www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 6 June 2016, Page No. 16886-16888

Review On Secure Anti-Collusion Data Sharing For Dynamic Group In The Cloud

Rahul S.Nandanwar[1], Vijendrasinh P.Thakur[2]

[1]M.Tech 2nd year, Dept of CSE, RGCER
[1]Nagpur, M.H, India
[1]rahulnandu.3@gmail.com

[2]Dept of CSE, RGCER.
[2]Nagpur, M.H, India.
[2]vijendrapthakur@gmail.com

Abstract*: Benefited from cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost.*

In multiuser cloud computing there may be a major problem to securely share documents. Frequent change of membership, challenging issues to prevent the system from collusion attack, to secure the system from the revoked user. In this paper we propose a secure data forwarding mechanism for dynamic member. Firstly, we propose a cloud system in which no of server should be present any user must store the file in any server. Secondly, the file must upload in no of blocks in the same server. Thirdly, the data forwarding; the uploading user may forward the data to the requested user in the cloud. If the member of cloud should exchange the information to one another they forward the data to the id of the members. Other member can't access file in the cloud without permission of file up loader. By this scheme the revoked user can't access the original data. in this scheme all the time the cloud member get permission from the up loader member for access the information at the time of file transfer up loader know the requested id he provide the server id and no of block to the downloader. The file should store in the server in maximum four no of block i.e. file is splitting in four parts. Each two block should be encrypted and store in the server. RSA and MD-5 encryption algorithm should be used for encrypting four blocks. In multiuser environment user doesn't know which encryption will used for which block.

Keywords: cloud computing, encryption, key distribution, forwarding mechanism.

1. Introduction

Intrinsic resource sharing and low maintenance characteristics the cloud computing is an alternative to traditional information technology.

[1] 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] 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.

2. Related Work

[3] 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] Explained and combined technique of key policy attribute-based encryption [5],proxy re-encryption and lazy re-encryption to achieve fine grained data access control without disclosing data content.

[6] 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.

[7] Propose secure multiowner data sharing scheme named as Mona. He claimed that his scheme achieve fine grained access control and revoked user can not access the shared data again after he was revoked. By the cloud and revoked user this scheme should be suffer from the collusion attack. Revoked users use his private key to decrypt the encrypted data after his revocation. For accessing file, in which revoked user send request to the cloud. Cloud respond the corresponding encrypted data file without verify the revocation list. Then the revoked users compute their decryption key by attack algorithm so the attack should be done.

[8] presented a secure access control scheme on encrypted data in cloud storage by invoking role-based encryption technique in this scheme can achieve efficient revocation that contain role-based access control. In this scheme verification between entities is not concern that is this scheme is easily suffer from attacks.

[9] Presented practical and flexible key management mechanism for trusted collaborative computing by leveraging access control polynomial for the dynamic group this scheme should be design to efficient access control secure way for sharing the personal permanent portable secret between the user and the server is not supported. If the attacker obtained the personal permanent portable secret it should disclosed the private key.

3. Proposed Scheme

[10] Proposed a scheme that provides a secure way for key distribution without secure communication channels. In which the user can securely obtain their private keys from the group manager without any certificate authority due to the verification for the public key of user. This scheme can achieve fine grained access control. This scheme uses the polynomial function for user revocation so it protect form collusion attack. This scheme support dynamic group efficiency in which private key will not be recomputed and update at the new user joining or user revocation.

In this paper we proposed a scheme that provides the anti-collusion data sharing in multiuser cloud. Firstly the user registration user can register in the system in which user provides the information about him and complete the registration process system provides the user id and password to access the cloud. This information should be managed by the group manager. The uploading user uploads a data into the cloud. The data must be stored in the no. of server in the cloud and the up loader user use the block for the data storage. The block that means the one file must stored in to the n0. Of blocks in the same server. All the activity should be manage by group manager. The file should be stored as no. of blocks in the server. The two types of encryption algorithm is used for the encryption. The encrypted data stored in server.

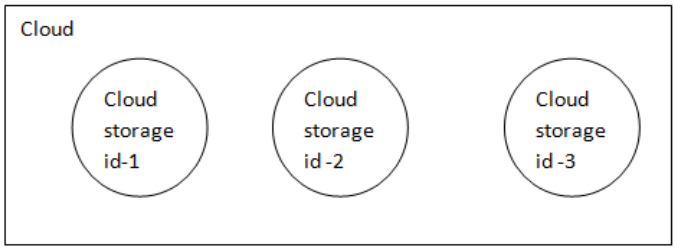

Fig.1 cloud server storage

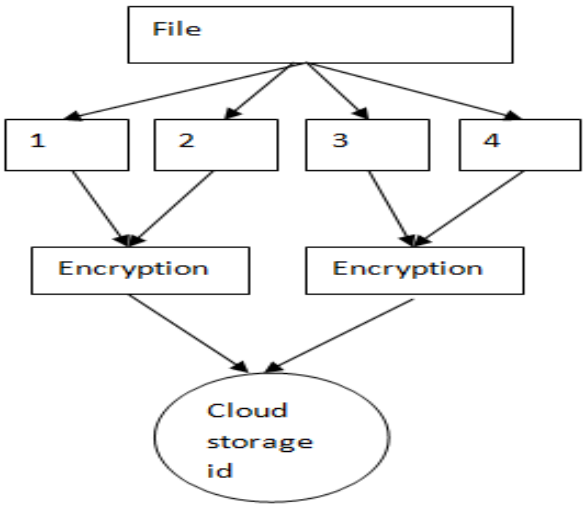

Fig.2 files uploading

The downloading user accesses the uploading data. It sends request to the uploading user the uploading user check that request and forwards the data to the requested user id. The uploading user forward the data that contend the information about the file name, stored server id, and no. of blocks used to store that file. The downloader user search that file in the server by its file name. The server request the block no and server id to the downloader, the downloader enter the server id and block no the server granting the access permission of that file to the user. The group manager can manage the information about the group manager and information details about the user it can monitor the activity of the uploading and downloading user. It can maintain the revoked user list if the user must be revoked the manager pleased this user as revoked.

