International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 10, December- 2012

Attribute Based Signature Scheme For Attribute Based Encrypted Data In Cloud

[1] Mr. Rupesh Vaishnav
[1]P.G. Student, Marwadi Education Foundation Group of Institutes, Rajkot, Gujarat.

Abstract

Storing data on untrusted storage like cloud space makes secure data sharing a challenging issue. To address that issue cryptographic methods are usually applied. Cryptographic methods have to achieve system scalability, data access control, key management etc. Attribute-based encryption (ABE) is one of the methods that is more preferable for storing data with encryption on cloud. This survey explains Key-policy attribute-based encryption (KP-ABE), Cipher-policy attribute-based encryption (CP-ABE) that are types of ABE, and covers Attribute-Based signatures (ABS) with variants ring signatures, group signatures, mesh signatures. ABS provides guarantees of unforgeability and signer secrecy.

1. Introduction

To keep data confidential to data servers the data owner encrypts data before upload. User access is granted by possessing the data decryption key(s). When this kind of cryptographic-based access control scheme provide security protection on data, there are also several major challenges pertained to the scheme design [8]. To gain privacy of data from cloud service provider and other non related nodes encryption techniques are key source that provides relevant security. Network security consists of number of methods to achieve cryptographic security. One of them is most popular method is Attribute-based encryption (ABE).

ABE is recently invented one-to-many public-key cryptography, has the potential to enforce the fine grained access policies for large-scale systems [7]. ABE does not provide assurances towards the authenticity of the data. Attribute Based Signing (ABS) is an adaptation of Attribute Based Encryption (ABE) for the purposes of providing guarantees towards the provenance of the signed data, and moreover towards the anonymity of the signer.

First section of this report describes ABE with its types Key-policy attribute-based encryption (KP-ABE) and, Cipher-policy attribute-based encryption (CP-ABE).Sub sections explains difference between two methods and encryption decryption specifications of each. It covers definition of attributes, how predicates help to gain privacy.

Second section of this report explains Attribute-Based signatures (ABS) that allows signing a document with the set of attributes.

ABS has variants like ring signatures, group signatures, mesh signatures that provide signatures from secret key authority. It covers behavior of signatures and method to apply signature to gain authenticity.

2. Attribute-based encryption (ABE)

Attribute-based encryption (ABE) is a cryptographic scheme that is targeted to achieve anonymous access control Attributed based encryption (ABE), first introduced by Sahai and Waters, provides a mechanism by which we can ensure that even if the storage is compromised, the loss of information will only be minimal. The basic concept was to encrypt the data before sending to the Cloud provider. But there is a problem still faced by the client. Because the Cloud provider needs to perform the calculations on data to respond the request from the client so he must provide the key to the server to decrypt the data before execute the calculations required, which might affect the confidentiality of data stored in the Cloud [1].

Mechanisms using data encryption, driven by policies, can be used to ensure degrees of (fine-grained) data protection, trusted third parties (called Trust Authorities (TAs)) can be used to provide compliance checking capabilities [2]. A user is able to decrypt the cipher text if and only if at least a threshold number of attributes overlap between the cipher text and user secret key.

An access control policy would be a policy that defines the kind of users who would have permissions to read the documents. e.g. In an academic setting, grade-sheets of a class may be accessible only to a professor handling the course and some teaching

assistants (TAs) of that course. We can express such a policy in terms of a predicate:

((Professor ^ CS dept.) V (M.tech student ^ course TA ^ CS dept.))

We will call the various credentials (or variables) of the predicate as attributes and the predicate itself which represents the access policy as the access-structure. In the example here the access structure is quite simple. But in reality, access policies may be quite complex and may involve a large number of attributes.

2.1 Key-policy attribute-based encryption (KP-ABE)

The idea of a KP-ABE scheme is as follows: the cipher text 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 cipher text if and only if the cipher text attributes satisfy the access structure embedded in its secret key [8]. In Key Policy-ABE attributes will be assigned to a cipher text (when creating the cipher text).

Policies will be assigned to users/keys by an authority (who creates the keys). A key can decrypt only those cipher texts whose attributes satisfy the policy.

