IJCAT International Journal of Computing and Technology, Volume 1, Issue 3, April 2014
ISSN : 2348 - 6090
www.IJCAT.org

An Efficient Approach to Share Data in Cloud with Multi-Owner Groups

[1] Tasmiya Sutana K, [2] Farhana Kausar

[1] M.Tech Student, Department of Computer Science and Engineering
Atria Institute of Technology, Bangalore, Karnataka, India

[2] Department of Computer Science & Engineering, Atria Institute of Technology
Bangalore, Karnataka, India

Abstract - Companies are into the cloud and provide services on it. The increasing popularity of cloud computing draws attention to its security challenges, which are particularly worsen due to resource sharing. Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose An Efficient Data sharing for multi-Owner dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. This paper addresses the security issues of storing sensitive data in a cloud storage service and the need for users to trust the commercial cloud providers.

Keywords **- Cloud computing, data sharing, privacy-preserving, encryption techniques, dynamic groups.**

1. 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 centers. 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 staffs in the same group or department 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. 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. First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable. Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner [3], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/ her part of data in the entire data file shared by the company. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management.

Several security schemes for data sharing on untrusted servers have been proposed [4], [5], [6]. In these approaches, data owners store the encrypted data files in

untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, Lu et al. Proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique [4], which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. Yu et al. [3] presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case, where any user is granted to store and share data.

1.1 Hall Marks of Cloud

On-demand self service, broadband network access, resource pooling, rapid elasticity are some of the essential characteristics of the cloud model. The cloud can be deployed for private, public, community or uses. Private cloud will be used by an organization and its customers, whereas public cloud is made available for public use. Community model is for a community of users having same mission/goal. Hybrid model of cloud shares the properties of any of the above models.

Shabeeb et al (2012) discussed about the cloud services. The cloud delivers its services in the form of software, platform and infrastructure. Costly applications like ERP, CRM will be offloaded onto the cloud by provider. They run at providers cost. Platform includes the languages, libraries etc. and the database, operating system, network bandwidth comes under infrastructure.

1.2 Security Issues

Trustworthiness of the cloud service provider is the key concern. The organizations are deliberately offloading their sensitive as well as insensitive data to cloud for getting the services. The cloud works on pay for use basis. If numerous requests are sent to a server on cloud by the DoS attacker, the owner of that particular cloud have more requests for process. Moreover, other users will be denied of the service which they request as the server on cloud is expending all its requests for serving the malicious DoS request. The situation will be more drastic if the attacker compromises some more hosts for sending the flood request, which is called DDoS.

Chonka et al (2011) discussed the variant forms of DDoS at-tack tools like Agobot, Mstream and Trinoo which are still used by attacker today. But, most attackers are more inclined to use the less complicated web based attack tools like Extensible XML-based Denial of Service (X-DoS) and HTTP-based Denial of Service (H-DoS) attack due to their simple implementation and lack of any real defences against them.

2. Overview

2.1 Denial-of-Service Attack

In computing, a **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

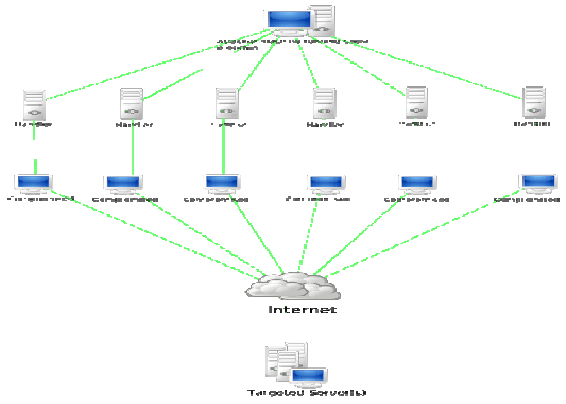

Fig. 1 Denial-of-service attack

Related Work

In Li et al. [1], proposed an Attribute Based Encryption (ABE) technique which allows Patient's Health Records (PHR) to be shared across various users in the field of medicine as well as for personal domain. This system consist two types of users: personnel users and professional users. Multiple security domains greatly reduce key management issues. Also, this system ensures high degree of patient privacy, supports user revocation at any time and also break-glass technique to access patient records in emergency scenarios. Here, data owner is free to change their access policies dynamically at any point of time.

