Cloud Data Security Using Access Control Policy with Attributes

Swati Gore[1] Said Shubhangi[2], Sonal Patel[3]
[1] Assistant Professor, Department of computer Engineering, JCOE,Kuran, India
[2]Assistant Professor,Department of computer Engineering, JCOE,Kuran, India
[3]Assistant Professor,Department of General Science, JCOE,Kuran, India

Abstract:
One of the important and promising things today is securing data in cloud. This paper focuses the security issues of storing sensitive,important, personal data in a cloud storage service and the need for users to trust the cloud security providers. Here discussed a different cryptographic technique for cloud storage, based on an attribute-based access policy using asymmetric key cryptography. This system has many advantages. First, it provides protection and security to data stored in cloud. Second, it offers controlled data access to only those users which are satisfying particular access policy. Here we discuss many access policies for securing data.

Keywords*: Access Control, Access policy, Cloud Storage, Asymmetric Encryption*

1.Introduction

Cloud computing is a popular and easy service for storage. In cloud computing, the security and privacy of personal information is very important issue. Data outsourcing is a very popular trend for all companies to maintain their data online. Much of the times personal information is being turned over to another organization, suppose in another country, it is important to ensure that the information is safe and only the people who need to access it are able to access the intended information. There can be the risk that personal and sensitive information stored on a cloud can be used for other purposes illegally. Information stored in cloud could also be accessed by government agencies, domestic or foreign areas. For business purpose which are using a cloud service, it is important to understand the privacy and security policies of the provider. Cloud computing significantly reduces the cost and complexity of owning and operating computers and networks.If any organization makes use of cloud provider, it does not need to pay money on information technology infrastructure, or for buying a new hardware or software licenses. Cloud services are often customized and very flexible to use, and providers can provide advanced services that an individual company might not have the money or expertise to develop. For business applications using a cloud service, cloud computing could provide better protection of personal and sensitive information compared with current security and privacy. Cloud providers are always attracted to build privacy protections by different new technology. Although cloud computing not increases the risk that personal or secure information will be misused or exposed improperly, it could increase the scale of exposure. The storage of all data in a cloud provider can make that data more attractive to cybercriminals for misuse.

Organizations uses the Cloud in different service models such as SaaS, PaaS, and IaaS and deployment models such as Private, Public, Hybrid, and Community. There are a number of security issues in cloud and concerns associated with it but these issues fall into two broad categories: security issues faced by cloud providers organizations providing Software as a service, Software as a service, or Infrastructure as a service using the cloud and security issues faced by their customers that is companies or organizations who host applications or store data on the cloud. The responsibility is for both the things, first that the provider must ensure that their infrastructure is secure and second that their client's data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization wants to store its data or different applications on the public cloud, it cannot have physical access to the servers hosting its information. As a result, business sensitive and confidential data is having a risk from insider attacks. According to a recent Cloud Security report, insider attacks is one of the biggest threat in cloud computing. Therefore, it is necessary for Cloud Service providers to note that all background checks are conducted for employees who have physical access to the servers in the data centre. However data centres should be frequently monitored for different malicious activity.

Access control is very important term to provide access to only valid and authorised users. Providing access is ability to do something with a computer resource such as using, changing, or viewing. Access control is the means by which the ability is explicitly enabled or restricted in some way usually through physical and system-based controls. There are different access control methodologies [7].

1) **User based Access control**- It contains a list of users called as**access control list** (**ACL**), is a list of permissions along with an resources. An ACL decides which users and system processes are given access to resources, and also what operations are allowed on given objects.

2) **Role-based access control,** access control are based on the roles that individual users have as part of an organization. Users are provided with roles such as doctor, nurse and manager. The process of providing roles should be based on a well analysis of how an organization operates and should include input from users in an organization. Access rights are managed by role name, and the use of resources is restricted to individuals authorized with a particular associated role. For example, in a hospital system the role of doctor can include operations to perform diagnosis, medical prescription, and some laboratory tests, and the role of researcher can be restricted to gathering anonymous clinical information for studies. The use of roles to control access can be an effective means for developing and enforcing enterprise specific security policies, and for streamlining the security management process.
3) **Attribute-based access control** (ABAC) defines a new access control methodology whereby access rights are provided to users through the use of policies which combine attributes together known as access policy. The policies can use different type of attributes such as user related attributes, resource related attributes, environment related attribute etc. Attribute values may be set valued or atomic valued depend on application. Set valued attributes can have more than one atomic values. Atomic valued attributes contains only one atomic value. Attributes are compared to static values or to one another thus enabling relation-based access control. This system uses attribute based access control scheme, for granting access to valid users.

