Journal of Engineering Sciences
Vol11,Issue2,FEB/2020
ISSN NO:0377-9254

SECURE DATA COMMUNITY AGGREGATION AND STORAGE OF ATTRIBUTES IN THE PUBLIC CLOUD

G. RADHA DEVI[1], Dr. G. NANTHA KUMAR[2]
1. Research Scholar, Department of Computer Science & Engineering, SSSUTMS, Sehore, MP.
2. Research Guide, Department of Computer Science & Engineering, SSSUTMS, Sehore, MP.

Abstract: The fast advancement of cloud administrations, immense volume of data is shared through cloud computing. Albeit cryptographic methods have been used to give data secrecy in cloud computing, current instruments can't authorize protection worries over ciphertext related with multiple owners, which makes co-owners unfit to suitably control whether data disseminators can really scatter their data. In this paper, we propose a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data disseminator can disseminate the data to a new group of users if the attributes satisfy the access policies in the ciphertext. We further present a multiparty access control mechanism over the disseminated ciphertext, in which the data co-owners can append new access policies to the ciphertext due to their privacy preferences. Moreover, three policy aggregation strategies, including full permit, owner priority and majority permit, are provided to solve the privacy conflicts problem caused by different access policies. The security analysis and experimental results show our scheme is practical and efficient for secure data sharing with multi-owner in cloud computing.

Keywords:-Data sharing, cloud computing, conditional proxy re-encryption, ciphertext, attribute-based encryption, privacy conflict.

I. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology [1] due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful data centres. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staff in the same group or department to store and share files in the cloud. By utilizing the cloud, the staff can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [2]. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

A. Identity Privacy: The major problem for the wide adoption of cloud computing is Identity Privacy. Cloud users may be doubtful to join cloud based computing systems without the assurance of identity privacy because if User privacy is not maintained properly then the actual identities of the user can be disclosed easily to the various kinds of intruders and cloud service providers (CSPs).

B. No Multiple-owner Manner: Multiple-owner manner is more flexible than single owner manner because multiple owner manners allow every member in the group should be able to alter their own data i.e. every member is able to not only read the data but also modify his part of data in the entire data file, whereas single owner manner allow only group manager to store and modify data in the cloud and members can only read the data.

C. Effect of Dynamic Groups: The joining of new staff and revocation of current employee makes the group dynamic in nature. The frequent alterations of membership make efficient and secure data sharing in Cloud very complicated and hard due to the following two primary reasons: First, new granted users are not allowed to learn the content of data files stored before their participation by the anonymous system, because it impossible for new granted users to directly contact

with anonymous data owners and get the corresponding decryption keys. Second, to reduce the complexity of key management it is desirable to obtain an efficient membership revocation mechanism without updating the secret keys of the remaining users.

There are several security schemes that have been proposed up-to-date for efficient and secure data sharing on untrusted servers. In all of these approaches, the encrypted data files are stored in untrusted storage and distribute the corresponding decryption keys only to authorized users by the data owners. But, the issues of user revocation and multiple-owner manner have not been addressed very efficiently in these schemes.

II. LITERATURE SURVEY

A. Plutus: Scalable Secure File Sharing on Untrusted Storage. M. Kallahalla et al. [2] proposed cryptographic storage system which is known as Plutus. Plutus enables secure file sharing on untrusted server by using client based key distribution. Plutus allow client to handle all the key management and distribution operations. As compared to client, Server incurs very little cryptographic overhead because Plutus does not place much trust on server, it eliminates almost all requirements of server trust. Plutus divide files into filegroups and enable data owner to share the filegroups with others by encrypting each filegroup with unique file-block key that can protect data. There are some limitations identified in the Plutus such as a) A heavy key distribution overhead for large-scale file sharing. b) The file- block key needs to be updated and distributed again for a user revocation. Thus Plutus provides end-to-end security for group sharing system with lazy revocation.

B. Sirius: Securing Remote Untrusted Storage. E. Goh et al. [3] proposed a SiRiUS, Securing Remote Untrusted Storage. A SiRiUS is designed to handle secure multi user file system over insecure network using cryptographic operations. SiRiUS implements cryptographic read-write access control for file sharing without the use of a block server. Also it is possible for SiRiUS to implement large scale group sharing using the NNL key revocation construction. Key management and revocation is simple with minimal out-of-band communication. SiRiUS provides secure NFS without changing the file server. SiRiUS has some limitation in case of user revocation and dynamic groups. The user revocation is difficult for large scale sharing. Private Key of every group member must be updated while joining of new user in the group.

C.Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage. Ateniese et al. [4] proposed proxy re-encryption method to add the access control to the secure file system and distributed storage. Blocks of content are encrypted with unique and symmetric content keys by the data owner. The resulting encrypted content keys are further encrypted under a master public key. Additionally, to grant a user's public key, the appropriate content keys from the master public key is directly re-encrypted using proxy cryptography which helps in maintaining the access control and improvement of security. To supervise access to encrypted content stored on distributed untrusted replicas, this scheme makes use of centralized access control server. The main benefits of this scheme are that they are unidirectional and only a limited amount of trust is placed in the proxy. However, a collusion attack can occur between any revoked malicious user and untrusted server allowing them to find out the decryption keys of all the encrypted blocks of content.

D. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing. Yu et al. [5] offered a scalable and fine-grained data access control scheme by defining access polices based on data attributes and KP-ABE technique. The combination of attribute-based encryption (ABE), proxy re-encryption and lazy re encryption permit the data owner to assign the computation tasks to untrusted server without revealing the necessary contents of data. Data files are encrypted using random key by data owner. Using key policy attribute-based encryption (KP-ABE), the random key is further encrypted with a set of attributes. Then the authorized users are assigned an access structure and corresponding secret key by the group manager. Thus, only the user with data file attributes that satisfy the access structure can decrypt a cipher text. This system has some limitations such as multiple-owner manner is not supported by this system so that those single owner manners make it less flexible as only group manager are responsible for modifying the data file shared. And user secret key needed to be updated after each revocation.

E. Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing. Lu et al. [6] proposed secure provenance scheme which records ownerships and process history of data object. This scheme is based on the bilinear pairing techniques which rely upon group signatures and cipher text-policy attribute based encryption (CP-ABE) techniques. The basic feature of this scheme is to offer the anonymous authentication for user accessing the files, information confidentiality on sensitive documents stored in cloud and tracking the provenance on disputed documents for revealing the identity. Mainly, the system consists of a single attribute. After the registration, each user in this scheme obtains two keys: a group signature key and an attribute key. Using attribute-based encryption (ABE) any user can encrypt a data file. For decryption of the encrypted data, an attribute key is used by other in the group. To accomplish privacy preserving and traceability features, the user signs encrypted data with group signature key. Unfortunately, the disadvantage of this scheme is that user revocation is not supported.

III. PROBLEM ANALYSIS

In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. The main contributions of our scheme include: 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 cannot be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

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.

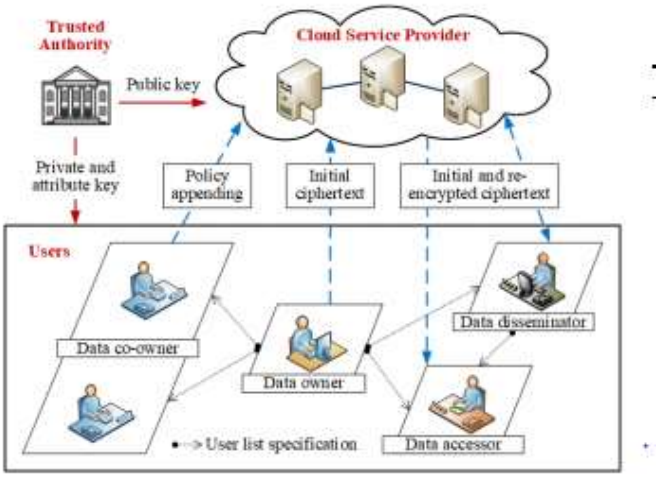

Fig: 3.1 System Model

3.1 POLICY AGGREGATION STRATEGIES

In our scheme, data co-owners can renew the ciphertext by appending their access policies as the dissemination conditions. We provide following strategies to fulfill the authorization requirements from multi-owner.

1) Full license: All owners (counting data owner and data co-owners) have a similar right to choose the scattering states of data. The data disseminator ought to fulfill all the entrance arrangements characterized by these owners.

2) Owner need: The data owner's choice has high need, however he labels the co-owners. The data disseminator can disperse the data just when he fulfills the entrance arrangement of data owner or all the entrance strategies of data co-owners.

3) Majority grant: The data owner right off the bat picks an edge esteem, and the data can be spread if and just if the entirety of access strategies fulfilled by disseminator's properties is more noteworthy than or equivalent to this fixed limit.

3.2 SECURITY MODEL

In our scheme, we assume the CA running on the trusted cloud platform to be fully trusted, which means it would not be compromised by malicious attackers, or collude with other malicious entities. However, we assume the CSP is honest but curious, which means it executes the tasks and may collude to get unauthorized data. Specifically, security requirements cover the following aspects.

1) Data confidentiality. The unauthorized users who are not the intended receivers defined by data owner should be prevented from accessing the data. Additionally, unauthorized access from CSP which is not fully trusted should also be prevented.

2) Re-encryption secrecy. The data disseminator whose attributes could not satisfy the access policy in ciphertext alone, or who tries to disseminate the ciphertext before specified releasing time, should be prevented from disseminating the ciphertext.

3) Flexible dissemination conditions. The data owner can custom fine-grained and timed-release conditions so that the data only can be disseminated by the users whose attributes satisfy these conditions after the releasing time.

