Improving Data Sharing Security in Cloud Computing

Ibtissam Ennajjar
Lirosa laboratory, Faculty of Sciences
Abdelmalek Essaadi University
Tetuan, Morocco
ennajjar.ibtissam@gmail.com

Youness Tabii
Lirosa laboratory, Faculty of Sciences
Abdelmalek Essaadi University
Tetuan, Morocco
youness.tabii@gmail.com

Abdelhamid Benkaddour
Lirosa laboratory, Faculty of Sciences
Abdelmalek Essaadi University
Tetuan, Morocco
Ham.benkaddour@yahoo.fr

***Abstract*— Cloud computing has emerged as a new computing paradigm where all IT infrastructure can be outsourced and working as on premise. It offers numerous advantages both for customers and providers and especially at the cost level that is typically low compared to buying your own resources, configuring and managing them. One of the tremendous services is the data sharing and the data storage. Customers can outsource a huge number of data in cloud without having to worry about the capacity of memory or the size of data as cloud system manage the scalability of servers needed to contains your data. Cloud is flexible, scalable and dynamic so don't worry about capacities. But, one of the predominant concerns encountered in cloud and that can change your mind about this nice view, is security. As more and more sensitive data and personal information placed in the cloud, security concerns grow up. Building trust in providers it is not an easy task with an amount of outages and threats declared since adoption of cloud computing. In this paper, we give a new approach to enhance the security of data outsourced in cloud environment. The approach is based on Cipher Policy- Attribute Based Encryption (CP-ABE) scheme. It consists of encrypting data before outsourcing it and controlling the access to it by encryption. Our method offers scalability, flexibility and fine grained access control of data in cloud. Also, it provides an efficient manner to share confidential data on cloud servers.**

Keywords—cloud computing; security; data; attribute based encryption; access control; data sharing

I. Introduction

Over the last decades, computing world has seen considerable changes. The combination of many technologies like virtualization, utility computing, web, clustering, networks and others make the computing environment suitable to create new paradigms to encourage the use of technology and enhance its efficiency. Also, the advent of various internet-connected devices and the high level of internet consumption over the world lead IT experts to wonder: why not open up the world of computing to a wider variety of applications and enjoy its numerous goods and services by giving access through any internet connection. So, we can imagine a delivery of computing as a service rather than as a product. When we use the word computing, it includes the cost of CPU, the memory, the storage, network and other software required to create the ecosystem needed by an IT infrastructure. So they try to bring together several existent technologies to come out with a new complex computing concept called cloud computing. Cloud computing gives the client cost efficiency, unlimited storage, scalability, mobility, accessibility and several other advantages to ensure that the work is done correctly and safely. The mechanism consists of a migration from owned resources to shared resources in which client users receive information technology services, on demand, from third-party service providers via the Internet.

This said, it is true that cloud computing offers potential benefits but that should not blind cloud consumers to its main risk and disadvantage which is security and privacy. Moving sensitive and personal data in public cloud may be a bad deal, unless having a great trust in all parties interacting in cloud environment. The entire IT infrastructure is under the control of the cloud provider. Also, it must not be forgotten that when this infrastructure is created, it inherits all security concerns that the distributed systems and virtual resources encounter in different levels like: data leakage, data remanence, hypervisor security issues [1], network penetration, insecure SSL trust configuration, injection flaws like SQL, Distributed Denial of Service attacks and others.

Additionally, the centralization of resources and the shared data environment make the cloud provider a very tempting target. Hackers, malicious insiders and malicious tenants can be source of various man-made threats. So, the menace of accessing user's sensitive information stored in cloud system is very high.

Access control is a fundamental feature of information security, since it consists of granting users authorization to access different resources. Improper or malicious operation can cause very potential damage to an individual or organization. Guarantying good access control mechanism in cloud can have a hugely positive impact on secrecy, integrity and availability of data and then on cloud environment security [2, 3, and 4].