In Wan et al. [2], proposed an alternative form of ABE called Hierarchical Attribute Set Based Encryption (HASBE) by extending Ciphertext Policy-ABE (CP-ABE). The proposed scheme could achieve scalability due to its hierarchical nature, also it is highly flexible. Fine grained access control in support to compound data

attributes. User revocation can be performed better than any other existing systems.

In [3], Yu et al. introduces a scalable and fine grained data access method in cloud by using Key Policy-Attribute based Encryption method in which the data owner can use any random key to encode the file, where the chosen random key is again encrypted along with a set of attributes using KP-ABE. Then, the group manager provides an access structure and decryption keys to the user. The ciphertext can be decrypted by the user if and only if the attributes satisfy the access structure assigned. To achieve user revocation, data owner needs to update all attributes and keys. Here single owner sharing does not allow multiple owner sharing and maximum utilization of cloud resources.

3. System Model and Design Goals

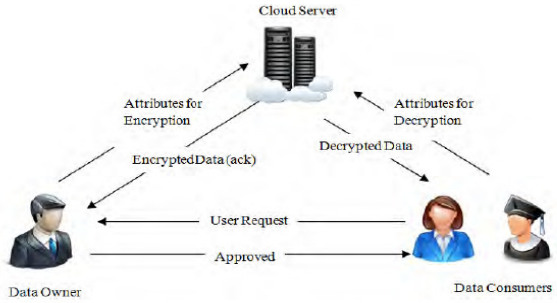

Fig.2: System Model

Cloud Server is a large repository of resources which can be delivered to its customers as a service. The cloud servers are maintained by cloud service providers who are all responsible for storing sensitive information in the cloud and provides whenever needed.

Data Owner is an entity who is going to store, share and manage data files stored in the cloud. He is also responsible for granting new users to access and improve cloud performance based on a request from them. Key management and distribution, monitoring of users, user revocation are other activities performed by data owner.

Data Consumers are the users of the system. They initially get registered with cloud system to become a part of cloud and to use services offered. Users can register with cloud system as Life Time User, and Guest.

3.1 Design Goals

Proposed system is designed to achieve the following goals. Each of them described briefly as follows.

Access control: Data Consumers including Data Owner can access the cloud if they have valid key. Unregistered members and revoked members are strictly prohibited from accessing the cloud. Challenging issues is to maintain confidentiality in dynamic membership. Because new user should able to decrypt the files while revoked users unable to decrypt shared files.

Anonymity and traceability: Anonymity guarantees flexible access to cloud without revealing real identities of user. Although anonymity provides protection to identity it poses some insider attack risks. Traceability allows identification of real identity of an inside attacker in case of any attack.

Efficiency: Efficiency of the proposed system can be explained as follows: Any user can store and share files with other users in the cloud. User revocation can be performed without disturbing remaining users. Remaining users don't need to update their private keys.

4. Proposed Scheme

4.1. Overview

Information storage and its secure sharing are more important and unavoidable processes that became a real life part of all individuals including both personal and professional uses. Many users are not interested to join and make an access to cloud service as it has security issues. So, a highly secured system with low complexity and key management issues is desired. Attribute Based Encryption technique can be used to design such a system which encrypts data files along with attributes relevant to the data files or user. The decryption process can be performed by using attributes and user's private key. User Revocation may be desirable, if the user performs malicious operations or his life time to access cloud services has been expired.

4.2 Techniques Used

Proposed system use a Technique called Attribute Based Encryption (ABE) is a public key cryptography which allows Data Owner to encrypt and decrypt his files by using set of attributes along with private key. For each user a dedicated access tree structure will be defined by using data attributes. When relevant attributes provided by user that satisfies the access tree structure then, decrypted file can be downloaded.

This algorithm takes security parameter k and set of attributes $U= \{1, 2 \ldots N\}$ of cardinality N. Also, defines bilinear group G of order m with a generator n. A bilinear mapping is defined as: $e: G \times G \rightarrow G1$. It returns Public Key P_k and system Base Key B_k as follows.

$P_k = \{X, Y1, Y2 \ldots YN$ (1)

$B_k = \{x, y1, y2 \ldots yN\}$ (2)

Where, Yi ε G and $y_i \varepsilon Z$.

ABE- Encryption algorithm takes Message *M*, Public Key *Pk*, and attribute set *A* as input which outputs Ciphertext *C* as follows:

$$C = (A, C', \{C_i\}_{i \in A}) \quad (3)$$

Key generation algorithm takes access tree *Y*, Base key B_k, and public key P_k which outputs user Private key S_k. Decryption algorithm takes Ciphertext *C* under attribute set *A*, secret key S_k for access tree *Y*, and public key P_k.