4) Collusion resistance. The unauthorized data disseminators cannot collude with each other to generate the re-encryption key, thus the re-encryption of ciphertext should not be successful.

IV. SYSTEM ANALYSIS

In the above analysis in the encryption phase, data owner defines a set of identities and an access policy, and then uploads the encrypted data to the CSP. We utilize the computation time and communication size as the metric to measure complexity. The computation time is mainly related to two factors, that are number of assessors and attributes in the access policy. The computation time of data encryption versus |U| under a fixed access policy with 5 attributes and 3 co-owners. Due to data owner should set up one and multiple empty policies for co-owners in owner priority strategy and majority permit strategy respectively, the computation cost of these two strategies is higher than that of full permit strategy. Compares the communication cost of data owner when he chooses each of three strategies. On the whole, ciphertext sizes in three strategies are all increasing linearly with No. More particularly, communication cost of majority permit strategy is the highest, and the communication cost of owner priority strategy is a little more than full permit strategy, since the number of shares of C7, C8, C9, C10 in owner priority strategy is twice as much as that in full permit strategy. The number of shares in majority permit strategy is equal to the number of co-owners,

V. CONCLUSION

In this paper, we propose a secure data group sharing and dissemination scheme in public cloud based on attribute-based and timed-release conditional identity-based broadcast PRE. Our scheme allows users to share data with a group of receivers by using identity such as email and username at one time, which would guarantee data sharing security and convenience in public cloud. Besides, with the usage of fine-grained and timed-release CPRE, our scheme allows data owners to custom access policies and time trapdoors in the ciphertext which could limit the dissemination conditions when outsourcing their data. The

CSP will re-encrypt the ciphertext successfully only when the attributes of data disseminator associated with the re-encryption key satisfy access policy in the initial ciphertext and the time trapdoors in the initial ciphertext are exposed. We conduct our experiments with pairing-based cryptography library. The theoretical analysis and experiment results have shown the security and efficiency of our scheme.

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, ―Security Challenges for the Public Cloud,‖ IEEEInternetComputing,vol. 16, no. 1, pp. 69-73,2012.

[2] C. Delerablée, ―Identity-based Broadcast Encryption with Constant Size Ciphertexts and Private Keys,‖ Proc. the 13th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007), pp. 200-215,2007.

[3] F. Beato, S. Meul, and B. Preneel, ―Practical Identity-based Private Sharing for Online Social Networks,‖ Computer Communications, vol. 73, pp. 243-250,2016.

[4] J. Bethencourt, A. Sahai, and B. Waters, ―Ciphertext-policy Attributebased Encryption,‖ Proc. the 28th IEEE Symposium on Security and Privacy (S&P2007),pp. 321-334, 2007.

[5] Z. Wan, J. Liu, and R. Deng, ―HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing,‖ IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754,2012.

[6] H. Hu, G. Ahn, and J. Jorgensen, ―Multiparty Access Control for Online Social Networks: Model and Mechanisms,‖ IEEE Transactions onKnowledge and Data Engineering,vol. 25, no. 7, pp. 1614-1627, 2013.

[7] M. Blaze, G. Bleumer, and M. Strauss, ―Divertible Protocols and Atomic Proxy

Cryptography,‖ Proc. Advances in CryptologyEUROCRYPT1998 (EUROCRYPT '98),pp.127-144,1998.

[8] D. Tran, H. Nguyen, W. Zha, and W. Ng, ―Towards Security in Sharing Data on Cloud-based Social Networks,‖ Proc. the 8th International Conference on Information, Communications and Signal Processing (ICICS2011), pp. 1-5,2011

[9] L. Liu, Y. Zhang, and X. Li, "KeyD: secure key-deduplication with identity-based broadcast encryption," IEEE Transactions on Cloud Computing, 2018, https://ieeexplore.ieee.org/document/8458136.

[10] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," IEEE Transactions on Services Computing, 2018, https://ieeexplore.ieee.org/document/8395392.

[11] H. He, R. Li, X. Dong, and Z. Zhang, "Secure, effective and finegrained data get to control component for P2P stockpiling cloud," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 471-484, 2014.

[12] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A study of intermediary reencryption for secure data partaking in cloud computing," IEEE Transactions on Services Computing, 2018, https://ieeexplore.ieee.org/docu ment/7448446.

[13] J. Child, D. Kim, R. Hussain, and H. Goodness, "Contingent intermediary reencryption for secure enormous data group partaking in cloud condition," Proc. of 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 541–546, 2014.

[14] L. Jiang, and D. Guo "Dynamic encoded data sharing plan dependent on contingent intermediary communicate re-encryption for cloud stockpiling," IEEE Access, vol. 5, pp. 13336 – 13345, 2017.

[15] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, "A protected and effective ciphertext-strategy characteristic based intermediary re-encryption for cloud data sharing," Future Generation Computer Systems, vol. 52, pp. 95-108, 2015.

[16] X. Li, Y. Zhang, B. Wang, and J. Yan, "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, 2013