IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 8, August 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

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

[1]S.David Arokkiya Doss, [2]A.Senthil Kumar,
[1]M.Phil Scholar, Tamil University, Thanjavur, Tamil Nadu, India.
[2]Assistant Professor, Tamil University, Thanjavur, Tamil Nadu, India.

1.ABSTRACT

Cloud computing also leverages perception from helpfulness computing to recommend metric on behalf of the services used. Such metrics are at the hub of the public cloud pay-per-use models. In addition, measured services are crucial parts of the feedback loop in autonomic computing, allowing services to range on-demand and to perform automatic failure recovery. Cloud computing is a sort of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute exhaustive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

Software as a Service (SaaS). The competence make available to the user is to use the provider's applications running on a cloud infrastructure. The applications are available from various client devices through either a thin client boundary, such as a web browser, or a program boundary.

Platform as a Service (PaaS). The ability afford to the consumer is to systematize onto the cloud infrastructure consumer-created or obtain applications created using programming languages, libraries, services, and tools supported by the contributor. possibly configuration settings for the application-hosting surroundings.

Infrastructure as a Service (IaaS). The potential provided to the consumer is to stipulation processing, storage, networks, and other fundamental computing possessions where the consumer is able to position and run random software, which can contain operating systems and applications.

2.INTRODUCTION

Benefited from cloud computing, users can bring about an successful and economical move toward for data sharing amongst group members in the cloud with the characters of low continuation and little management cost. Meanwhile, we must afford security guarantees for the allocation data files since they are outsourced. Unfortunately, because of the regular change of the membership,
Sharing data though providing privacy-preserving is immobile a challenging issue, especially for an untrusted shade due to the collusion attack. Moreover, for existing schemes, the refuge of key distribution is based on the secure communication channel, however, to have such direct is a strong postulation and is difficult for practice. In this paper, we propose a locked data sharing scheme for dynamic members. First, we

propose a locked way for key distribution without any secure communication channels, and the users can steadily obtain their private keys from group manager. Second, our method can achieve fine-grained access control, any user in the group can use the cause in the cloud and revoked users cannot access the cloud once more after they are revoked. Third, we can protect the method from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. In our move toward, by leveraging polynomial function, we can realize a secure user revocation scheme. Finally, our scheme can realize fine efficiency, which resources previous users need not to keep informed their private keys for the condition either a new user joins in the collection or a user is revoked from the group.

3. REVIEW OF LITERATURE

Paper 1: 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,

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.

Paper 2: Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage".

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

Paper 3: 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.

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

Paper 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.

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. after that the revoked users compute their decryption key by attack algorithm so the assault should be done presented a sheltered 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. 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 protected way for sharing the personal enduring portable secret between the user and the server is not supported. If the enemy obtained the personal permanent convenient secret it should disclosed the private key.

4. A SECURE ANTI-COLLUSION

In cloud providing security, guarantees for the sharing data file. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. In this research work, we propose a secure data sharing scheme for dynamic members Firstly, we propose a secure way for key distribution without any secure communication channels, and the
Users can steadily attain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Thirdly, we can defend the system from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. This scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group.

As cloud computing turn out to be common, more and more responsive information By storing their data into the cloud, the data owners can be relieved from the burden of data storage and maintenance, so as to enjoy the on-demand high quality data storage service cloud server are not in the same trusted domain may put the outsourced data at risk. In this work, a secure data sharing scheme, which can achieve secure key distribution and data sharing for a dynamic group in the cloud.

The main contributions of this scheme include:

- A way for key distribution without any secure communication channels. The users protected can steadily obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
- This scheme 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.
- A secure data sharing scheme can be protected from collusion attack. The revoked users cannot be able to get original data files once they are revoked even if they conspire with the untrusted cloud. This scheme can achieve secure user revocation with the help of polynomial function.

5 . DATA SHARING SCHEME FOR DYNAMICGROUPS

Major problem in public clouds is how to share documents based on fine-grained attribute based access control policies, sharing data in a dynamic groups while preserving data and identity privacy from an un trusted cloud is still a challenging issue, due to the frequent change of the membership., encrypting documents with different keys using a public key cryptosystem such as attribute based encryption (ABE), and proxy re-encryption (PRE) approach has some weaknesses: it

cannot efficiently handle adding/revoking users or identity attributes, and policy changes; it requires to keep multiple encrypted copies of the same documents; it incurs high computational costs. In this paper, I propose a secure multi-owner attribute authorities based data sharing scheme for dynamic groups in the cloud. The aim of my paper is secure data sharing in a dynamic group where the there is no fixed Attribute authorities where as multi – owner attribute authorities scheme is possible. key policy key policy attribute-based encryption (KP-ABE) method is used to select dynamic AA (Attribute authorities) . By leveraging cluster name, signed receipts and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. As the result the computation cost is reduced and storage overhead and encryption computation cost of our scheme are independent with the number of revoked users so the encryption cost is also reduced.

Therefore, an important state is to hold fine-grained access control, based on policy spicier using individuality attributes, over encrypted data. However, it also poses important risk to the discretion of those stored files. To protect data privacy, a basic answer is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an well-organized and secure data sharing scheme for groups in the cloud is not an easy mission due to the following challenging issues. First, identity Second, it is recommended that any member in a group should be intelligent 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, Third, member revocation and signed reception e.g., new member participation and current member revocation in a group. The changes of membership formulate secure data sharing extremely complicated, it is impossible for new granted users to speak to with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, a competent membership re-vocation mechanism without updating of the secret keys of the remaining users decrease the complexity of key management, signed acceptance is collected after every member revocation in the group it minimizes the multiple copies of encrypted file and also reduces calculation cost.

6. CONCLUSION

Data secrecy requires that unapproved clients including the cloud are unequipped for taking in the matter of the put away information. To keep up the accessibility of information secrecy for element gatherings is still an necessary and testing issue. In particular, renounced clients can't decode the put away information document after the disagreement. Any gathering part can store up and impart information records to others in the assembly by the cloud. Client repudiation can be accomplished without including the others, which involve that the remaining clients don't have to revamp their private keys. A protected against accord information sharing plan for element bunches in the cloud. In our plan, the clients can safely acquire their private keys from gathering director Certificate Authorities and secure communication channels. Likewise, our plan can reinforce dynamic gatherings proficiently, when another client joins in the gathering or a client is deprived of from the

gathering, the private keys of exchange clients don't should be recomputed and redesigned. In addition, our plan can complete secure client repudiation, the disavowed clients cannot have the ability to get the first information records once they are denied not considering of the possibility that they plan with the untrusted cloud

7.REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski,
G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[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 untrusted 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.