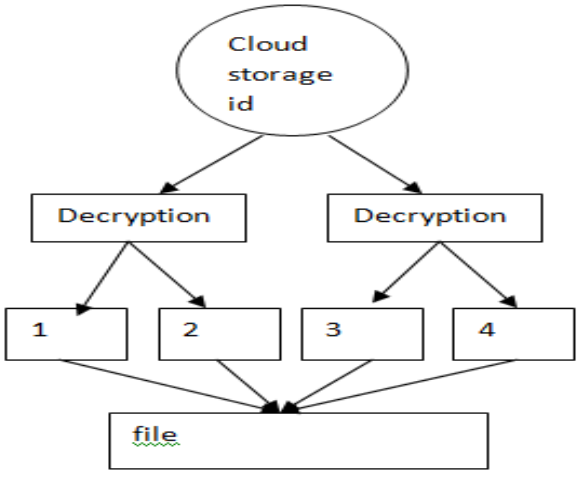

Fig.3 files downloading

4. Proposed Architecture

Following architecture shows that the cloud storage has many storage areas in which user stored his file. The admin manage all the activity like maintain the vendors list and revoked user list. The file is stored in the storage area before that it will split into four blocks and the encrypted by two encryption algorithm RSA and MD-5. After that at the time of downloading the user must request to the file access to the

uploading user the admin check that request and grant his request. He sends the access key to the requested user throw the mail. The user doesn't know the encryption pattern.

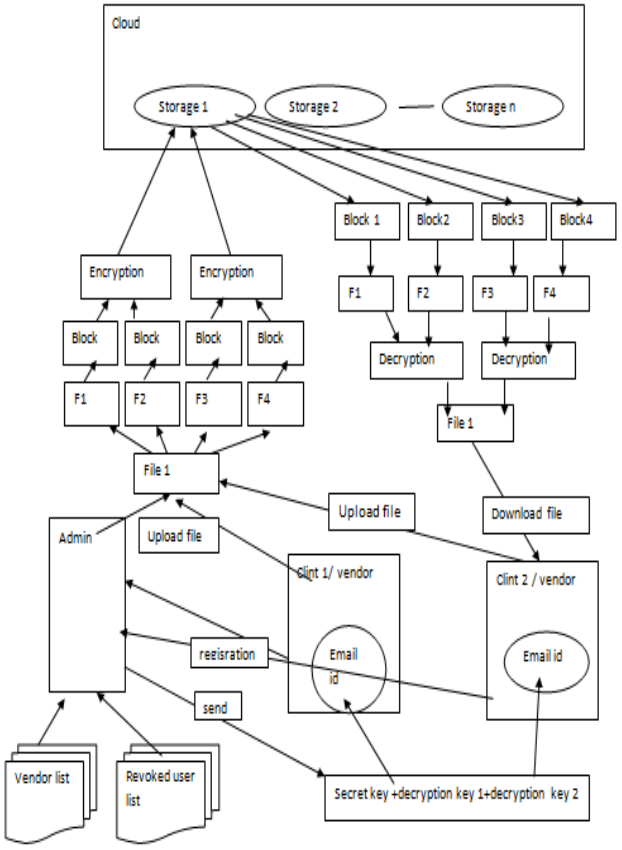

Fig.4 Architecture of anti-collusion data sharing in dynamic group

The main goal of the proposed scheme including access control, data confidentiality, efficiency as follows.

Access control:

The cloud member are able to use the cloud resources for data operation. Unauthorized user can not access the cloud and the revoked user will be incapable of using cloud once again after they are revoked.

Data confidentiality:

For data confidentiality it required that the unauthorized user and the cloud are incapable to learn the content of stored data and the important thing is that it always available for dynamic groups. New users decrypt data before they participate and revoked user can not decrypt data after they are revoked.

Efficiency:

The efficiency is that, any user in the cloud can store and share the data to any other. Revocation can be achieved without involving remaining user. Without any updating system may work after the revocation.

5. Conclusion

In this paper, we design anti-collusion data sharing scheme for dynamic group in the cloud. In our scheme we use two types of algorithms to encrypt and decrypt the data stored in the cloud for more security that is used to make more difficult system for attack. In this scheme we use forwarding mechanism in which uploading user has authority to forward his data to the other user and requested user I. e downloading user will request for data to the uploading user. All the activity can be manage by the manager

References

[1] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. of FC, January 2010, pp. 136-149.

[2] 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.

[3] 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.

[4]] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[5] 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

[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] I.Varun and Vamsee Mohan.B," An Efficient Secure Multi Owner Data Sharing for Dynamic Groups in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June-2014, pg. 730-734

[8] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[9]] Xukai Zou, Yuan-shun Dai, and Elisa Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," INFOCOM 2008, pp. 1211-1219.

[10] Zhongma Zhu and Rui Jiang," A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems DOI:10.1109/TPDS.2015.2388446.

Author Profile

Rahul S. Nandanwar M.Tech 2nd Year, Computer Science and Engineering, Rajiv Gandhi College of Engineering & Research, Wanadongri Nagpur,441110.

Vijendrasinh P. Thakur Assistant Professor Dept Of Computer Science and Engineering, Rajiv Gandhi College of Engineering & Research, Wanadongri Nagpur,441110.