An Efficient approach to Store and Share Sensitive Information In Cloud

Ranjith.K,
M.Tech Student
Department of Information Technology
V.S.B Engineering College
Karur, India
mails2ranju@gmail.com

Abstract— Cloud computing has emerged as a new type of commercial paradigm in which resources are provided as services via network. The word Cloud is very popular and has drawn attention from both education and research. With the character of low maintenance and ease of use cloud services are attracted by even domestic users. However, this dramatic technology experiences many new challenges among which security and integrity are most common. Many algorithms have been put forward to resolve these issues. Even though, those issues still remains unresolved. This paper brings an efficient mechanism where the Data Owner can securely store his personal records in the cloud and can be shared among multiple users on a request basis. Attribute Based Encryption (ABE) is the background technique used to achieve this goal. As this system offers high level of scalability, it ensures efficient data sharing among multiple users based on user priority. Also, it ensures secure storage and integrity of decrypted data.

Keywords- Cloud computing, resource sharing, scalability, Encryption, Services.

I. INTRODUCTION

Cloud computing is a promising technology that emerged recently that has the character of low maintenance and ease of use when compared with similar technologies. With a short time span itself cloud got wide popularity among domestic users also. Improvements in Mobile internet paved a new way for cloud computing. Many new users are interested to join clouds, but due to some challenging issues, all of them are not fully trusted on cloud servers. Even though, cloud computing and its popularity increases day by day. Cloud Computing provides resources as services over internet which makes it different from others. Cloud offers three main types of services such as: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and many more has to come. Among Storage as a Service is widely using. As people rely more and more on the internet and cloud technology, security of their privacy becomes more challenging.

Many potential customers depend on cloud to store their Personal records and like to share those details on a request basis. Let us consider a real time scenario. A Professor allows his students and colleagues to share files stored in cloud. Those files may include internal assessment of students, his personal information, student's personal information, research details, other staff details etc. By utilizing cloud, students and other employees can get relevant information on a request basis. However, it poses some confidentiality risks. The cloud service provider or third party may not fully trusted by the users. A possible approach would be to encrypt entire data files before outsourcing in order to achieve more integrity. Still it is challenging due to following reasons. First, identity privacy is one of the challenging problems for cloud deployment. Without guarantee of identity privacy, users are unwilling to join the cloud group. Because, their real identity, other related information may vulnerable to an attack. Second, it is highly recommended that the entire cloud services should be fully used by all the users.

In this paper, it is focused on secure storage and sharing of personal files for all requested and authorized users with limited key management issues. It can be achieved by a technique called Attribute Based Encryption (ABE) in which each data files can be encrypted along with attributes relevant to the data file. During decryption, the user need to provide relevant attributes that satisfies the access structure of data file. In this paper, I have the following contributions:

1. I propose an Attribute Based Encryption (ABE) which allows encryption of data files with relevant attributes. Key management issues can be resolved by creating two types of users: public users and private users. Attributes for decryption will already distribute across users based on their category.
2. Proposed system supports multiple users and each user can communicate with each other through data sharing.
3. Data owners can dynamically update their policy, Break-Glass method to access data files in emergency situations are special features of the proposed system.

II. 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.

III. SYSTEM MODEL AND DESIGN GOALS

A. System model

The proposed system model can be explained with an example. Consider, a university maintains a cloud server, where professors can share their personal and academic files to his colleagues and students via cloud servers. The system model consist three entities: Cloud Server, Data Owner, and Data Consumer. System model is given in Fig.1.

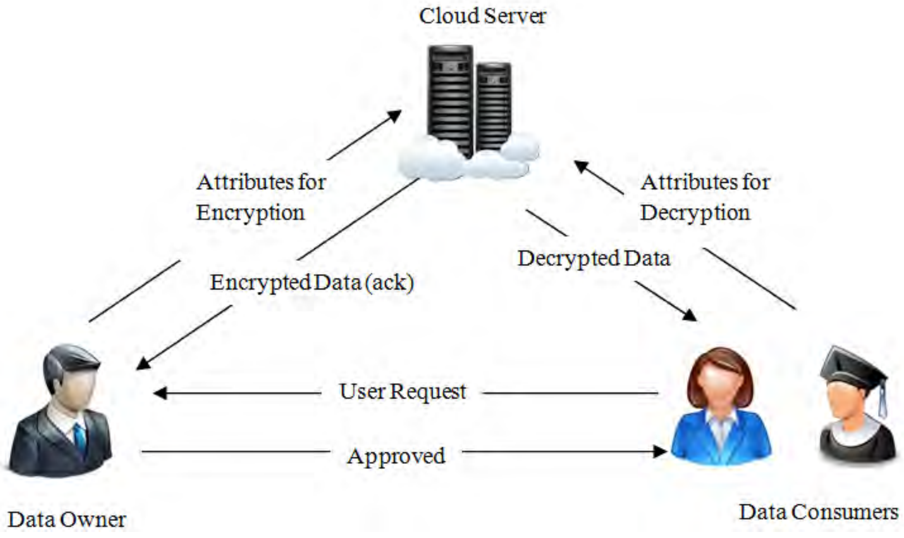

Fig.1: System Model

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.

B. 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.

Data confidentiality: Unauthorized users can't know the content of stored data including the cloud. One of the 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 incase 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.

IV. PROPOSED SCHEME

A. 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.

B. 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: $e: G \; X \; G \to G1$. It returns Public Key P_k and system Base Key B_k as follows.

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

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

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:

$$C= (A, C', \{C_i\}_{i \, \varepsilon A}) \qquad (3)$$

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.

C. 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.

V. CONCLUSION

In this paper, I have proposed novel 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. Moreover, 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 Didtributed 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.