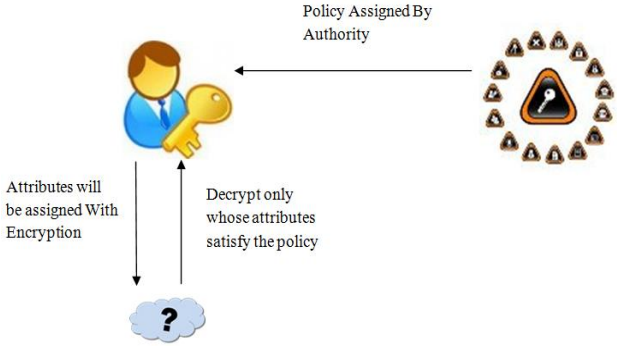

Figure1. Key-Policy attribute-based encryption

KP-ABE setup algorithm takes as input a security parameter K and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. Master secret key is used to produce new user secret keys and is known only to the authority.

KP-ABE Encryption algorithm takes a message M, the public key PK, and a set of attributes S as input. It outputs the cipher text E.KP-ABE Key Generation algorithm takes as input an access structure T and the master secret key MK. It generates a secret key which allows the person to decrypt a message encrypted under a set of attributes S if S matches access structure.

The technique KP-ABE Decryption takes as input the user's secret key for access structure T and the cipher text, which was encrypted under the attribute set S. This algorithm outputs the message M if and only if the attribute set S satisfies the user's access structure T.

2.2 Cipher-policy attribute-based encryption (CP-ABE)

Cipher Policy-ABE works in the reverse way of Key Policy-ABE in the sense that in Cipher Policy-ABE the cipher text is associated with an access structure and each user secret key is embedded with a set of attributes [8].Cipher Policy-ABE setup algorithm takes as input a security parameter K and returns the public key as well as a system master secret key.

PK is used by message senders for encryption. Master secret key is used to generate user secret keys and is known only to the trust authority. CP-ABE Encrypt algorithm takes as input the public parameter PK, a message M, and an access structure T.

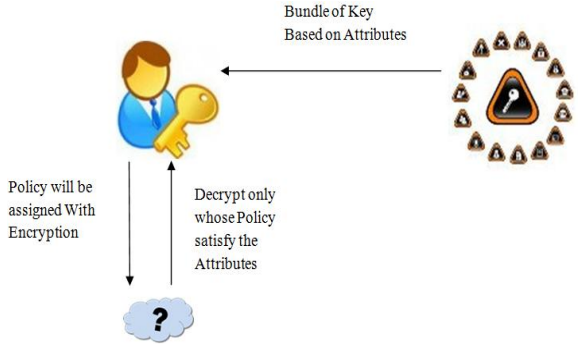

Figure 2. Cipher-Policy attribute-based encryption

It generates the cipher text .Cipher Policy-ABE Key Gen algorithm takes as input a set of attributes S associated with the user and the master secret key Master secret Key. It generates a secret key that permits the user to decrypt a message encrypted under an access structure T if and only if S matches access structure T.

Cipher Policy-ABE Decrypt algorithm takes as input the cipher text and a secret key for an attributes set S. It returns the message M if and only if S satisfies the access structure associated with the cipher text.

2.3 KP-ABE verses CP-ABE

In KP-ABE they encrypt the attributes along with the data and give the access structure to each user as part of their secret key. But attribute based encryption is more applicable in the regular world if the access structure can be embedded in the cipher text and the users can have their attributes saved in their secret keys. This second form of ABE is known as cipher text-policy based (CP-ABE) and was introduced by Bettencourt et al. [3].

Both these initial schemes were largely based on the secret sharing scheme developed by Shamir. However, it is cipher text policy based ABE that has become more popular in later. This might be largely due to the fact that CP-ABE represents a natural and more intuitive way to view ABE.

Say Bob wants to encrypt and send a message to people who have at least 3 out of 6 properties - {Colonel, Major, Navy, Op-X, Op-Y, Op-Z}. I.e. The recipient should have any 3 of the properties: a) Colonel, b) Major, c) Navy, d) worked in operation-X, e) worked in operation-Y, f) worked in operation-Z. For instance, a person who successfully decrypts the message may be an army major with experience in operations X and Y.

Equivalently the message can be opened by a naval colonel who has worked in operation Z. Thus 3 is just a minimum threshold of the attributes that must be satisfied by the recipient. In general if the threshold is (t, n), then the decryptor must have t or more of the specified n attributes. So, from the comparisons of both the techniques of Attribute-based encryption the Cipher- Policy ABE can be appropriate in cloud computing.

