International Journal of Research Studies in Electrical and Electronics Engineering (IJRSEEE)
Volume 2, Issue 1, 2016, PP 1-5
ISSN 2454-9460 (Online)
www.arcjournals.org

Controlling data access in cloud based on Multiple Level Attribute-set-based Encryption

Rohan Shrivastava
Department of Electronics Engineering
Shah and Anchor Kuttchi Engineering College
Chembur, Mumbai, Maharashtra
Rohanshrivastava.98@gmail.com

Prof. Asha Durafe
Department of Electronics Engineering
Shah and Anchor Kuttchi Engineering College
Chembur, Mumbai, Maharashtra
Ashachaskar17@gmail.com

Abstract: *Cloud computing is one of the latest technologies that is much talked about these days. In the IT world cloud computing is considered as a revolutionary technology which has been built by consolidating the already existing techniques such as grid computing, virtualization, and cryptography. Apart from having a number of advantages, cloud computing is still struggling with some security issues. System security is one of the major roadblocks for the sustainability of cloud in the future. Since the introduction of cloud in the current world the work is continuously being done for the security issues. A number of techniques have already been deployed to overcome these security concerns and still people are working to improve the security of cloud based systems. These schemes are mainly classified as Access control policies and Attribute based Encryption schemes. But all these schemes are still facing the problem of expressibility. One more constraint is that they only work for systems where the data owner and the service provider are in the same trusted domain. Apart from this these policies are also short of flexibility in attribute management and lacks scalability in dealing with multiple-levels of attribute authorities. The primary focus of our work is to overcome these limitations in the policies. Our aim is to provide securable and flexible access control which will be authenticated properly. This will help to maintain the data securely. In this paper we proposed a ML-ASBE scheme which will overcome all the limitations of the existing system. This will also deal with collusion resistance and decreases the complexity of computation.*

Keywords: *Cloud security, Attribute set based encryption, Access control policy*

1. INTRODUCTION

Cloud computing is one of the most emerging technologies in modern world. In a simple language we can define cloud computing as a centralized system which can be used for the purpose of data storage, data processing and data transfer. Cloud is a technique that is a collaboration of multiple already existing technologies. Cloud is managed by the cloud service providers and it is provided to the users who have registered for the service. Cloud equips its client with a number of facilities such as flexibility, scalability, pay-as-you-go and infrastructure. Apart from all these it is cost effective system. Cloud computing has combined advantage of all the technologies like virtualization, cryptography and grid computing [4]. But on the other side of the coin due to collaboration of different technologies it also inherits the problems related to the core technologies involved in it [6]. For example virtualization is the heart of cloud computing. So all the security issues related to virtualization is automatically attached with the cloud computing. Similarly the issues related to other technologies involved in cloud are also attached with the cloud. The deployment model of cloud is mainly classified into three categories. These are public, private and hybrid cloud. Private cloud is deployed at the organization level and deals with the security of the data confidential to the organization. Therefore it is very important to ensure the full security of the data. No organization or even an individual wants their data to get compromised. So to avoid any security breach cryptographic techniques are used. Cryptography is a technique in which the data is encoded in a different form to protect it from hackers. But now day's different algorithms are present to decode the data. So even encrypted data is not secured enough. The primary objective of our work in this paper is of information security by presenting a proposal for secure access control with authorization. In the past various access control schemes were proposed to achieve the secure data access [5][1][2]. These schemes are having limitations in terms of flexibility in attribute management, lacks scalability in dealing with multiple-levels of attribute authorities [11][2]. They also have constraints that the data

owner and the service provider should be in the same domain. Through our proposed system we can achieve scalability as well as flexibility by Multiple-level-based attribute set based encryption (ML-ASBE).

2. RELATED WORK

2.1. Access Control

To ensure the physical as well as information security, it is very important to apply the selective restriction of access to a place or other resource. This unit of security is termed as authorization unit.

