ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(S9), 306–311, May 2015*
DOI: 10.17485/ijst/2015/v8iS9/65587

Efficient ABBE for Improving Cloud Security in a Dynamically Changing User Environment

B. Akshaya*, C. Sudha, B. Suvedha, P. Shanthi and A. Umamakeswari

Department of CSE, School of Computing, SASTRA University, Thanjavur – 613401, Tamil Nadu, India; akshu.bala@gmail.com, sudha0894@gmail.com, suvedha1993@gmail.com, shanthip@cse.sastra.edu, aum@cse.sastra.edu

Abstract

The existing scenario to store a large amount of data in a centralized server is complex as the information stored is immense. To avert this organizations move to cloud this causes some security issues. The paper focuses on ABBE (Attribute Based Broadcast Encryption) which is an enhancement of ABE (Attribute Based Encryption) which uses ABE to encrypt the data (AES key) and then broadcasts the cipher in order to provide fine grained access. This also avoids collusion and excess key generation. In addition to this multiple data owner scenario scheme is part of our proposal wherein the whole system is divided into multiple domains. AES encryption is used to encrypt data and ABBE to encrypt the AES key to be broadcasted. ABBE has minimized implementation complexity and less effort with respect to computation when compared to that of ABE. This imposes no limit on the attribute's size, when those attributes sets are used for encryption and has a huge attribute universe. Also the cost of cryptographic functions like encryption and decryption is minimum. It also enables modification of accessibility or modification of attributes dynamically and also it supports effective user or attribute revocation as per the demand. By having multiple domains the management complexity of keys is also minimum. This novel framework is developed for educational institutions to securely share the information through cloud.

Keywords: ABBE, AES, Attributes, Broadcast Encryption, Cloud Security

1. Introduction

Storing a large amount of information local to an institute or an organization incurs a lot of storage overhead and expenses. To overcome this, a need to move to the cloud arises wherein storing information in a cloud and retrieving the information only when required is made possible because of its high availability. With the advantage of it comes the major issue of cloud in terms of security[1]. The various kinds of security breach in cloud environment makes it inefficient for confidential data. To improve cloud security various cryptographic algorithms have been proposed. These cryptographic algorithms add some computational overhead to the system with the advantage of security. To improve security as well to reduce the overhead imposed by the traditional cryptographic algorithms, an efficient method that combines ABE with Broadcast Encryption, ABBE (Attribute Based Broadcast Encryption) that prevents collision attack and handles dynamic user revocation is proposed. Thus an evolutionary path is set from ID based encryption to ABE (Attribute Based Encryption), then to Constant CP-ABE which finally led to the development of ABBE. The idea of ABBE rooted when ABE started to evolve. In the ABE system, we use attributes of different users to form the access policy. Only those users whose attributes matches the attribute chosen by the encryptor can decrypt the message. ABE is of two types namely Key Policy ABE (KP-ABE) and Cipher-text Policy ABE (CP-ABE). In the first variation, the private key with respect to each user is nested with the defined access policy and every cipher text is combined with a set of attributes[2].

*Author for correspondence

Decryption of the data can be done only when the attributes present in the cipher text and the desirable access policy formed is mapped exactly and embedded in the private keys of the users. The second variation CP-ABE has it in reverse where each user has a group of attributes corresponding to the private key of the users and the encryption of data is done using the access policy. The attributes associated with the private key of the users must be valid for the given access policy present in the cipher text to decrypt the data[3]. In CP-ABE the cipher text size increases linearly with an increase in number of the attributes used. In CCP-ABE, a constant size cipher text is achieved by using logical AND of the attributes. This sets the size of cipher text constant for any number of attributes thus decreasing the storage overhead. Moreover it has been proved that CCP-ABE is CPA secure[4]. The proposed ABBE system has a constant size cipher text as it uses CCP-ABE for encryption. It then uses broadcast scheme to broadcast the encoded key which should be used for decryption. There are many broadcast encryption scheme which involves sending a common key for decryption to N number of users. Almost all the broadcast scheme requires the recipient details on hand to broadcast the information[5]. This involves heavy computation and high expenses when it comes to large number of users. In ABBE attributes are used to select the user list. This reduces the need to know the list of users and also minimizes storage cost as it generates only constant sized cipher. In addition to ABBE that is prevalent now-a-days, the proposed system improves the security by adding another level of encryption. The Authority first encrypts the file to be stored in the cloud using AES technique and then encrypt the decryption key of AES using ABBE to provide an extra level of security. Since ABBE has less computation, communication and storage overhead this double round of encryption does not incur much overhead to the system. The usage of AES makes the system a symmetric key system. Symmetric algorithms have the upper hand over other algorithms. They don't consume too much computing power and also achieves a high speed encryption[6]. Also the key length in AES can include 128,192 or 256 and block length can be of 128, 196 or 2567 which is a constant. Here the encryption key and decryption key used are the same which minimizes the key generation. As well symmetric key algorithms are proved to be faster and cheaper than asymmetric algorithms, which is an added advantage for our system. In the proposed system, since the entire file is encrypted using AES and not using ABBE, if the attributes and access policy keeps changing it is enough that the encryption can be done only to the AES decryption key and not the entire data. This is highly recommended for a dynamically changing scalable environment.

