Secure Service Provisioning in Cloud using Attribute Based Encryption

Phyo Thandar Thant, Thinn Thu Naing
University of Computer Studies, Yangon
phyothandarthant.ptdt@gmail.com, thinnthu@gmail.com

Abstract

Today, cloud computing has become important research area and more enterprises are adopting the Cloud based strategy for their businesses. In this case, user access control is the primary concern for cloud users and cloud service providers. User accesses are key factor in determining how much they have to pay to the service provider (SP). So, SP needs to deploy secure access control mechanism in provisioning the services to the users.

In cloud computing, services are delivered as web services using SOAP message format. And to protect service provisioning to unauthorized users, many security access control mechanisms have been proposed.

This paper intends to examine how Attribute Based Encryption mechanism used to control users' accesses among cluster based private cloud and data center private cloud in our university campus. By using this mechanism, service providers can ensure that secure services are delivered only to the authorized users.

1. Introduction

Security is the number one issue in cloud computing. In cloud computing, unlike in a secure network where access from outside the network can be completely prohibited, anybody can access the services from anywhere over the web. For secure cloud computing, companies must adopt effective and efficient technologies to prevent unauthorized access to their services. Cloud provides services as web service so cloud services are in the form of SOAP messages. For this reason, we need to consider the security of service information in SOAP message as well as access controls of authorized users by using effective cryptographic techniques.

Attribute-Based Encryption (ABE) is a novel mechanism for the realization of access control policy in a cryptographic way. Generally, there are two kinds of ABE schemes, key policy ABE (KP-ABE) and ciphertext policy ABE (CP-ABE) schemes. In the KP-ABE schemes [5], ciphertexts are associated with sets of attributes and users' secret keys are associated with access control policies. In the CP-ABE schemes [1], each ciphertext is associated with an access control policies. The access control policies are described with the attributes and thus CP-ABE is closely related to Role-Based Access Control [10] and Attributed Based Access Control [11]. But, cloud computing is a dynamic environment and as a result of this, stable role structure is not suitable for this environment. So it's natural for us to choose ABE in order to ease the private key management and enable the service providers to exert the access control policy defined by themselves over service requestors.

The rest of paper is organized as follows: section 2 lists related work, section 3 describes the theory Background, section 4 gives information about the proposed system and section 5 provides conclusion and future work.

2. Related Work

Attribute-Based Encryption (ABE) was first proposed by A. Sahai and B. Waters [9] with the name of Fuzzy Identity-Based Encryption, with the original goal of providing an error-tolerant identity-based encryption scheme that uses biometric identities. V. Goyal, et. al., enhanced the original ABE scheme by embedding a

monotone access structure into user secret key. The scheme is called Key-Policy Attribute-Based Encryption (KP-ABE) [5]. They also proposed Ciphertext-Policy Attribute Based Encryption (CP-ABE. In CP-ABE ciphertexts are associated with an access structure. That approach allows encrypted data can be kept confidential even if the storage server is untrusted. Both KP-ABE and CP-ABE are able to enforce general access policies that can be described by a monotone access structure. In [8], R. Ostrovsky, et.al., proposed an enhanced KP-ABE scheme which supports non-monotone access structures. [4] M. C . Gorantla et. present a generic one-round AB-AKE protocol that satisfies AKE-security notion. The protocol is generically constructed from any EP-AB-KEM that satisfies chosen ciphertext security. J. Bethencourt, et. al., [2] proposed the first CP-ABE construction with security under the Generic Group model. In [3], L. Cheung and C. Newport presented a CCA-secure CP-ABE construction under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. In [3], the CCAsecure scheme just supports AND gates in the access structure. Towards proposing a provably secure CP-ABE scheme supporting general access structure, V. Goyal, et. al., [6]. Aside from providing basic functionalities for ABE, there are also many works proposed to provide better security/privacy protection for ABE. S Luo et. al., [7] examined how attributes-based encryption might be used to provide privacy and security for web services and intend to implement ABE in web services. The evaluation demonstrate that ABE is efficient and feasible with desirable performance in web services. In 2010, S. Yu [12] proposed three enhancements in ABE: how to revoke users with the help of untrusted users, about key abuse attacks and issue of privacy preserving.

