavowed clients can't get to the cloud again after they are denied. Also the system can protect the system form collusion attack, which means that users cannot get original data files even if they conspire with entrusted cloud.

KEYWORDS: Access control, privacy-preserving, key distribution, cloud computing

I. INTRODUCTION

Cloud computing is a type of internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a style of computing in which dynamically scalable and often virtualization resources are provided as a service over the internet. 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. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud.

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. Therefore, traceability, which enables the group manager to reveal the real identity of a user, is also highly desirable. 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. 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

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. Several security schemes for data sharing an untruth servers have been proposed . In these approaches, data owners store the encrypted data files in entrusted storage and distribute the corresponding decryption.

II. RELATED WORK

1) *Paper Name:- "Cryptographic cloud storage," in Proc. of FC, January 2010, pp. 136-149.*
Authors:- S. Kamara and K. Lauter
Abstract:-The cloud provider provides one of the best services is data storage the security and privacy issue have major concern for organization for utilizing such service.

2) *Paper Name:- "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*
Authors:-R. Lu, X. Lin, X. Liang, and X. Shen,
Abstract:-It is a greatest platform that provides data storage in very lesser cost and all time it should be available over the internet. The security must be important in the cloud computing. The encryption technique is commonly adopted by the cloud computing that means the encrypted data should be stored on the storage of cloud to protect the data. Encryption is no sufficient as organization obtain have to enforce fine-grained access control on data. Such control is based on the attribute that system is known as the attribute based system. For the data privacy it is important to encrypt the data and upload the encrypted data on the cloud. In cloud it is not easy to design efficient and secure data sharing scheme in multiowner system due to the following challenging issues. Identity, revocation and new member participation i.e. the changes of membership make securely data sharing extremely difficult. On the other hand an efficient member revocation without updating the secret key of remaining user to minimize the complexity of key management. Signed receipt is caused after every member revocation in group that minimizes multiple copy of encrypted file it can help to minimize computation cost

3) *Paper Name:-* "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
Authors:- M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,
Abstract:-Presented cryptographic storage system that enable secure data sharing. In this technique dividing file into the file group and encrypt each file group with a file block key. In this scheme at the time of user revocation the file block key need to be updated and distributed to the user therefore the system had a heavy key distribution overhead.

4) *Paper Name:-* "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing
Authors: - R. Lu, X. Lin, X. Liang, and X. Shen
Abstract:-Proposed a secure provenance scheme by leveraging group signature and cipher text policy attributes-based encryption technique , after registration each user he obtain two key in which the attribute key is used to decryption which is encrypted by the attribute based encryption. Group signature key is used for privacy preserving and traceability. So, that in this technique revocation is not supported.

III. EXISTING SYSTEM APPROACH

1. In existing system the security of key distribution is based on the secure communication channel however to have such channel is a strong assumption and is difficult for practice.
2. To share data while providing privacy-preserving is still a challenging issue, especially for untruth cloud due to collusion attack.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Attribute- based encryption technique:
Attribute-based encryption is a type of public key in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text

Disadvantages:-

1. Data are not secure when sharing data.
2. Revoked users will be able to access the data after they revoked.

IV. PROPOSED SYSTEM ARCHITECTURE

1. In this system propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group.
2. The system provides a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
3. The system can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
4. Secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untruth cloud. Our scheme can achieve secure user revocation with the help of polynomial function.
5. System is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.
6. System will provide security analysis to prove the security of our scheme.

ADVANTAGES OF PROPOSED SYSTEM

1. The computation cost is irrelevant to the number of revoked users in RBAC scheme. The reason is that no matter how many users are revoked, the operations for members to decrypt the data files almost remain the same.
2. The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The reason for the small computation cost of the cloud in the phase of file upload in RBAC scheme is that the verifications between communication entities are not concerned in this scheme.
3. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user

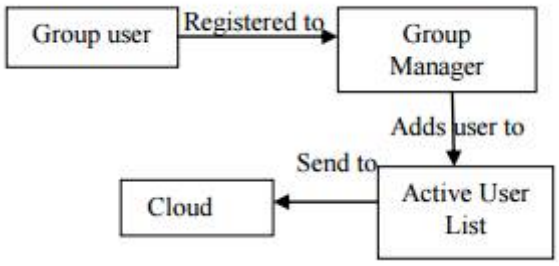

Fig 1.Proposed System Architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

V. CONCLUSION

The system is design for secure data sharing scheme, for dynamic groups in an untruth 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. A new type authentication system, which is highly secure, has been proposed in this system.

REFERENCES

[1] Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud Xuefeng Liu, YuqingZhangBoyang Wang, and Jingbo Yan 2013 IEEE.
[2] S.Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.
[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote entrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw.Distrib. Syst. Security Symp., 2005, pp. 29–43.
[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput.Commun. Security, 2010, pp. 282–292.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput.Commun.Security,
2010, pp. 282–292.
[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.
[10] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans.ParallelDistrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.