2. Literature Survey

The concept of attribute-based encryption (ABE) has been proposed by Sahai and Waters [3]. ABE is considered as a generalization of identity based encryption [4] (IBE), where the encryption is based on some identity of user. ABE is more efficient than IBE. In an ABE system, the plaintext is encrypted with a set of attributes to get ciphertext. The KDC that is Key distribution centre, which possesses the master key, provides different private keys to users after authenticating the attributes they possess. Thus, these private keys are provided along with the set of attributes each user possessed. In its simplest form, a user can decrypt a cipher text if and only if there is a match between the attributes of the ciphertext and the user's key. For example, user A has the attributes "role = doc" and "age > 18". Now user B encrypts a message using the attributes ("role = student" AND "age > 18"). User A can decrypt the message as she satisfies both attributes. User B encrypts another message using the attributes ("role = professor" OR "role = staff"). User A cannot decrypt the message as he/she does not satisfy the policy. The workings of the actual ABE schemes are a little different from the above examples, but they give the good idea of using that schemes.
There are two important types of ABE.

1. Key Policy ABE (KP-ABE)
2. Ciphertext Policy ABE (CP-ABE)

Goyal et al. [5] introduced the idea of KP-ABE systems and Bethencourt et al. [6] introduced the idea of CP-ABE systems. Let's try to understand the idea behind these two variants using diagrams.

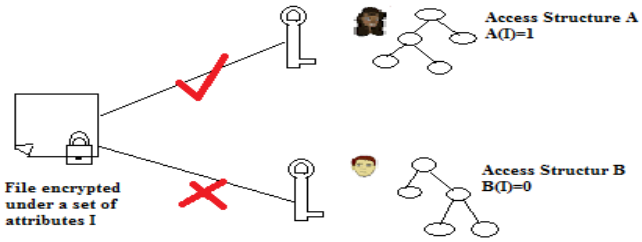

Figure 1. KP-ABE

As shown in the above diagram, in KP-ABE[5], user A encrypts a message with the help of a set of attributes. It defines an access structure, which is a access tree of the policy that user A should satisfy. User B and user C tries to decrypt the message. The attributes user B has satisfy the access structure and hence he/she can derive the key and decrypt the document. The attributes user C has do not satisfy the access structure and therefore cannot derive the key to decrypt the message. The main key idea here is that the key is associated with the policy using an access structure.

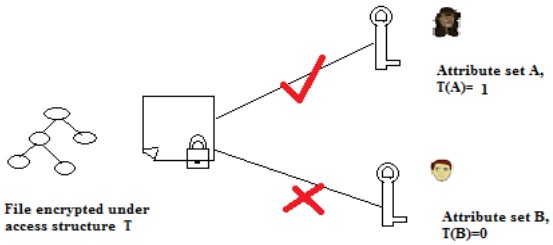

Figure 2. CP-ABE

As shown in the above diagram, CP-ABE[6] reverses the role of encryption and key derivation. The encryption is associated with an access structure which is constructed using the same access policy. Key generator simply issues private keys for the attributes users have. If users with their attributes satisfy the access structure defined by owner, they can decrypt it. The second scheme is closer to encryption found in open systems as the ciphertext is associated the some access policy.

3. System architecture

The architecture is decentralized, meaning that there are several KDC's for key distribution. There are three different types of users, a creator, a reader and writer. Creator receives a token from the trustee (shown in fig 4), who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. For example, these can be servers in different parts of the world. A creator after validating the token to one or more KDCs, receives keys for encryption/decryption and signing (shown in fig 5). The message is encrypted using the access policy. The access policy provides rights to who can access the data stored in the cloud. The creator decides on a claim policy, to prove his/her authenticity and signs the message using this claim. The ciphertext along with signature is sent to the cloud. The cloud verifies the generated signature and stores the ciphertext in the cloud. When a reader wants to read the information on cloud, the cloud sends ciphertext and not actual information. If the user has attributes matching with access policy, he/she can decrypt and get original message. Writing process is similar as file creation. By assigning the verification process to the cloud, individual users are relived from time consuming verification process. When a reader needs to read data in the cloud, it tries to decrypt data in ciphertext form using the secret keys it receives from the KDCs. If user satisfy sufficient attributes matching with the access policy defined, then he/she can decrypt the information stored in the cloud. Access policy can be changed on regular basis to provide more security. Algorithm for encryption and decryption used is Paillier Cryptosystem and for signature generation and verification SHA.

Sothis system consist of four different modules
1. Trustee
2. KDCs
3. Users
4. Cloud storage