3. Theory Background

3.1.Attribute Based Encryption

A. Sahai and B. Waters [9] first introduced the public-key cryptography attribute based encryption (ABE) for cryptographically enforced access control. In ABE both the user secret key and the cipher-text are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the ciphertext and user secret key. Different from traditional public key cryptography such as Identity-Based Encryption [1], ABE is intended for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. To enable more general access control, V. Goyal, et. al., [5] proposed a key-policy attribute-based encryption (KP-ABE) scheme i.e., a variant of ABE. The idea of a KP-ABE scheme is as follows: the ciphertext is associated with a set of attributes and each user secret key is embedded with an access structure which can be any monotonic tree access structure. A user is able to decrypt a ciphertext if and only if the ciphertext attributes satisfy the access structure embedded in her secret key. In the same work, Goyal et. al., introduced the concept of ciphertext policy attribute-based encryption (CP-ABE). CP-ABE works in the reverse way of KP-ABE in the sense that in CP-ABE the ciphertext is associated with an access structure and each user secret key is embedded with a set of attributes.

In ABE, KP-ABE and CP-ABE, the authority runs the algorithm *Setup* and *Key Generation* to generate system *MK*, *PK*, and user secret keys. Only authorized users are able to decrypt by calling the algorithm *Decryption*.

3.2. Key Policy Attribute Based Encryption

A KP-ABE scheme consists of the following four algorithms.

Setup : This algorithm takes as input a security parameter κ and returns the public key *PK* as well as a system master secret key *MK*. *PK* is used by message senders for encryption. *MK* is used to generate user secret keys and is known only to the authority.

Encryption : This algorithm takes a message *M*, the public key *PK*, and a set of attributes γ as input. It outputs the ciphertext *E*.

Key Generation : This algorithm takes as input an access structure *T* and the master secret key *MK*. It outputs a secret key *SK* that enables the user to decrypt a message encrypted under a set of attributes γ if and only if γ matches *T*.

Decryption : It takes as input the user's secret key *SK* for access structure *T* and the ciphertext *E*, which was encrypted under the attribute set γ. This algorithmoutputs the message *M* if and only if the attribute set γ satisfies the user's access structure *T*.

3.3. Ciphertext Policy Attribute Based Encryption

In CP-ABE, each user is associated with a set of attributes and his/her secret key is generated based on these attributes. When encrypting a message, the encryptor specifies the threshold access structure for his/her interested attributes. Message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP ABE technique, encrypted data can be kept confidential and secure against collusion attacks.

A CP-ABE scheme consists of four algorithms:

Setup : This algorithm takes as input a security parameter κ and returns the public key *PK* as well as a system master secret key *MK*. *PK* is used by message senders for encryption. *MK* is used to generate user secret keys and is known only to the authority.

Encrypt : This algorithm takes as input the public parameter *PK*, a message *M*, and an access structure *T*. It outputs the cihphertext *CT*.

KeyGen : This algorithm takes as input a set of attributes γ associated with the user and the master secret key *MK*. It outputs a secret key *SK* that enables the user to decrypt a message encrypted under an access structure *T* if and only if γ matches *T*.

Decrypt : This algorithm takes as input the ciphertext *CT* and a secret key *SK* for an attributes set γ. It returns the message *M* if and only if γ satisfies the access structure associated with the ciphertext *CT*.

3.4. Definition of Access Structure

Let $\{P_1,P_2,\ldots,P_n\}$ be a set of parties. A collection $A \subseteq 2^{\{P1,P2,\ldots,Pn\}}$ is monotone if $\forall B, C$: if B $\in$ A and B $\subseteq$ C then C $\in$ A. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of $\{P_1,P_2,\ldots,P_n\}$, i.e., $A \subseteq 2^{\{P1,P2,\ldots,Pn\}} \setminus \{\emptyset\}$. The sets in A are called the authorized sets, and the sets not in A are called the unauthorized sets [2].

At a mathematical level, access structures are described by a monotonic access tree, where nodes of the access structure are composed of threshold gates and the leaves describe attributes. AND gates can be constructed as n-of-n threshold gates and OR gates as 1-of-n threshold gates. Furthermore, there may be more complex access controls such as numeric ranges by converting them to small access trees.

3.4.1. Access Tree

Access tree T . Let T be a tree representing an access structure. Each non-leaf node of the tree represents a threshold gate, described by its children and a threshold value. If num_x is the number of children of a node x and k_x is its threshold value, then $0 < k_x \leq num_x$. When $k_x = 1$, the threshold gate is an OR gate and when $k_x = num_x$, it is an AND gate. Each leaf node x of the tree is described by an attribute and a threshold value $k_x = 1$.