Generally in order to store the data securely it is encrypted and then saved on the common servers that can be used by multiple users. Then authorization is done to ensure that only the genuine users can access the data. The requirement of this system is a defined PKI (public key infrastructure).There is a requirement of a key management system to manage the keys. There are various disadvantages of the PKI systems [8]. When the number of users increases the complexity of the system also goes up. It becomes cumbersome to manage such a large number of keys. So in other words we can say that it is not optimum for scalability. Apart from scalability PKI systems are also not efficient in flexibility. The system is not much flexible to handle the ever changing requirement. There is one more concern. There is also a case of user revoking their data. When user wants to quit the system then he revoke his data. At this time re-issuing of keys are done which becomes a great overload on the system. Also the process of re-encryption is not effective in PKI system. In all the PKI systems there is a basic limitation that the data owner required to be online every time. While user is offline the process of key distribution, encryption and re-encryption of the data is not possible in this system. There are a number of schemes for access control that are vital for the purpose of security[10][11][9][8]. But in the cloud the relation among the users and resources is dynamic. Also cloud service providers and clients are generally not in the same domain. Therefore security system based on identity cannot be used in open environment. Users are generally not identified by some predefined identities. They are recognized by the attributes or characteristics.

2.2. Attribute Based Encryption

As can be understood from the name itself Attribute based encryption uses the attributes of the user for the purpose of encryption as well as decryption. Encryption can be defines as a process that converts the data into some coded version to hide it from unauthorized users. ABE is mainly classified into two categories. First one is Key-policy ABE (KP-ABE)[5].Basically there are two important parts of any policy. These are cipher text and private key. In KP-ABE the set of attributes is attached with the cipher text and private key is attached with access policy which forms a key policy pair. In order to decrypt the data the user's attribute must satisfies the key-policy pair. But as can be seen there is a limitation that the data owner cannot decide regarding which user can decrypt the cipher text. User can only choose a set of attributes that control the access of cipher text. Also the access structure is monotonic due to which this policy is not able to exclude the users who cannot access the data. There is a possibility that some other user which is having the same attribute can access the data. In other words we can say that there is lack of expressibility in this policy.

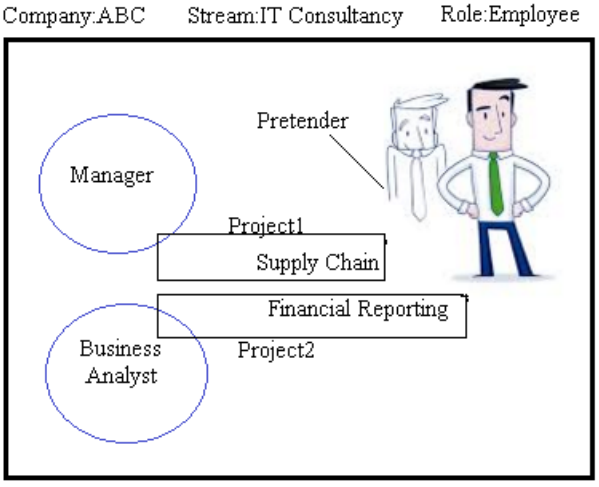

Fig1. *Collusion Problem CPABE*

The second policy is the CP-ABE [2]. This is just opposite to the KP-ABE. In Cipher text–policy ABE, we attach with the cipher text the access policy and set of attributes is associated with the private key. This is the reason due to which it is closer to real life scenario. Example: Assuming, Ashish is a employee of company TPS. In that company he belongs to two different projects. In one project he is playing the role of manager and in another project he is business analyst. Thus Ashish is playing multiple roles in the company and have different attributes. So Ashish is having the following key structure of depth 2.

{Company: ABC Domain: IT consultancy Role: employee,

{Project: Supply chain Role: Manager},

{Project: Financial reporting Role: Business analyst}}

So as we can see that different values can be allocated for the same attribute. These different values form various sets of attributes. So there should not be a case in which Ashish can combine can combine Role: business analyst with Project: Supply chain and can access the data. So there is a chance of security breach as a user who is not authorized to access the data is can manipulate the system. So a person who is having multiple attributes can combine them and thus he can access the data of different users. So a system in which this combination is not possible cannot be implemented with CP-ASBE. To overcome this issue we are proposing the system of ML-ASBE. In ML-ASBE we are keeping a constraint that the attributes can be combined only in the same set. So user cannot combine the values of attributes belonging to different sets, due to which this unauthorized access becomes impossible.