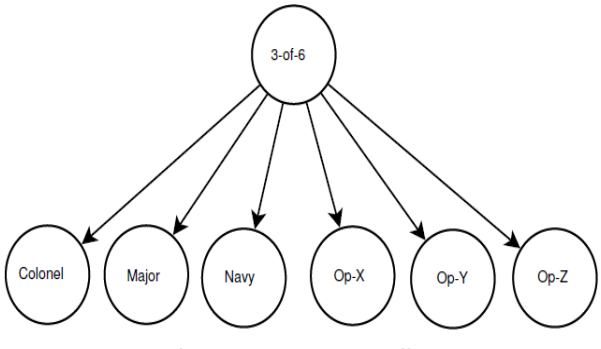

Figure 3. Access Policy

3. Attribute-based signature (ABS)

A digital signature scheme is a mathematical scheme for representing the authenticity of a digital message or document. A valid digital signature gives an assured reason to believe that the message was created by a known sender, and that it was not altered during data transfer. Attribute-based signature (ABS), which allows a signer to choose a set of attributes instead of a single string representing the signer‘s identity, under standard cryptographic assumption in the standard model is a challenging problem.

Signatures in an ABS scheme describe a message and a predicate over the universe of attributes. A valid ABS signature attests to the fact that a single user, whose attributes satisfy the predicate, endorsed the message. We emphasize the word single in this informal security guarantee ABS signatures, as in most attribute-based systems, require that colluding parties not be able to pool their attributes together.

Furthermore, attribute signatures do not reveal more than the claim being made regarding the attributes, even in the presence of other signatures. An attribute-based signature assures the verifier that a signer, whose set of attributes satisfies a (possibly) complex predicate, has endorsed the message [6].The following example illustrates the concept. Suppose we have the following predicate:

Professor OR (((Biology Department OR Female) OR above 50 years old) AND University A).

Alice‘s attributes are (University A, Female). Bob‘s attributes are (above 50 years old, Professor). Although their attributes are quite different, it is clear that Alice and Bob can generate a signature on this predicate, and such a signature releases no information regarding the attribute or identity of the signer, i.e. Alice or Bob, except that the attribute of the signer satisfies the predicate. Attribute-Based Signatures were first introduced by Magi, Prabhakaran, and Rosales (2008) as a way to let a signature attest not to the identity of the individual who endorsed a message, but instead to a (possibly complex) claim regarding the attributes she possesses. They constructed an ABS scheme that supports a powerful set of predicates, namely, any predicate consists of AND, OR, and Threshold gates [6].

3.1 Group Signatures

Group signatures are digital signatures that allow any member of a group to sign anonymously on behalf of

the group and in case of a dispute, a trusted group manager can revoke that anonymity.

Important concern to a group signature scheme is a group manager, who is responsible of adding group members and has the ability to disclose the original signer in the occurrence of ambiguity. In several systems the tasks of adding members and canceling signature secrecy are separated and given to a membership manager and cancelation manager respectively.

Suppose the Ministry of Health is the group manager. Any doctor that is registered in the group can sign a prescription. The pharmacy does not need to have a list of doctors anymore because it verifies the signature on a higher level. In other words, verification is done with the question, does whoever signed belong to the group of certified doctors[3]?

3.2 Ring Signatures

A ring signature is similar in concept with group signatures but differs in three key ways. First of all, there is no way to revoke the anonymity of an individual signature (i.e. no one can tell the signer of a message not even the group manager). The next distinction is other group of users can be considered as a group without additional setup.

The last distinction is that every user has a public and private key. The way ring signatures work is by having a member choose any set of possible signers that includes him-self, and he signs a message by using his secret key and the others' public keys, without getting their approval or assistance [3]. It is used as a structural block of several cryptosystems.

Technically, ring signatures can be viewed as a witness-indistinguishable disjoint of regular signatures, but because of this, only signer who have previously published a confirmation key are suitable to be enrolled in such a group. Ring signatures can thus only ever associate users who, by the act of publishing their key, are declaring their approval.

3.3 Mesh Signatures

The idea can be considered as an addition to ring signatures, but with added modularity and a much comfortable primitives for expressing signer ambiguity. Intuitively, mesh signatures (as in ring signatures) need to be anonymous and unforgeable.

The access structure can be satisfied using different combinations of atomic signatures, once created the mesh signature will not release what particular subset was used. The atomic signatures may be "static" and repeatedly usable, as different to new. Hence PKI Certificates are suitable even if the mesh signer not have the trust authority's signing key. In view of the fact that additionally the access structure is powerful enough to express disjoint of certificate chains, we are no longer satisfying to the prior declaration of all the ring keys.

A mesh signature is a non-interactive witness-identical proof that some decentralized Boolean expression is true, where each input of that expression is labeled with a key and message pair and is true only if the mesh signer is in ownership of a valid signature on the stated message under the stated key.