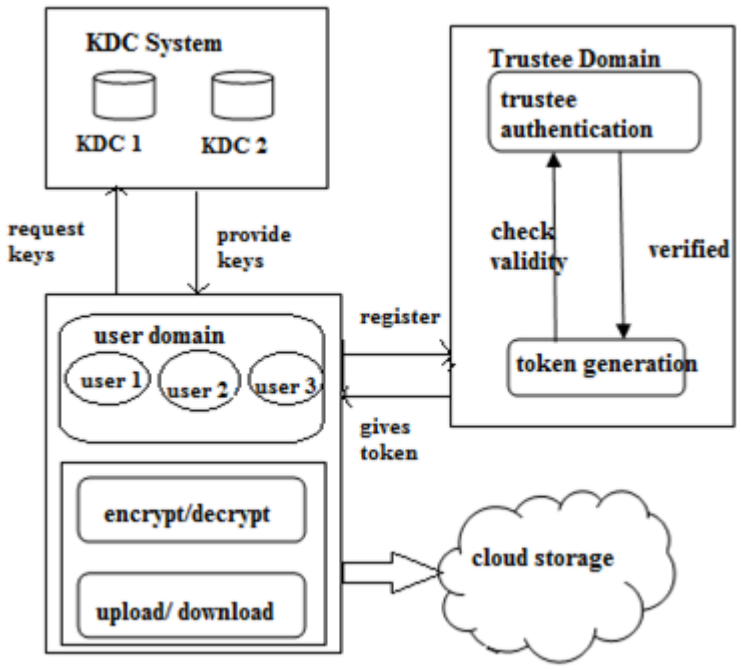

Figure 3. System Architecture

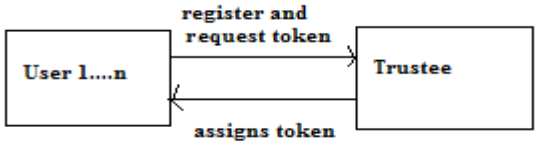

Figure 4 Trustee

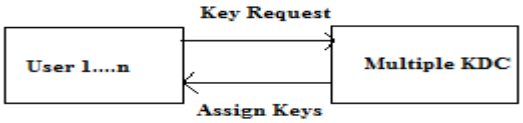

Figure 5. Multiple KDCs

4.Real Time Examples

Consider the example which explains how system can be used. Suppose a law student in university X want to show some reports about some malpractices by authorities of university X to other law student of university X, all the professors of university X research chairs of other universities in the country. She/ He wants to remain unknown form all this members while showing these reports of malpractices. Access control is important here as only authorized users can have access the data. It is also important point that information shown comes from reliable source. For this reason he/she also sends a claim message which states that he/she Is a law student or Is a student counselor or Professor at university X. The tree corresponding to the claim policy is shown in Fig. 6. The leaves of the tree consist of attributes and the intermediary nodes consist of Boolean operators.

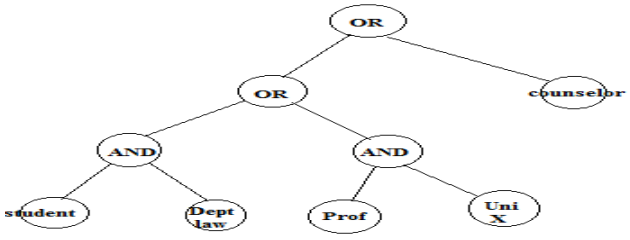

Figure 6. Access policy

In this example the attributes are Student, Prof, Dept Law, Uni X, Counselor. The above claim policy can be written as a Boolean function of attributes as

((Student AND Dept Law) OR (Prof AND Uni X)) OR (Student Counselor).

5. Results

This system generates a graph for each file stored on cloud by comparing time required for uploading and downloading using DES(symmetric key encryption) and Paillier(asymmetric key encryption) algorithm. Comparison of results so obtained by DES and paillier algorithm are shown in fig 7 (graphical representation).

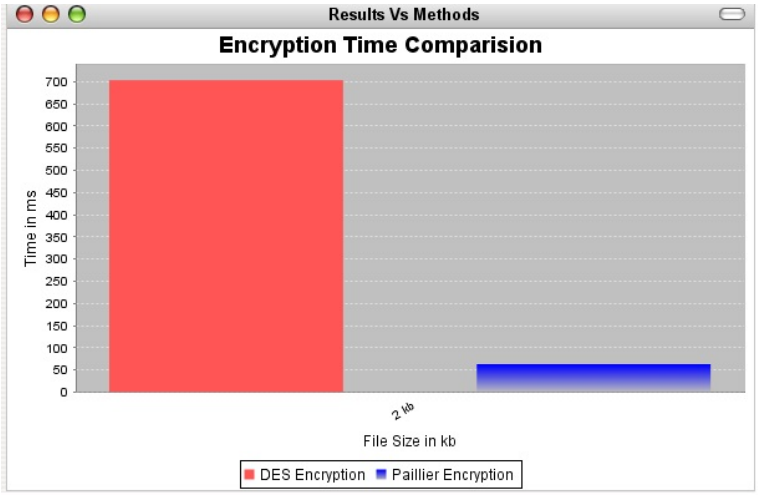

Figure 7. Graph showing comparison with DES algorithm

6. Conclusion

This paper proposes a privacy preserving cloud storage access control scheme that addresses security, authentication problems in the cloud. Many applications can use this system like medical centers, social networking sites where user can store data securely and can share with selected groups of people. This system uses homomorphic encryption which is computationally complex and requires less encryption/decryption time than symmetric key algorithm like DES.

References

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr. June 2012.

[3] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptolog(EUROCRYPT), pp. 457-473, 2005.

[4] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[5] 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, pp. 89-98, 2006.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[8] Jianwei Chen, Huadong Ma "Privacy – Preserving Decentralized Access control for cloud storage System" Proc. 2014 IEEE 7th International Conference on Cloude Computing.

[9] Swati Gore, ShyamraoGumaste,"Accessing Storage in Cloud using Access Policy" ,Global Journal of Engineering Science and Reasearchers.