Attribute based encryption is generally classified into two categories. One type of ABE is having the Access Structure that is monotonic in nature and another one is that which is having a non-monotonic Access Structure. In Monotonic Access structure ‘AND gate’, ‘OR gate’, or ‘k out of N’ threshold gate is generally used. On the other hand the Non-Monotonic Access structure make use of Monotonic Access structure and additional ‘NOT gate’.

In ML-ASBE, the attributes are present at different levels [1][8]. In other words we can say that the attributes are categorized according to the levels that they occupy. The levels are decided according to the access control structure. These multiple levels scheme provides the depth to the system and thus helps in maintaining a fine grained access control. Each and every level is associated with certain number of attributes. The attributes at a higher level can be used to reach the lower level attributes but not vice-versa use is possible. In the below example attribute 1 is at the first level, attribute 2 and 3 at second level and attribute 4 and 5 at third level. So from attribute 1 second level attributes can be derived but from attribute 2 or 3, attribute 1 cannot be derived. This is an example of depth 3.

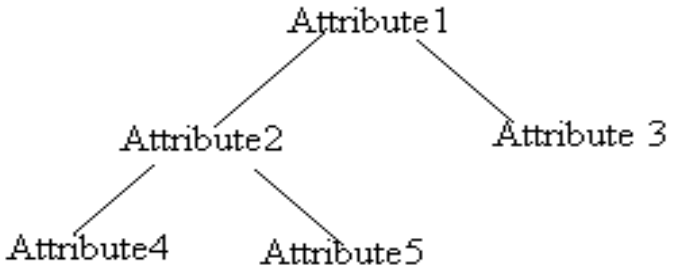

Fig2. *ML-ASBE based authority*

3. PROPOSED SYSTEM

As we saw in the earlier sections that existing works are having a lot of limitations. So to overcome the issues of existing work we propose our new approach that is Multiple Levels Attribute Set Based Encryption (ML-ASBE).Our work is the extension for the Cipher texts – Policy Attribute Set Based Encryption (CP-ASBE or ASBE) and Hierarchal –ASBE[10]. The propose work will be able to solve the problems related to access control and scalability. Here we will be using the following parameters to solve the access control problem: Cloud services provider, data owners, data consumers, domain authorities and trusted authority.

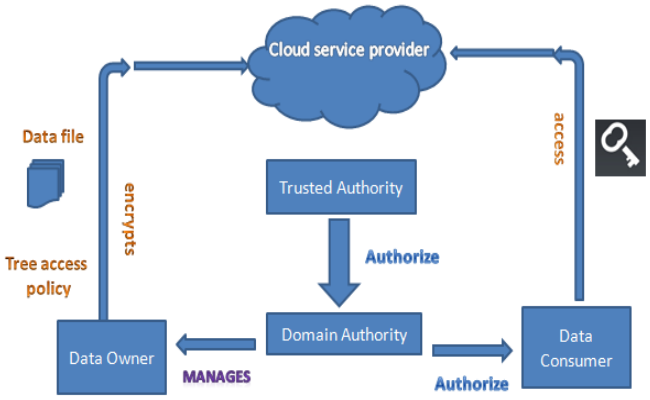

Fig3. *ML-ASBE system architecture*

Trusted Authority: The job of the Trusted Authority is to do the system set up, top level domain authority grant, create domain authority and key update. While doing the system set up trusted authority creates the public key and master key. These keys are generated according to the attribute sets range or depth of domain services. A unique id is generated for a domain. After that trusted authority validates that the domain is genuine or not. If the domain is valid then only the unique id will be provided to the domain and it is created. Then the domain authority will able to create the sub domain and the users.