3.4.2. Satisfying the Access Tree

Let T be an access tree with root r. Denote by T_x the subtree of T rooted at the node x. Hence T is the same as T_r. If a set of attributes γ satisfies the access tree T_x, denote it as $T_x(\gamma) = 1$. $T_x(\gamma)$ can be computed recursively as follows:

If x is a non-leaf node, evaluate $T_x(\gamma)$ for all children x' of node x. T_x (γ) returns 1 if and only

if at least k_x children return 1. If x is a leaf node, then $T_x(\gamma)$ returns 1 if and only if $att(x) \in \gamma$.

3.5. Simple Object Access Protocol (SOAP)

Clouds offer services as web services. Generally, web service requests are sent in the form of SOAP messages.

SOAP is an HTTP-XML based protocol that enables applications to communicate over the Internet, by using XML documents called SOAP messages. SOAP is compatible with any object model, because it includes only functions and capabilities that are absolutely necessary for defining a communication framework. Thus, SOAP is both platform and software independent, and any programming language can implement it. SOAP supports transport using almost any conceivable protocol. For example, SOAP binds to HTTP and follows the HTTP request-response model. SOAP also supports any method of encoding data, which enables SOAP based applications to send virtually any type of information (img, obj, doc, etc) in SOAP messages.

3.5.1. Structure of SOAP Message

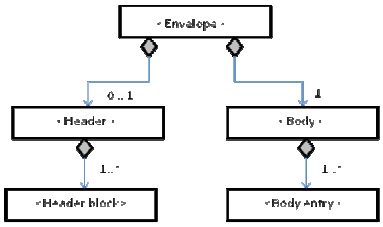

Figure 1. Structure of SOAP message

SOAP is versatile message format. It is based on message exchanges and messages are seen as envelopes. Envelope consists of an <Envelope> element containing an optional <Header> and a mandatory <Body> element. The contents of these elements are application defined. A <Header> contains blocks of information relevant to how the message is to be processed and pass information that is not for the application but for the SOAP engine. The SOAP <Body> is where the main end-to-end information conveyed in a SOAP message must be carried.

3.5.2. Securing the SOAP Message

Header entries can modularly extend the message for purposes such as authentication, transaction management and payment as well as end-to-end message confidentiality using XML Encryption and end-to-end message integrity using XML Digital Signature. The body of a SOAP message contains application-specific data for the intended recipient of the message. To insert security in SOAP message, it is needed to add security related information in SOAP header and some related encrypted information in SOAP body.

4. System Design of Proposed System

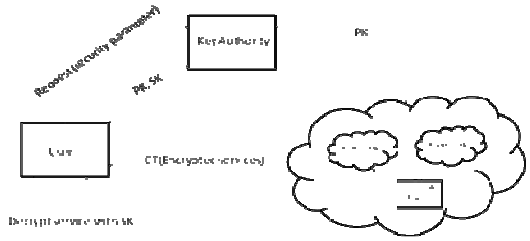

Figure 2. System design

4.1. Overview of Proposed System

Step 1: User → Security parameter → KA

Step 2: KA → PK, SK → User

KA → PK → Service Provider

Step 3: SP → Encrypted web services. CT → User

CT = Encrypt(PK,Reply,T)

Step 4: User decrypt service reply

Reply=Decrypt(SK,CT,γ)

In this system, there are two private clouds called private cloud-1 which stores text files, image files, multimedia files, dataset files etc., to give data as a service to its users and private cloud 2 provides application as a service.

User access controls are defined according to the corresponding attributes of the users. When user want to access a service, firstly users have to request to the key authority. Key Authority make some computation using the attributes that the user sent as a request and gives public parameter PK and private key SK back to the user. Then the key authority also gives PK to the service provider. After that service provider encrypt the service response using PK and access control policies called access control structure (T) that are defined in advance. And send the encrypted web service (CT) to the user via SOAP message. After receiving the encrypted response, user decrypt that response with his/her private key, SK. At this time, the user can only accessible to the service if the attributes in SK of user satisfies the access structure information in CT. In this way, service provider provide secure provisioning of services to the authorized users.

4.2. Components of Proposed Scheme

4.2.1. Policy Formulation

Attributes Definition

i. Subject (S)
ii. Resource (R)

$SA_k\ (1 \leq k \leq K)$ $RA_m\ (1 \leq m \leq M)$

ATTR(s), ATTR(r) are attribute assignment relation for subject s and resource r.

ATTR(s) $\subseteq SA_1 \times SA_2 \times \ldots \times SA_k$

ATTR(r) $\subseteq RA_1 \times RA_2 \times \ldots \times RA_m$

In the most general form, the policy rule that decides on whether a subject can access a resource r is a Boolean functioin of s, r :

Rule X: can access(s,r) ← f(ATTR(s),ATTR(r))

4.2.2. Key Authority/ Key Management

In the proposed scheme, identities are viewed as sets of attributes and let the value d represent the error tolerance in terms of minimal set overlap. When an authority is creating a private key for a user, the authority will associate a random d-1 degree polynomial, q(x) , with each user with the restriction that each polynomial have the same valuation at point 0, that is q(0) = y.

