© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Novel Approach for Secure Knowledge Sharing through Multi-Owner for Static and Dynamic Teams within the Cloud

K. Ram Mohan Goud, A. Shiva Raj, A. Srisylam

Department of Computer Science & Engineering, Sri Indu College of Engineering & Technology, Hyderabad, India

ABSTRACT

With the character of low maintenance, cloud computing provides a cheap and economical answer for sharing cluster resource among cloud users. sadly, sharing knowledge during a exceedingly in a very multi-owner manner whereas conserving knowledge and identity privacy from an untrusted cloud remains a difficult issue, as a result of the frequent amendment of the membership. during this paper, we tend to propose a secure multi owner knowledge sharing theme for Static and dynamic teams within the cloud. By investment cluster signature and dynamic broadcast secret writing techniques, any cloud user will anonymously share knowledge with others. Meanwhile, the storage overhead and secret writing computation price of our theme square measure freelance with the quantity of revoked users. Additionally, we tend to analyze the safety of our theme with rigorous proofs, and demonstrate the potency of our theme in experiments.

Keywords: Cloud Computing, Knowledge Sharing, Privacy-preserving, Access Control, Dynamic groups

I. INTRODUCTION

Cloud computing is recognized as another to ancient information technology thanks to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), like Amazon, area unit able to deliver various services to cloud users with the help of powerful data centres. By migrating the native info management systems into cloud servers, users can fancy high-quality services and save necessary investments on their native infrastructures. One in each of the foremost elementary services offered by cloud suppliers is info storage. Enable United States to accept a smart info application. A company permits its staffs at intervals constant cluster or department to store and share files at intervals the cloud. By utilizing the cloud, the staffs could also be totally discharged from the tough native info storage and maintenance. However, it to boot poses an enormous risk to the confidentiality of those keep files. Specifically, the cloud servers managed by cloud suppliers are not completely positive by users whereas the information files keep at intervals the cloud is additionally sensitive and confidential, like business plans. To preserve info privacy, a basic answer is to cipher info files, therefore transfer the encrypted info into the cloud. Sadly, coming up with Associate in economical and secure info sharing theme for groups at intervals the cloud is not an easy task thanks to the next tough issues. First, identity privacy is one in each of the foremost necessary obstacles for the wide preparation of cloud computing. Whereas not the guarantee of identity privacy, users is additionally unwilling to hitch in cloud computing systems as a results of their real identities may be merely disclosed to cloud suppliers and attackers. On the other hand, unconditional identity privacy would possibly incur the abuse of privacy. For instance, misbehaved employees will deceive others within the company by sharing false files while not being traceable. Therefore, traceability, that allows the cluster manager (e.g., an organization manager) to reveal the $64000 identity of a user, is additionally extremely fascinating. Second, it's extremely counselled that any member during a cluster ought to be ready to absolutely fancy the

info storing and sharing services provided by the cloud, that is outlined because the multiple-owner manner. Compared with the single-owner manner, wherever solely the cluster manager will store and modify information within the cloud, the multiple-owner manner is additional versatile in sensible applications. Additional concretely, every user within the cluster is in a position to not solely read information, however additionally modify his/ her part of information within the entire record shared by the corporate. Last however not least, teams square measure commonly dynamic in observes, e.g., new employee's participation and current worker revocation during a company. The changes of membership build secure information sharing extraordinarily tough. On one hand, the anonymous system challenges new granted users to find out the content of information files keep before their participation, as a result of its not possible for brand spanking new granted users to contact with anonymous information homeowners, and acquire the corresponding decipherment keys. On the opposite hand, Associate in economical membership revocation mechanism while not change the key keys of the remaining users is additionally desired to reduce the complexness of key management. Many security schemes for information sharing on untrusted servers are projected. In these approaches, information homeowners store the encrypted information files in untrusted storage and distribute the corresponding decipherment keys solely to approved users. Thus, unauthorized users further as storage servers cannot learn the content of the info files as a result of them need no information of the decipherment keys. However, the complexities of user participation and revocation in these schemes square measure linearly increasing with variety the amount the quantity of information homeowners and also the number of revoked users, respectively. By setting a bunch with one attribute, a secure origin theme supported the cipher text-policy attribute-based coding technique, which permits any member during a cluster to share information with others. However, the problem of user revocation isn't self-addressed in their theme bestowed an ascendable and fine-grained information access management theme in cloud computing supported the key policy attribute-based coding (KP-ABE) technique. Sadly, the one owner manner hinders the adoption of their theme into the case, wherever any user is granted to store and share information. Our contributions to unravel the challenges bestowed higher than, we tend to propose Anglesey Island, a secure multi-owner information sharing theme for dynamic teams within the cloud.

II. METHODS AND MATERIAL

A. Systems Models and Goals

System Model

We consider a cloud computing architecture by combining with an example that a company uses a cloud to enable its staffs in the same group or department to share files. The system model consists of three different entities: the cloud, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs) as illustrated in Fig. 1. Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes but will try to learn the content of the stored data and the identities of cloud users. Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties. Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

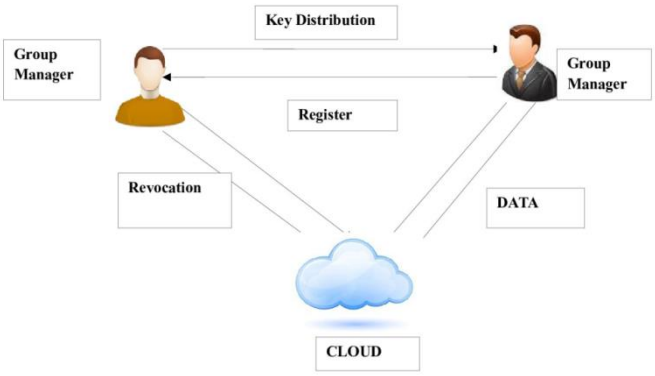

Figure 1. System Model

Design Goals

In this section, we describe the main design goals of the proposed scheme including access control, data confidentiality, anonymity and traceability, and efficiency as follows: Access control: The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked. Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of Fig. 1. System model. Learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation. Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners. Efficiency: The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

B. Existing Systems

In the existing group resource system, the group resources have been saved to cloud for low maintenance and cost effectiveness. In existing system a group resource saved to cloud and can be get by any group member as required. The issue with this system is that cloud is not a trusted one and can reveal the group information to other. And if any group member going to leave the group after leaving that group also he can use the resources by old credentials because in existing system there is no user revocation mechanism is present.

III. RESULTS AND DISCUSSION

Proposed Systems

In overcome to existed system we proposed a new system which stores the group resource to cloud with data broadcasting mechanism and with user revocation system. In proposed system when a group resource is storing into the cloud, it will not store in original manner, we using cryptography technique to secure group resource and key of that resource will share among group members. When a group member join the group he will get a group signature which will be common for all group member .Member can get into group by that signature only and get the key for resource by which he can decrypt the resource. In our proposed system we using revocation system it means when a member is going to leave the group the group signature will change and new signature will share among other member so old member cannot get interacted with the group and when a new member will join the group he will get that signature. The main contributions of this paper include:

1. We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.
2. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. 3. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.4. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

IV. CONCLUSION

In this paper, we design a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

V. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. 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] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM,pp. 534-542, 2010.

[4] 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.

[5] 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.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to SecureDistributed Storage,"Proc. Network and Distributed Systems Security Symp. (NDSS),pp. 29-43, 2005.

[7] 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.

[8] 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.

[9] 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.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers,"Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-62, 2001.