Surely there are many kinds of Access control models and schemes which have demonstrated their effectiveness, but with the particularity of cloud infrastructure, it has become necessary to strengthen earlier models and explore new approaches to meet changes introduced by cloud computing in organizations' infrastructure.

In this paper we will propose a new cryptographic access control approach for cloud storage. It is based on Ciphertext Policy - Attribute Based Encryption scheme. We propose a new method of applying CP-ABE scheme in cloud architecture with the target of improving security of shared data in cloud area.

The paper is structured as follows: section II introduces many cryptographic access control techniques used to secure data in outsourced servers. Section III presents cloud security needs in term of data sharing and access control and exposes our approach. Finally, Section IV discusses the conclusion and perspectives.

II. Cryptographic Schemes of Access Control

Since cloud storage is full with personal and sensitive data shared by consumers, the higher complex that obsesses cloud users is how to keep data confidential and accord access only to authorized individual or group. Ensuring data confidentiality and a fine grained, scalable and flexible access control system still a preeminent concern in cloud area, what makes researchers looking continuously of new methods to secure data sharing and data access over cloud computing. Confidentiality can be reached by encrypting data before outsourcing it. And to secure access control, there are many encryption schemes for access control that are proposed to access encrypted data in untrusted servers. In this section we will expose some of them that can be helpful to ensure security in cloud.

Starting with traditional public key encryption (PKE) and why it is in some situations qualified as outdated. Applying PKE in cloud can be an acceptable manner to strengthen confidentiality of data but the scalability of cloud and a huge number of users make this technique impractical. In PKE process, the data owner needs one public key for each user to encrypt data what makes handling keys difficult and it impacts storage computation capacity [6]. Moreover the loss of private key or its theft can be a big dilemma [7].

Consequently, researchers shift their attention towards other techniques like Attribute Based Encryption (ABE). First researches about attribute-based encryption were presented by Sahai and Waters in [8] as a new type of Identity-Based encryption (IBE) scheme. In ABE system the encryption scheme is based on a set of attributes that contribute in the generation of the private and public keys. For instance, if you want to share a document or any data with a specific group of users you have first to specify a number of attributes that describe this group then you encrypt your data based on those attributes. When users want to see data they must provide a private key with a set of attributes that is close to ones used in encryption. In this way, ciphertext can be encrypted to a group of users and not just for one as in traditional public key encryption. What make ABE scheme suitable with distributed systems and then with cloud environments. Also data can be stored in untrusted server as they are encrypted and the access to it is controlled by encryption. But as any new technique, ABE had also its drawbacks and limits due to the lack of expression of attributes described as not very expressive, what limits its applicability to larger systems [8].

What was a wake-up call for researchers to extend it and produce other concepts based on it such as KP-ABE, CP-ABE, HABE, HASBE and MAABE. Here we give a little description of each one of these listed schemes.

A. *Key-Policy Attribute Based Encryption (KP-ABE)*

The Key-Policy Attribute Based Encryption (KP-ABE) scheme was proposed in 2006 by Goyal et al based on ABE [8]. Encrypted data in KP-ABE is combined to a set of attributes that describe the user who has the authorization to decrypt data. To do a matching between user and data, user's private key must contain an access policy to decrypt data when ciphertext attributes match the policy. For example, a ciphertext with attributes {Computer Science AND Student} and an access structure {Computer Science AND (Student OR Professor)} can be combined and then the data can be visible to the user.

B. *Ciphertext- Policy Attribute Based Encryption (CP-ABE)*

Ciphertext- Policy Attribute Based Encryption (CP-ABE) was proposed by Bethencourt et al based on ABE and KP-ABE [9]. The main idea of this scheme is not very far from KP-ABE, there is just a difference at level of the incorporation of the access policy. In CP-ABE, the access policy is in the encrypted data (ciphertext) and the set of descriptive attributes are associated with the user's private key, unlike KP-ABE where the access policy is included in user's private key and the set of attributes characterizes the ciphertext. The user can decrypt data if only if his private key's attributes correspond to the access structure. Let us take, for instance the following access structure combined with the ciphertext {Computer Science AND (Professor OR Student)}. If user's private key has a set of attributes {Computer Science AND Student} OR {Computer Science AND Professor}, then the user can access to decrypted data, what don't work with other combinations. See Figure2.