4.3. Scheme Description

My proposed system consists following entities and techniques:

System Setup: System initialization can be performed by forming a cloud architecture in which data owner creates an account with cloud server. Further, more users can join with data owner to share files. This is possible through making a request to data owner. During registration process users need to fill their personal information which will be evaluated by data owner to provide an approval for data access in cloud. Once, user got registered with the cloud system, he is free to access any file until life time expiry or revocation on the basis of request. Initially, Data Owner collects attributes relevant to the data file units and are encrypted, then uploaded to cloud server. Policy engine used in the system automatically runs and generates access structure of the data file. Also, generates user's public key. Once the access structure satisfies the attributes given by the user the decrypted file can be downloaded by them.

User Registration: After successful creation of cloud setup, users need to get registered with the system through user registration process. While registering, users need to submit their personal details for completion of registration process. But, the system guarantees Identity privacy. During registration process, user got unique identity *I* and access structure *T*. This generates secret key S_k for I. So that, S_k <- *Keygen(Pk,* B_k*)* . Data file *F* can be then encrypted by using *I*'s Public Key *Pk* to generate Ciphertext *C*.

User Revocation: User revocation is the process of removal of user from system user list which is performed by Data Owner. The system maintains Attribute History List (AHL) for each attributes. For the user to be revoked, his access structure is removed from AHL, so that they can't have more access to cloud.

File Upload: Before uploading files, Data Owner assign File identity *ID* to selected data files and then encrypts file using his public key *Pk*. Along with encryption attributes for encryption is added. *File Access:* Users can access data files if they have valid secret key. While accessing files, user's secret key is validated against access structure of the user. If it satisfies user's access structure, decrypted data file can be downloaded by Data Consumer.

File Deletion: This operation can be performed by Data Owners, if they no longer needed that files. For file deletion, Data Owner needs to provide File Identifier along with secret key. If owner's signature is verified successfully then cloud server successfully deletes the file with specified identity.

Dynamic Policy Updates: Data owner can update their data attributes for a particular file whenever needed to achieve more security and integrity.

Break-glass Access: In emergency situations, someone may need to access data files from cloud without contacting data owners. In such scenarios Break-glass access method can be used to get sensitive information. For example, Personal Health Records (PHR) of an individual may need in emergency. But, this access is only available to personal users such closely related persons.

5. Conclusion

In this paper, I have proposed sensitive information sharing by using Attribute Based Encryption technique which encrypts the data files and provides high security. As it has two types of user domains: public and private user domains, this system can be used to share both personal and professional information within a single system itself which considerably reduces maintenance and establishment charges along with guaranteed security. 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. More over, the storage overhead and the encryption computation cost are constant. The system supports Break-glass access that enables its personal users to access cloud data under emergency scenarios. Dynamic policy updates ensures more integrity and confidentiality. Also, the system is highly scalable and can support multiple users to register and access cloud services.

References

[1] Ming Li, Schuchen Yu, Yao Zheng, Kui Ren, Wenjing, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE Transactions on Parallel and Distributed Systems, vol.1, No.1, January 2013.

[2] Zhigu Wan, June Liu, Robert.H.Deng, "HASBE: Hierarchical attribute based solution for flexible and scalable access control in cloud computing",IEEE

Transactions on Information Forensics and Security, vol.7, No.2, April 2012.

[3] Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] Chenguang He, Xiaomao Fan, Ye Li, "Towrd ubiquitous healthcare services with anovel efficient cloud platform", IEEE Transactions on Biomedical Engineering, Vol.6, No.1, January 2013.

[5] Xuefeng Liu, Yuqing Zhang, Boyang Wang, Jingbo Yan, "Mona: secure multi-owner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, Vol.24, No.6, June 2013.

[6] 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.

[7] 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.

[8] 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.

[9] 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 Security Symp. (NDSS), pp. 29-43, 2005.

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

[11] 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

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

[13] 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.

Tasmiya Sultana K, Student of Atria Institute of Technology, Bangalore Pursuing M.tech Final Year. She received her B.E degree in Computer Science and Engineering from NDIT, Bangalore in 2012. She has received progressive success in various games and curricular activities. Her main research interests include network securities, Cryptography, Database Management, and Cloud Computing and learning with the upcoming new technologies.

Farhana Kausar Mtech (CSE), currently working as Assistant Professor in Atria Institute of Technology.