4. Future Directions

Let us assume we have two enterprises A and B. An enterprise A have a public cloud with data, software's and applications. .Company B wants a secure data from A's Cloud .We are here, trying to send a secure data to B by using ABS algorithm. We are taking some steps to implementing Digital signature with ABE algorithm. Suppose Alice is an employee of an enterprise A and Bob is an employee of a company B.

Step1.Alice takes a document from cloud, which Bob wants.
Step2.The document will crunched into few lines by using some Hash function the hash value is referred as message digest.
Step3. Alice software then encrypts the message digest with his ABE scheme. The result is the ABS.

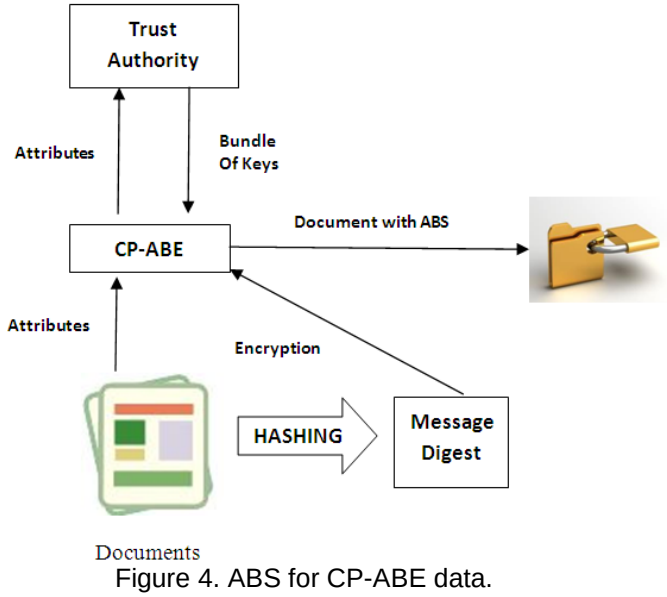

Figure 4. ABS for CP-ABE data.

4.1 Conclusion

The consumer of cloud services are having noticeable issue is security and privacy of data before sharing it with cloud service provider (CSP). Consumers can adopt different encryption techniques to achieve security but they have to compromise their keys to CSP when some course of computation needed by CSP.

ABE scheme is one of the efficient methods to sort out this issue. ABE have two variants like KP-ABE and CP-ABE but from the comparisons CP-ABE is appropriate scheme to adopt for security and privacy.

To achieve authentication and trust on CP-ABE based encrypted documents. ABS is needed to be applied by CSP while returning documents to consumer and vice versa. ABS also have variants like group ABS, ring ABS and mesh ABS any of the ABS scheme is adoptable according to consumers perspective. Thus, ABS proves to verify that the signer holds a subset of attributes satisfying that signing policy. It can be efficiently used in real scenarios like data sharing in cloud computing for certification and confidentiality with satisfying signing policies.

5. References

[1] M. Tebba, S.EL Hajji, A.EL Ghazi," Homomorphic encryption method applied to Cloud Computing," proc.of Network Security and Systems (JNS2), 2012 National Days of Network Security & Systems, pp.86-89, 20-21 April 2012.

[2] S. Pearson, M. Casassa Mont, L. Chen,"End-to-End Policy-Based Encryption and Management of Data in the Cloud," Third IEEE International Conference on Could Computing Technology and Science, pp.764-771, Nov. 29 2011-Dec.1 2011.

[3] J. Bethencourt, A. Sahai, B. Waters, "Cipher text-Policy Attribute-Based Encryption," Proceedings IEEE Symposium on Security and Privacy, pp. 321- 334, Washington, USA, 2007.

[4] S. Venugopalan," Attribute Based Cryptology," PhD Dissertation Indian Institute Of Technology Madras, April-2011.

[5] P.Yang,T.Zia,Z.Cao,X.Dong, "Efficient And Expressive Fully Secure Attribute-Based Signature In The Standard Model," 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, pp. 252-261, 2011.

[6] H. Maji, M. Prabhakaran, M. Rsulek."Attribute Based Signatures," Cryptology ePrint Archive, Report 010/595. Version 2010-1124:045114. Nov. 2010.

[7] Y. Shucheng,"Data Sharing on Untrusted Storage with Attribute-Based Encryption," PhD Dissertation Worcester Polytechnic Institute, July-2010.

[8] D.Khader," Attribute Based Authentication Schemes," PhD Dissertation University of Bath, 2009.