For each of the attributes associated with a user's identity, the key generation algorithm will issue a private key component that is tied to the user's random polynomial q(x). If the user is able to "match" at least d components of the cipher with their private key components, then they will be able to perform decryption,

i.e., a ciphertext created using identity ω can be decrypted only by a secret key $\acute{\omega}$ where $|\omega \cap \acute{\omega}| \geq d$.

However since the private key components are tied to random polynomials, multiple users are unable to combine them in anyway that allows for collusion attacks[9].

4.2.3. SOAP Security

In this paper, we intend to implement ABE to ensure fine grained access control of cloud services' customers. Current approaches focus on traditional encryption methods such as Data Encryption Standard(DES), AES and so on. In order to implement ABE in SOAP message security, we need to insert ABE mechanism in SOAP header portion. The figure below shows example of how ABE is used in controlling the web services accesses via SOAP messages.

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV=".">
<SOAP-ENV:Header>
   <wsabe>
<EncryptionMethod Algorithm="cp-abe">
    <KeyInfo>
    <PubKey>  ...  </PubKey>
    </KeyInfo>
```

```
    </wsabe>
</SOAP-ENV:Header>
 <SOAP-ENV:Body>
<EncryptedData>
     <CipherData>
          <Policy>  ...  </Policy>
          <CipherValue>  ...</CipherValue>
     </CipherData>
</EncryptedData>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Figure 3. Insertion of ABE access control mechanism in SOAP message

As can be seen from the figure, <wsabe> portion take part in controlling the user accesses and encrypted information is in <SOAP-ENV:Body> portion. The encrypted ciphertext is within <CipherValue> tag. In this way, all service requests are delivered only to the authorized users and the confidentiality of service information is achieved.

5. Conclusion and Future Work

This paper proposes secure service provisioning in cloud using ABE. ABE provides normal encryption and extra access control function. ABE is more efficient, flexible and suitable than other cryptographic techniques and may be a lightweight security solution for web services[7]. Cloud services are also delivered as web services. Thus, proposed system intends to implement ABE based security in provisioning cloud services to the users. With this approach, confidentiality of service information can be achieved even if control is lost over the service reply during transmission.

Future work lies in implementing the system in the private-cloud systems in our university campus and proving the effectiveness of our proposed system.

References

[1] D.Boneh and M. Franklin. "Identity-Based Encryption from The Weil Pairing." *In Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001.*

[2] J.Bethencourt, A. Sahai, and B. Waters. "Ciphertext-Policy Attribute-Based Encryption." *In Proc. of SP'07, Washington, DC, USA, 2007.*

[3] L.Cheung and C. Newport. "Provably Secure Ciphertext Policy ABE". *In Proc. of CCS'07, New York, NY, USA, 2007.*

[4] M.C.Gorantla, C Boyd, and J. Manuel G Nieto. "Attribute-based Authenticated Key Exchange". *In Proceedings of the 15th Australasian Conference, ACISP July 2010, Macquarie Graduate School of Management, Sydney.*

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data". *In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.*

[6] V. Goyal, A. Jain, O. Pandey and A. Sahai, "Bounded Ciphertext-Policy Attribute based Encryption", *In Proc. of ICALP'08, Reykjavik, Iceland, 2008.*

[7] S. Luo, J. Hu and Z. Chen " Implementing Attribute-Based Encryption in Web Services*". In 2010 IEEE International Conference on Web Services.*

[8] R.Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with non-monotonic access structures". *In Proc. of CCS'06, New York, NY, 2007.*

[9] A.Sahai and B. Waters. "Fuzzy Identity-Based Encryption." *In Proc. of EUROCRYPT'05, Aarhus, Denmark, 2005*.

[10] R.S.Sandhu, E.J.Coyne, H.L.Feinstein and C.E.Youman, "Role-based access control models." *IEEE Computer, 29(2):38-47,February 1996.*

[11] E.Yuan, J.Tong, "Attributed Based Access Control (ABAC) for Web Services". *In: Proceedings of the IEEE International Conference on Web Services (ICWS'05), Orlando, Florida, July 2005.*

[12] S. Yu "Data Sharing on Untrusted Storage with Attribute-Based Encryption." A Dissertation Submitted to the Faculty of the Worcester Polytechnic Institute, July 2010.