International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 3: March 2015, pp 50-52. www.aetsjournal.com ISSN (Online) : 2394-6237

Secure Data Sharing for Multi-Owners in the Cloud

C.K.Vijayalakshmi, B.Vanitha

Abstract— Cloud computing affords a cost-effective and efficient solution for sharing group resource among cloud users with the character of low and cost effective maintenance. But the major drawback of cloud computing is sharing data in a multi-owner manner, preserving data and identity privacy from an untrusted cloud. In this present investigation, a secure multi-owner data sharing structure called as Mona, for dynamic groups in the cloud is proposed. Any cloud handler can secretly share data with others through leveraging group signature and active broadcast encryption methods. Also, the overhead storage and encryption computation cost of this scheme are self-determining with the number of revoked users. The security of the proposed scheme was analyzed and demonstrated in this study.

Keywords— Cloud computing, Privacy, Dynamic group, Data sharing.

I. INTRODUCTION

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services like servers, storage and applications are delivered to an organization's computers and devices through the internet.

Cloud computing is accepted as an alternative to traditional information technologybecause of its fundamental resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Google, SAP, Oracle, etc. are providing number of services to their cloud users through powerful datacenters.

Data storage is one of the supremeessential services offered by cloud. Let us consider a practical data application. A firm allows its staffs in the same division to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. Conversely, 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 protect data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task.

C.K.Vijayalakshmi is with Department of Computer Science & Engineering,Podhigai College of Engineering & Technology, Tamilnadu, India.

B.Vanitha is with Department of Computer Science & Engineering,Podhigai College of Engineering & Technology, Tamilnadu, India.

II. AVAILABLE SYSTEM

Numerous security structures for data sharing on untrusted servers have been proposed already. In all these types, encrypted data files storage and their corresponding decryption keys are available only for the authorized users. So, the unauthorized users as well as storage servers cannot access the files due to unavailability of decryption keys. However, the difficulties of user contribution and reversal in these structures are linearly increasing with the number of data owners and the number of revoked users, respectively. Through a group with a single attribute, the secure provenance scheme can be proposed based on the cipher text policy attributebased encryption method, which allows any member in a group to share data with others. But, user revocation issue is not mentioned their structure. Based on the key policy attributebased encryption (KP-ABE) method, a scalable and fine-grained data access control structure in cloud computing can be presented. Unluckily, the single-owner manner hinders the adoption of their structure into the case, where any user is granted to store and share data.

III. RELATED WORK

A cryptographic storage system that permits secure file sharing on untrusted servers, named Plutus is proposed here. The data owner can share the file groups with others by delivering the equivalent lockbox key by dividing files into file groups and encrypting each file group with a unique file-block key.

However, it conveys about a heavy key distribution overhead for large-scale file sharing. Moreover, the file-block key wants to be updated and distributed again for a user revocation.

File metadata and file data are the two parts in the file stored in the untrusted server. The file metadata suggests the access control information containing a sequence of encrypted key blocks, each of which is encrypted under the public key of authorized users. Therefore, the file metadata size is proportional to the number of authorized users. The user revocation in the structure is anheadstrong issue specifically for large-scale sharing, since the file metadata wants to be

updated. NNL construction is used for efficient key revocation in their extension. Conversely, when a new user enters the group, the private key of each user in an NNL system needs to be recomputed, which may limit the application for active groups. Additional concern is that the computation overhead of encryption linearly increases with the sharing scale.

It leveraged proxy reencryptions to protected distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly reencrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the un-trusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks.

Scalable and fine-grained data admittance control scheme in cloud computing based on the KP-ABE technique is presented here. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager allots an access arrangement and the corresponding secret key to authorized ciphertext if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file reencryption and user secret key update to cloud servers. However, the single-owner manner may hinder the implementation of applica-tions with the scenario, where any member in a group should be allowed to store and share data files with others.

IV. PROPOSED SYSTEM

Mona, a secure multi-owner data sharing structure for active groups in the cloud to solve the challenges was presented. The main contributions of this present study contains:

1. Aproposed 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. This scheme is able to support active 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. Secure and privacy-preserving access control to users was presented here, which guarantees any member in a group to anonymously utilize the cloud resource.

4. Rigorous security analysis was provided to validate the efficiency of our structure in terms of storage and computation overhead. This was helped to solve the challenges presented above.

V.ALGORITHMS USED

Signature generation and signature confirmation were for the analysis.

VI. SYSTEM MODEL

The proposed system model can be explained with an example that a company uses a cloud to enable its staffs in the same group or department to share files and data.

The system model contains three different entities:

- Cloud Server,
- Group manager (i.e., the company manager), and a
- Large number of group members (i.e., the staffs)

Cloud Server is a bulkysource of resources which can be distributed to its customers as a service. The cloud service providers maintain the cloud servers who are all responsible for storing complex information in the cloud and offers whenever needed. It 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. Cloud server will not unkindly delete or adjust user data due to the fortification of data auditing arrangements, but will try to learn the content of the stored data and the identities of cloud users.

Group manager is aunitwhich is designed for storing, sharing and managing data files stored inthe cloud. Group manager is responsible for granting new users to access and increase cloud performance based on a request from them. Hetakes 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.

Registration-In this module anuser has to register first, then only he/she has to access the data base.

Login- In this module, any of the above mentioned person have to login, they should enter their confidentialpassword for loging in.

File Upload- In this module the owner uploads the fileinto database, with the help of this metadata and its contents, the end user has to download the file. The uploaded file was in encrypted form, only registered user can decrypt it. Even CSP can only view the encrypted file form.

Chart Creation-Here, the user can view the chart, which is actively developed by computing the size of the file.

File Download-The Registered users can download the file and can do updates. The modified file will be uploaded into cloud server by the user.

User Deletion-The admin can reject the user, so as that rejected user doesn't login and access the database.

SIMULATION

C programming language with GMP Library was used to simulate the Mona and the performance was studied.Three simulation components, namely client side, manager side and cloud side were used for this simulation. Both client-side and

manager-side simulation are conducted in a laptop with Core 2 T7250 2.0 GHzand the cloud-side process is conducted in machine that equipped with Core 2 i3-2350 2.3 GHz. An elliptic curve with 160-bit group order was choosed in this simulation to provide a competitive security level with 1,024-bit RSA.

VII. Conclusion

In the present study, design was made for a secure data sharing structure, Mona, for active groups in an untrusted cloud. In Mona, the user can share data with others in the group without enlightening identity privacy to the cloud. Moreover, Mona supports effective user revocation and new user joining.

References

[1] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), 257-265, 1991.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[7] 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.

[8] 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.