International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 4 Issue 4 April 2018
ISSN (Online): 2455-4723

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

Ayushi Dashore[1] Mohit Jain[2]
1 M.Tech Scholar 2 Head of Department Computer Science
1,2 Department of Computer Science & Engineering
1,2 BM Group of College of Engineering and Technology, Indore, Madhya Pradesh, India

Abstract -**Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database.**

In the proposed project we are going to deal with data security in cloud .The key feature of our project is to create a system which work with data security, access control and Group Management. For this we examine the number of algorithms and techniques to implement our system and now we are going to use some of them to implement our system.

Key terms: - Access control, security, privacy, cloud computing, Group Management.

I. INTRODUCTION

Cloud storage is a simple and scalable way to store, access, and share data over the Internet. Cloud storage is a service model in which data is maintained, managed, backed up remotely and made available to users over a network .In this data can be shared in secured manner, in cloud it can be achieve secure data sharing in dynamic groups. Cloud computing offers an infinite storage space. In our scheme, secured data sharing can be protected from collusion attack [1]. The key aim of the proposed work is to include the four factors in the proposed approach of the system:

Secure manner of key distribution

- ✓ Access control
- ✓ Secure way of data sharing
- ✓ Dynamic group management

A. Security Issues

- ✓ **Data protection: -**Data protection is the process of safeguarding important information from corruption, compromise or loss [2]. Data security plays an important role in cloud computing environment where encryption technology is the best option whether data at rest or transmitted over the internet.
- ✓ **Confidentiality:-**Confidentiality refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data [4].
- ✓ **Availability**:- When the data is shared among many users, there has to be more flexibility in the encryption process to handle users of the group, manage the keys between users, and enforce the access control policy in order to protect the data confidentiality
- ✓ **Access control**: - When data is outsourced to the cloud, which is untrusted because it is in a domain where security is not managed by the data owner, data security has to be given more attention. When more than one entity want to share data, there has to be a mechanism to restrict who can access that data.[3]
- ✓ **Integrity:-**Data that is stored in the cloud could suffer from the damage on transmitting to/from cloud data storage. Since the data and computation are outsourced to a remote server, the data integrity should be maintained and checked constantly in order to prove that data and computation are intact. Data integrity means data should be kept from unauthorized modification. Any modification to the data should be detected. [3]

II. PROBLEM DOMAIN

1. In the existing system there is three main entities Cloud, Group manager and Group Member. Each time a new user joins the group or leaves the group hence there is always need of a group manager or Certificate Authority. It increases the overhead of a system. This type of Dynamic membership includes dynamic overhead over group Manager.
2. Access Control is a second part of Authentication process which also needs attention of Certificate Authority to support data access.

III. SOLUTION APPROACH

Basically in an access control based data sharing system the access policies and user credentials are included. The access policy defines the role of users in the groups and

decides which user can perform which task. Therefore the system can be demonstrated using the following tuple.

[User list, access policy]

In this context the user list is fluctuating factor which is depends on the users exist in a group, additionally their revocation of group and joining new members. If the user attributes are directly used then for each joining of new member and revocation impact on the key generation. And need to be update keys frequently. Therefore in order to deal with the existing problem without including the additional authority a new kind of solution is required**.**

In order to accomplish the two aspects of the objective namely for access control and the dynamic group management the following concept is included.

1. User credentials are used only for the authentication purpose that helps to manage the dynamic group management.
2. Additionally association of tuple helps to identify the access policy of the user.

The figure 1 helps to understand the process of the authentication and authorization. This process helps to identify the first attribute of data cryptography. On the other hand the data attribute is used as the second parameter for encryption and data sharing. The process of data encryption and sharing is defined in figure 2.

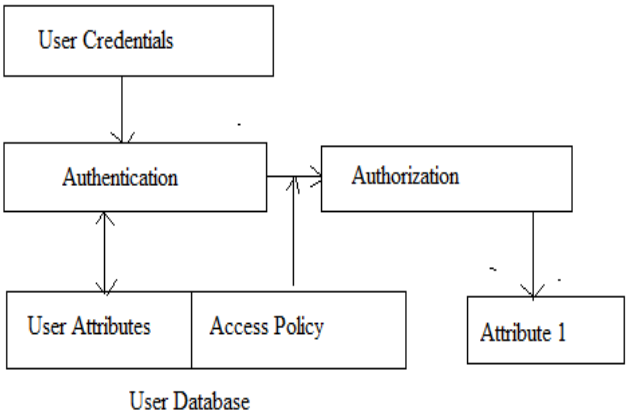
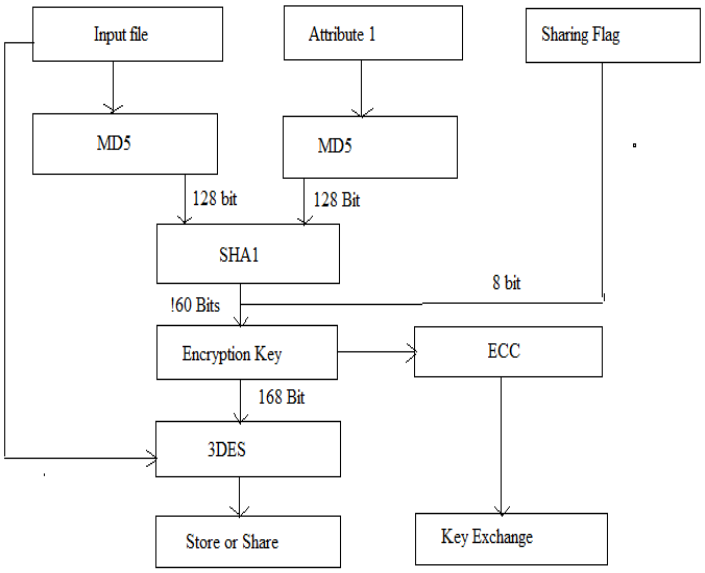
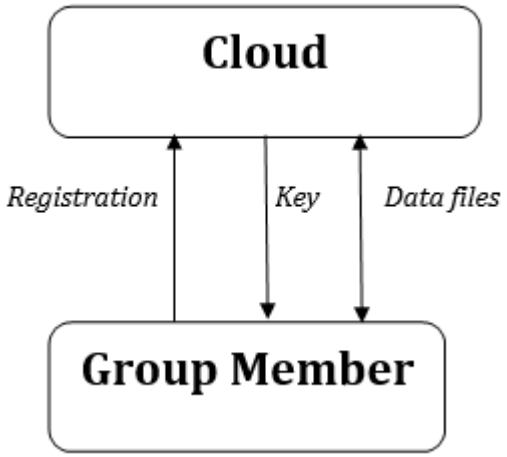


