© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

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

Mohd.Zameer
Kopal Institute Of Science & Technology
CSE,Bhopal (M.P)

Prof. Nitin Choudhary
Kopal Institute Of Science & Technology
CSE,Bhopal (M.P)

ABSTRACT: Benefited from cloud computing environment, client users can attain an effective and economical approach for data sharing among group members in the cloud with the characters of small maintenance and short management cost. Meanwhile, in this we must provide security guarantees for the sharing data file since they are outsourced the data. Unfortunately, because of the continual 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 paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. We propose a 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 untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function.

KEYWORDS— Access control, Privacy-preserving, Key distribution, Cloud computing

ISSN : 2278-6848
03
9 772278 684800
© International Journal for Research Publication and Seminar

1. INTRODUCTION:

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. Security concerns become the main limitation as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a main approach is to encrypt data files before the clients upload the encrypted data into the cloud. Unfortunately, this is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. A cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file block key. However, the file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead. However, the difficulties to user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users. A secure multi-owner data sharing scheme. It is claimed that the scheme can achieve fine-grained access control and revoked users will not be able to access the sharing data again once they are revoked. This scheme will easily suffer from the collusion attack by the revoked user and the cloud. The revoked user can use his private key to decrypt the encrypted data file and get the secret data after his revocation by conspiring with the cloud. In the phase of file access, first of all, the revoked user sends his request to the cloud, then the cloud responds the corresponding encrypted data file and revocation list to the revoked user without verifications. Next, the revoked user can compute the decryption key with the help of the attack algorithm. Finally, this attack can lead to the revoked users getting the sharing data and disclosing other secrets of legitimate members. Presented a secure access control scheme on encrypted data in cloud storage by invoking role-based encryption technique.

2. PROBLEM DEFINATION

In this, file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead. The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users. The single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.In our approach, by leveraging polynomial function; we can achieve a secure user revocation scheme. Finally, our 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.

3. PROPOSED WORK

In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. We provide 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.Our 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 after they are revoked. We propose a 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 untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function. Our scheme 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. We provide security analysis to prove the security of our scheme. 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 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. Below diagram show system architecture of proposed work

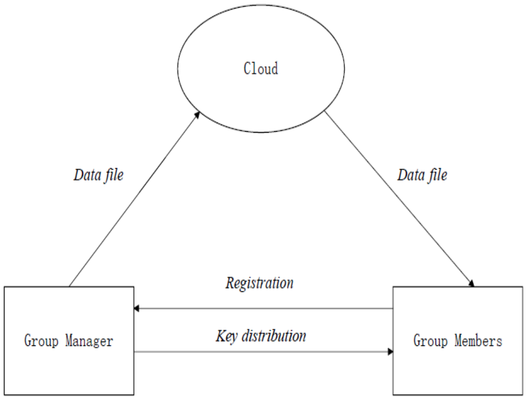
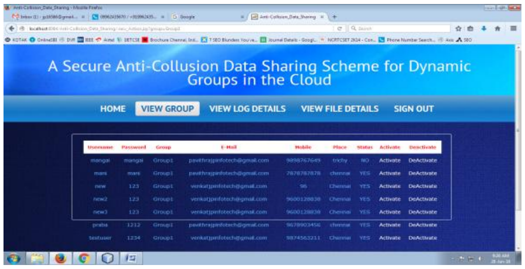


Fig 1: System Architecture

4. IMPLEMENTATION

We provide 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. 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. Below Diagram show the Implementation of proposed work.


Anti-Collusion_Data_Sharing - Mozilla Firefox
Google
Anti-Collusion_Data_Sharing
A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud
HOME
VIEW GROUP
VIEW LOG DETAILS
VIEW FILE DETAILS
SIGN OUT

Username	Password	Group	E-Mail	Mobile	Place	Status	Activate	Deactivate
mangai	mangai	Group1	pavithrajpinfotech@gmail.com	9898767649	trichy	NO	Activate	DeActivate
mani	mani	Group1	pavithrajpinfotech@gmail.com	7878787878	chennai	YES	Activate	DeActivate
new	123	Group1	venkatjpinfotech@gmail.com	98	Chennai	YES	Activate	DeActivate
new2	123	Group1	venkatjpinfotech@gmail.com	9600128838	Chennai	YES	Activate	DeActivate
new3	123	Group1	venkatjpinfotech@gmail.com	9600128838	Chennai	YES	Activate	DeActivate
praba	1212	Group1	pavithrajpinfotech@gmail.com	9678903456	chennai	YES	Activate	DeActivate
testuser	1234	Group1	venkatjpinfotech@gmail.com	9874563211	Chennai	YES	Activate	DeActivate

Fig2: show Implantation of Proposed Work

5. CONCLUSION AND FUTURE WORK

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. 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 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. Moreover, our scheme can achieve secure user revocation; the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

REFERENCES

[1] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Katz,A.Konwinski, G. Lee, D.Patterson, A.Rabkin, I.Stoica, andM.Zaharia. “A View of Cloud Computing,”Comm. ACM, vol. 53,no.4, pp.50-58, Apr.2010.

[2] S.Kamara and K.Lauter,“Cryptographic Cloud Storage,” Proc.Int’l Conf.Financial Cryptography and Data Security (FC), pp.136-149, Jan. 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] E.Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing Remote Untrusted Storage,” Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,“Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.

[6] 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.

[7] 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

[8] 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.

[9] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008

[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.