International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

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

M.Swapna & P.Sailaja Rani
1PG Scholar, Dept of CSE, Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam (Dt), AP, India.
2Assistant Professor, Dept of CSE, Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam (Dt), AP, India.

Abstract- *The Benefited from Cloud Computing, clients can achieve a flourishing and moderate methodology for information sharing among gathering individuals in the cloud with the characters of low upkeep and little administration cost. Then, security certifications to the sharing information records will be given since they are outsourced. Horribly, due to the never-ending change of the enrolment, sharing information while giving protection saving is still a testing issue, particularly for an untrusted cloud because of the agreement attack. In addition, for existing plans, the security of key dispersion depends on the safe communication channel, then again, to have such channel is a solid feeling and is difficult for practice. In this paper, we propose a safe information sharing plan for element individuals. Firstly, we propose a safe route for key dispersion with no safe correspondence channels, and the clients can safely acquire their private keys from gathering administrator. Besides, the plan can accomplish fine-grained access control, any client in the gathering can utilize the source in the cloud and refused clients can't get to the cloud again after they are rejected. Thirdly, we can protect the plan from trickery attack, which implies that rejected clients can't get the first information record regardless of the possibility that they scheme with the untrusted cloud. In this methodology, by utilizing polynomial capacity, we can achieve a protected client denial plan. At long last, our plan can bring about fine productivity, which implies past clients need not to overhaul their private keys for the circumstance either another client joins in the gathering or a client is give up from the gathering.*

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

1. INTRODUCTION:

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers. However, security concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud. Unfortunately, it 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 complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.

The techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents. However, 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. However, the 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, and 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. Unfortunately, the secure way for sharing the personal permanent portable secret between the user and the server is not supported and the private key will be Disclosed once the personal permanent portable secret is obtained by the attackers.

3. RELATED WORK:

In segment 2, we demonstrate the framework model and configuration objectives. In this paper, we propose a safe information sharing plan, which can accomplish secure key appropriation and information sharing for element bunch. The primary commitments of thisplan include:

1.We give a safe approach to key dispersion with no protected correspondence channels. The clients can safely acquire their private keys from gathering director with no Certificate Authorities because of the check for people in general key of the client.

2.This plan can bring about fine-grained access control, with the assistance of the gathering client list, any client in the gathering can utilize the source in the cloud and disclaim clients can't get to the cloud again after they are renounced.

3.We suggest a safe information sharing plan which can be protected from plot attack. The repudiated clients can not have the capacity to get the first information documents once they are denied in spite of of the fact that they plan with the untrusted cloud. Our plan can achieve secure client renouncement with the assistance of polynomial capacity.

4.The proposed plan can support dynamic gatherings effectively, when another client joins in the gathering or a client is disavowed from the gathering, the private keys of alternate clients don't should be recomputed and upgraded.

5. security examination to demonstrate the security of our plan. In extension, we additionally perform reenactments to exhibit the ability of our plan.

3. PROBLEM STATEMENT:

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

4. SCOPE:

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. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. 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. Moreover, for existing schemes, 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.

In this paper, 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 securely obtain 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 protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. 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. 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.

5. ALGORITHM:

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. The below steps are included in this algorithms,

1. 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.

2. 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.

3. 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.

4. 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.

5. We provide security analysis to prove the security of our scheme. In addition, we also perform simulations to demonstrate the efficiency of our scheme.

6. EXISTING SYSTEM:

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. Key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents.

DISADVANTAGES:

□ The 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.

7. PROPOSED SYSTEM:

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.

8.CONCLUSION:

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, and M.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

Distributed Systems 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.

Author's Details

M.Swapna Persuing M.Tech in Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India.

P.Sailaja Rani currently working as assistant professor in Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India. She is Highly Passionate and Enthusiastic about Her Teaching and Believes that Inspiring Students to Give of Her Best in Order to Discover What He Already Knows is Better Than Simply Teaching..She is having 10+ experience in teaching field currently working as assistant professor in Malineni Lakshmaiah Engineering College, Singarayakonda, Prakasam(Dt), AP, India.