C. *Hierarchical Attribute Based Encryption(HABE)*

In 2011, Wang et al. proposed a hierarchical attribute-based encryption scheme composed of a hierarchical identity-based encryption scheme (HIBE) and a ciphertext-policy attribute-based encryption scheme [11]. This scheme uses the property of hierarchical generation of keys in HIBE scheme to generate keys. It was proposed to be applied in cloud storage where the cloud storage service, data owner, the root authority, the do- main authority, and data users are the actors in this process. The role of cloud storage service is to let a data owner can store data and share data with users. The role of data owner is encrypting data and sharing data with users. The role of the root authority is generating system parameters and domain keys, to distribute them. The role of domain authority is managing the domain authority at next level and all users in its domain, to delegate keys for them. Besides, it can distribute secret keys for users. And users can use their secret keys to decrypt the encrypted data and obtain the message [5].

D. Hierarchical Attribute Set Based Encryption(HASBE)

Zhiguo Wan et al proposed HASBE scheme in [12]. The HASBE scheme extends the ASBE scheme to handle the hierarchical structure of system as shown in figure 1. The trusted authority is responsible for managing top-level domain authorities. It is root level authority. For example, for an enterprise, employees are kept in the lowest domain level and above that there is department and above that there is top level of domain we call it as a trusted domain. It generates and distributes system parameters and also root-master keys. And it authorizes the top-level domain authorities. A domain authority delegates the keys to its next level sub-domain authorities. Each user in the system is assigned a key structure. Key specifies the attributes associated with the user's decryption key. HASBE scheme was proposed for scalable, flexible, and fine grained access control in cloud computing. It consists of hierarchical structure of system users by using a delegation algorithm to CP-ASBE.

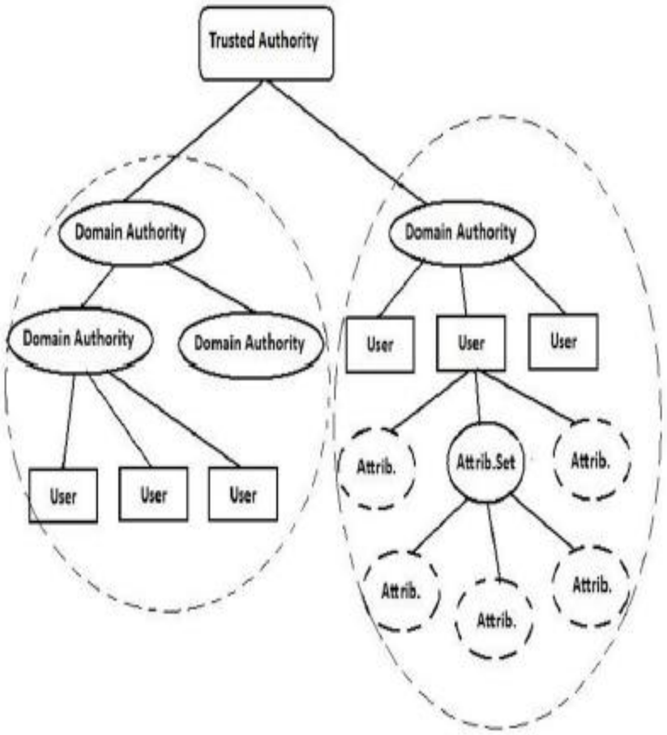

Figure1: HASBE Model

E. Multi AuthorityAttribute Based Encryption(MAABE)

Multi-authority ABE system was proposed by Chase. It consists of many attributes authorities and many users [13]. There are also a set of system wide public parameters available to everyone (either created by a trusted party, or by a distributed protocol between the authorities). A user can choose to go to an attribute authority, prove that it is entitled to some of the attributes handled by that authority, and request the corresponding decryption keys. The authority will run the attribute key generation algorithm, and return the result to the user. Any party can also choose to encrypt a message, in which case he uses the public parameters together with an attribute set of his choice to form the ciphertext. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