Figure 1 First Attribute Derivation



IV. SYSTEM ARCHITECTURE

Our project consists of two entities: - Group Member, and Cloud. it really refers to saving data to an off-site storage system maintained by a third party. Instead of storing information to your computer's hard drive or other local storage device, you save it to a remote database. The Internet provides the connection between your computer and the database. The group members will store their data files in cloud and share them to others. In the plan, a new client can be register and revoked any time.



A. Dynamic Groups

The number of users keep changing in dynamic groups and also data security is very difficult. Hence two major issues to be addressed in dynamic groups are

- ✓ Newly approved user must be able to get all the files shared prior to their joining without contacting data owner
- ✓ After each revocation, key of remaining members in the group need not be updated**.**

B. Modules

1. User Registration
2. Login
3. File Upload
4. File Access and Download
5. User Revocation

C. Advantages of Proposed System

- ✓ Any user in the group can store and share data files with others by the cloud after registration.
- ✓ The encryption complexity and size of cipher text are independent with the number of revoked user in the system.
- ✓ User revocation can be achieved without updating the private keys of remaining users.

V. COMPARATIVE STUDY

S. No.	Paper Title	Publication and Year	Algorithm/ Method used	Remark
1.	Mona: Secure Multi Owner Data Sharing for Dynamic Groups in the Cloud	IEEE Transactions on parallel and distributed system Vol24 NO6 June 2013	Dynamic Broadcast Encryption and Digital signature	This paper combines the group signature and dynamic broadcast encryption scheme to give the facility to use the cloud resources and allow data owner to securely share their data.
2.	Key Policy Attribute Based Encryption (KP-ABE)	International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 2, 2015	KP-ABE CP-ABE	In our proposed system, it resolve KP-ABE access scheme in manner such that the encrypter cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data
3.	Privacy preserving policy based content sharing in public	International Journal of Scientific Engineering and technology Research Vol.04	Two layer Encryption (TLE) based approach	Current approaches to enforce ACPs on outsourced data using selective encryption require

	clouds	Issue27,july 2015 Page5169-5172		organizations to manage all keys and encryptions and upload the encrypted data to the remote storage. This paper proposed a two layer encryption to reduce the overhead at the Owner.
4.	Achieving secure, scalable and fine-grained data access control in cloud computing	International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2440-2447	attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption	In this paper we propose a scheme to achieve this goal by exploiting KP-ABE and uniquely combining it with techniques of proxy re-encryption and lazy re-encryption
5.	A secure anti-collusion data sharing scheme for dynamic groups in the cloud	JETIR October 2016, Volume 3, Issue 10 Page 196-199	Symmetric key algorithms and Asymmetric key algorithms	In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels.

VI. CONCLUSION

In this, we design a secure anti-collusion sharing of the data for dynamic groups in the cloud. Private key of the group member not need to be updated or recomputed when the user joins or leaves the group. Revoked user are unable to get their original data from the cloud after their revocation. This scheme can achieve secure user revocation.In this paper there is no need for Certificate Authority that is no need of group manager, which reduces the overhead of system.

REFERENCES

[1] M.Nikitha,R.Aiswarya,N.praveena and N.Ramakalpana "Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in Cloud " in International Research Journal of Engineering and Technology (IRJET) ,pp 230-237 Volume: 04 Issue: 03 ,Mar -2017

[2] http://searchdatabackup.techtarget.com/definition/data-protection.

[3] Sultan Aldossary and William Allen "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions" in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016, pp.485-498.

[4] https://developer.mozilla.org/enUS/docs/Web/Security/Information_Security_Basics/Confidentiality,_Integrity,_and_Availability.

[5] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.

[6] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc.

Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.

[7] 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.

[8] 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.

[9] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[10] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.

[11] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602–2614, Nov. 2013.

[12] 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.

[13] p.hemalatha, and pallachamundeswari " a secure anti-collusion data sharing scheme for dynamic groups in the cloud" in JETIR, October 2016, Volume 3, Issue 10 pp 196-199.

[14] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptograph2007, pp. 39–59.