Domain Authority: The whole system is divided into different regions or parts. Each region or part can be termed as a domain or domain authority. Domain Authority will be able the create the new sub domain authority and new users. Each user belongs to a particular domain and is controlled by the same domain. This concept gives the depth to the access tree structures. The domain or sub domain authority will be able to create the users. These users can be either data owner or data consumer.

Data Owner: As we mentioned earlier there are two types of users. As the name suggests Data owner is that user who owns the data. Basically he is the client for which CSP handles the data. Data owner is able to create file, encrypt file, re-encrypt file, file upload permissions. To create a file data owner uses a unique id to encrypt the file. After encryption data owner set tree access structure and after that it finally store the file in the cloud. There is also an option to re-encrypt the file for the owner.

Data Consumer: The second type of user is the data consumer. These are basically the users who use the data published by the data owner in the system. The data consumer is also handled by the domain or sub domain authority. In order to access the data data owner requires a key. This key is provided to data consumer by the domain authority. The process flow starts with the data consumer sending request to the domain authority for accessing a file. After this domain authority checks that this is a valid user or not. If the user is authorized then domain authority grants the key to user. To access the data they need a key to access the file on the cloud, the key is provided by the domain authority. This key contains the information of the file, decryption key value and access structure of the file. So with the help of this key user can access the data published by the data owner.

Cloud Service Provider: The cloud service provider or CSP is the one who provides all the services to the user. It is the responsibility of the CSP to manage a cloud that provides the data storage services.

4. CONCLUSION

In this paper, we proposed the ML-ASBE scheme to achieve more scalable and flexible system which is having a fine-grained access control in cloud computing. The ML-ASBE scheme that we are proposing is able to overcome the limitations of already existing systems. It overcomes a very basic limitation that the data owner needs to remain online always. In our proposed user need not be online always. By applying the multiple levels in the system a fine grained access control is achieved.

REFERENCES

[1] Zhiguo Wan ; Key Lab. for Inf. Syst. Security, Tsinghua Univ., Beijing, China ; Jun'e Liu ; Deng, R.H. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing 2013.

[2] AttributeBasedEncryption,https://www.cs.utexas.edu/~bwaters/publications/papers/cp-abe Bobba, Himanshu Khurana and Manoj Prabhakaran

[3] Xingbing Fu and Zufeng Wu:Ciphertext Policy Attribute Based Encryption withImmediate Attribute Revocation for Fine-Grained Access Control in Cloud Storage ,IEEE 2013

[4] Ling Leng, Lin Wang, "Research on cloud computing and key technologies," 2012 International Conference on Computer Science and Information Processing (CSIP)

[5] IEEE transactions on information forensics and security, vol. 7, no. 2, april 2012 , 743hasbe: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing zhiguo wan, jun'e liu, and robert h. deng, senior member, IEEE.

[6] Kevin hamlen, Murat Kantarcioglu, Latifur khan and Bhavani Thuraisingham, Security Issues for cloud Computing,Technical report UTDCS-02-10FeB 2010

[7] Kevin hamlen,Murat Kantarcioglu, Latifur khan and Bhavani Thuraisingham, Security Issues for cloud Computing,Technical report UTDCS-02-10FeB 2010

[8] Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption Rakesh, University of Illinois at Urbana-Champaign {rbobba,hkhurana,mmp}@illinois.edu,July 27, 2009

[9] D.F. Ferraiolo and D.R. Kuhn (1992) "Role Based Access Control" 15th National Computer Security Conf. Oct 13-16, 1992, pp. 554-563 the original paper that evolved into the NISTRBAC mode

[10] The Public Key Infrastructure Approach Security https://docs.oracle,.com/cd/B10501_01/ network. 920/a96582/pki.htm

[11] Dan Boneh, Matthew Franklin: Identity-Based Encryption from the Weil Pairing, Appears in SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003. An extended abstract of this paper appears in the Proceedings of Crypto 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229, Springer-Verlag, 2001