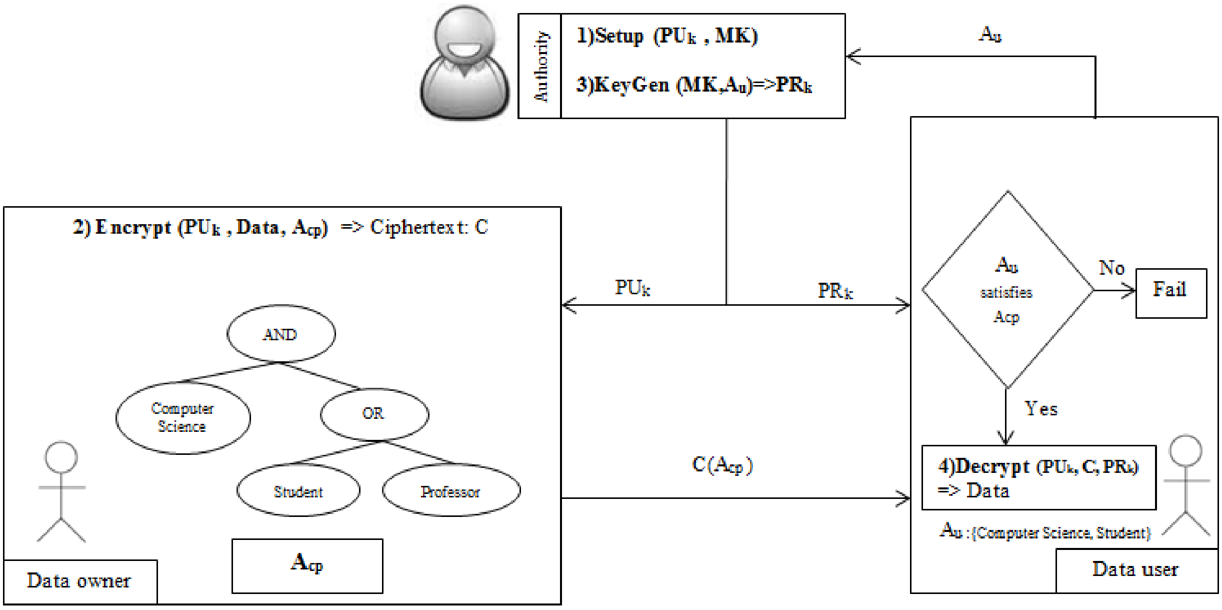

Figure2: CP-ABE process

III. Proposed Approach

In cloud computing, there are many different issues related to the security of data. When we outsource our data to untrusted servers managed by a third party, it is very recommended to encrypt it before, and having a control to who can access to it. The existing systems don't usually provide an efficient mode of security that can resist against possible attack of clouds like collusion attack, DDOS attack and others that can lead our data to be stolen or lost. Furthermore, designing a useful and effective manner of securing the data shared in cloud is based on applying a number of instructions that suit with the cloud distinction. We try here to give some of them that we will take in consideration in our system architecture. Then we give the scenario of our model.

A. *System instructions*

1. The data owner should to encrypt its data before outsourcing it and identifying who can access the ciphertext.
   - ➢ This instruction can be realized by incorporating CP-ABE in our model. The owner will create the ciphertext by combining data, public key and the access control structure where he defines the correspondent user.
2. Separate the entity distributing keys from the cloud provider.
   - ➢ The owner must choose a third party entity (authority) to manage the publication of security keys that is different from the cloud provider. It is recommended to be sure that there are no communication between cloud provider and the authority who manage keys.
3. The access control must be fine grained.
   - ➢ Users sharing the same access structure can have different access rights.
4. The system should be scalable as cloud it is.
   - ➢ The system has to work efficiently even if the number of users increases.
5. The system should manage the user accountability.
   - ➢ The key must be with the appropriate user. Untruthful user can share the secret key with unauthorized one.
6. The system must manage the revocation of user.
   - ➢ If a user changes his profile or quit the system the access accorded to him must be denied.
7. The system has to be a collusion resistant.
   - ➢ The combination of attributes in order to satisfy the access policy is not legal.
   - ➢ CP-ABE and other encryption schemes have the possibility to prevent collusion attack.

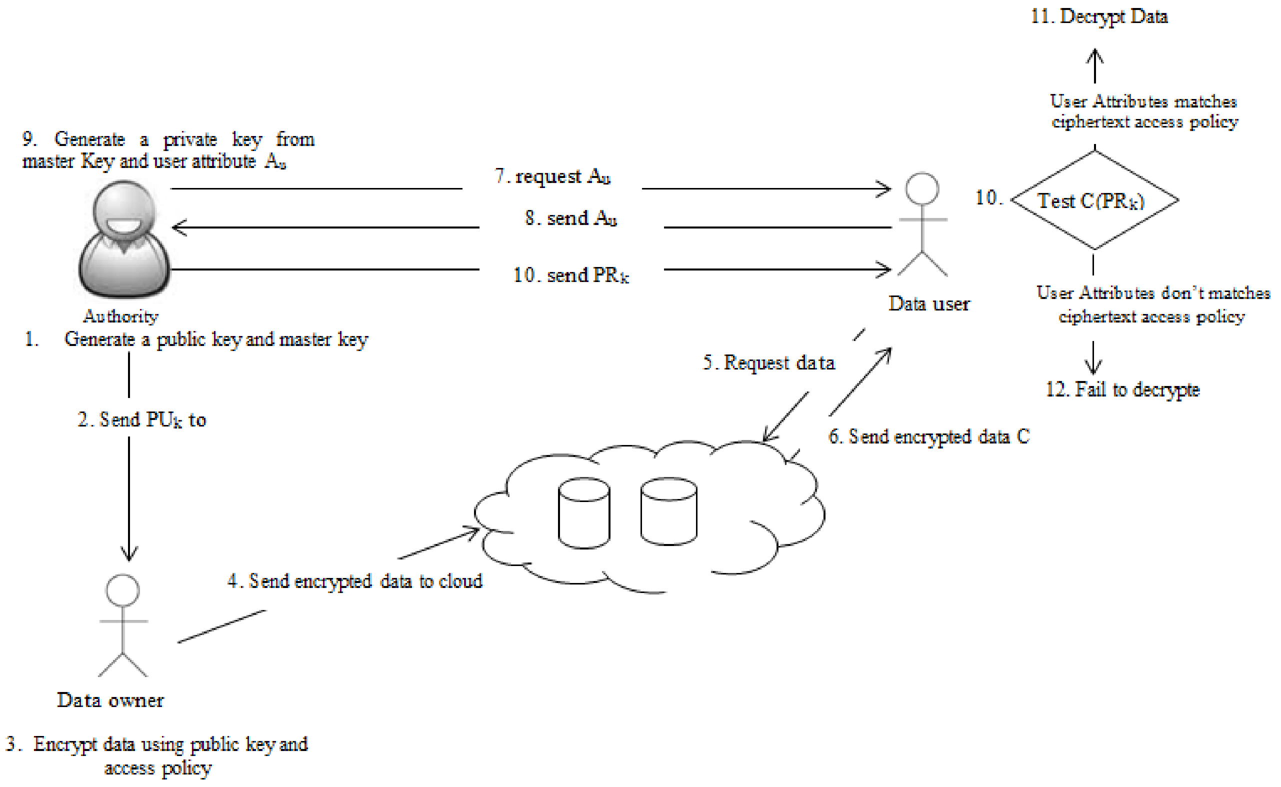
11. Decrypt Data
User Attributes matches ciphertext access policy
9. Generate a private key from master Key and user attribute A_u
7. request A_u
8. send A_u
10. send PR_k
10.
Test C(PR_k)
Data user
Authority
1. Generate a public key and master key
User Attributes don't matches ciphertext access policy
5. Request data
12. Fail to decrypte
2. Send PU_k to
6. Send encrypted data C
4. Send encrypted data to cloud
Data owner
3. Encrypt data using public key and access policy

Figure 3 : proposed architecture

B. *Proposed model*

Our model consists of applying the CP-ABE scheme in cloud computing by introducing a third party that manages keys distribution independently from the cloud provider.

As represented in figure 3, the data owner first asks the authority to generate the master key and the public key by which he will encrypt its data. Then he encrypts data using the public key combined with the access policy that he wants to put on data to specify who can access it and so who can decrypt it. After that he sends encrypted data to cloud for storing it. When a user asks for data, he receives encrypted one. To decrypt it he must send its access attributes to the third party, which generates a private key according to the master key of data and the user's attributes and sends it to user. If private key contains access attributes that matches the access policy incorporated in cipher data then data will be decrypted. Otherwise, user can't see it and the operation fails.

CONCLUSION

On this paper we present a new approach to enhance security when sharing data over cloud computing that consists of using Ciphertext Policy Attribute Based Encryption scheme to ensure fine grained and flexible access control system. We give the architecture of our model with the aim to design it and construct a specific security model based on mathematical modules in future. Our model represents an extension of the use of CP-ABE scheme in cloud storage. In our future work we tend to detail more our architecture, construct a more expressive security scheme and try to handle many CP-ABE limits like user revocation and full delegation with the purpose to provide an efficient encryption scheme designed to cloud environment.

REFERENCES

[1] S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing" Journal of Network and Computer Applications pp. 1–11, 2011.

[2] S. rehman, R. Gautam," Research on Access Control Techniques in SaaS of Cloud Computing" , SSCC 2014, CCIS 467, pp. 92–100, 2014.

[3] R.Aluvalu, L. Muddana, "A Survey on Access Control Models in Cloud Computing", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1, pp 653-664, 2015.

[4] N. Meghanathan, "Review of access control models for cloud computing" Computer Science & Information Technology (CS & IT), pp 77-85, 2013.

[5] C. Lee, P. Chung, M. Hwang ," A survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013.

[6] M. Rasseena, G R. Harikrishnan, "Secure Sharing of Data over Cloud Computing using Different Encryption Schemes An overview", International Journal of Computing and Technology, Volume1, Issue 2, pp 8-11, 2014 .

[7] A.Sahai, B.Waters, "Fuzzy Identity-Based Encryption", Advances in Cryptology V EUROCRYPT, vol.3494 of LNCS, pp. 457-473, 2005.

[8] V.Goyal et al., "Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data", ACM conference on Computer and Communicatios Security(ACM CCS),2006.

[9] J. Bethencourt et al., "Ciphertext-Policy Attribute-Based Encryption", IEEE Symposium on Security and Privacy(SP'07),2007.

[10] S.Gokuldev, S.Leelavathi, "HASBE: AHierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing", International Journal of Engineering Science and Innovative Technology(IJESIT), Volume 2, Issue 3, May 2013.

[11] G.Wang, Q.Liu, J.Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Serrvices" , in Proceeding of ACM conference Computer and Communications Security (ACM CCS), Chicago, IL,2010.

[12] WAN, Zhiguo; LIU, June; and DENG, Huijie, Robert. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud ComputingIEEE Transactions on Information Forensics and Security (TIFS), pp. 743-754, 2012.

[13] Melissa Chase. Multi-authority Attribute Based Encryption. In TCC, volume 4392 of LNCS, pp. 515–534. Springer, 2007.