1.1 Overview of Cloud Technology

In recent days, the cloud technology has emerged as a more flexible and scalable technology as it provides various services to satisfy users' needs. Consider in particular, the services offered for storage using which the data owner can store and share the data effectively and cheaply i.e., the owner needs to pay only for the storage space used, but one problem which remains a puzzle unsolved is the security because the cloud storage space cannot be trusted completely[8]. Cloud technology is vulnerable to a number of crypt attacks. This forces the data owner to make a strong access control structure, which allows only the permitted users to access the particular data.

1.2 Public Key Cryptography

The traditional public key infrastructure uses a public key to encrypt the data before uploading to cloud[9]. If the owner or some user requests the cloud for the data, the corresponding cipher-text will be returned, which then will be decrypted using a private key which is kept secret[10]. The main disadvantage of this structure is that the storage overhead is very large because, a single plain-text will be encrypted with different public keys. Here the public keys and private keys used are mathematically related[10]. Identity Based Encryption (IBE) technique is a one form of public key encryption where it uses some unique information about the user such as cell phone number is used as the public key of the user and is called an identity. An identity is a 1-1 mapped string for all the users. The private key of the user which corresponds to the user's unique ID is generated by a trusted body and the public key is that ID itself. The data is encrypted using the unique ID and can be decrypted by the user only with the help of the private key corresponding to the ID. Also the encryption here is one-to-one[11]. The first implementation of IBE was proposed by Adi Shamir in 1984 where he used the users' e-mail addresses as the unique ID[12]. This system eradicates the need for distribution of public keys

and the public keys authenticity is guaranteed unless the private keys of that particular user is kept secured. But if the private key is compromised, all the messages protected using public-private key pairs will be compromised.

1.3 Attribute based Encryption (ABE)

To overcome the disadvantages of the above mentioned techniques, Waters and Sahai proposed a new scheme based on attributes called Attribute-Based Encryption (ABE) in 2005. It was introduced as a fuzzy version of IBE[13,] and this version views a set of attributes as the identity in other words the unique ID of a user. Attributes are nothing but a string which is descriptive in nature and can be mapped to the users who uses information in the cloud. Encryption and decryption of data is done with the help of these attributes[14]. The disadvantage of ABE scheme is that, the encryption of data is done with each authorized user's attributes. This involves a lot of computation overhead. In the same year, Nail et al. introduced a threshold attribute-based encryption which can prevent the collusion attacks[15].

1.4 Key Policy Attribute based Encryption (KP-ABE)

In 2006, Goyal et al. introduced a Key Policy ABE (KP-ABE) scheme2 which makes use of the user's access policy as the private key and the user's attributes as the public key to encrypt the data. Fine-grained access control can be achieved using this scheme and it is more flexible than ABE. The disadvantage of KP-ABE is in this access policy is the private key of the user which makes the data owner unable to specify the users who can decrypt the data but setting the policy with a set of attributes that describes the data. Besides, KP-ABE has a monotonic access structure which can't use the negative attributes exclude the users with whom the owner need not want to share the data.

1.5 Cipher Policy Attribute based Encryption (CP-ABE)

Another variant of ABE is the Cipher-Text Policy ABE (CP-ABE) scheme (3) where the desirable access policy of the user is used to encrypt the data and the set of attributes pertaining with the user is used as the user's private key. In order to decrypt the data, the attributes in the private key of every user needs to satisfy the access policy. Although this ABE scheme is capable of constructing strong and flexible data access control structure, it suffers from a large cipher text size problem i.e. the size of the cipher text will increase in linear with the increase count of attributes. To overcome this problem, CP-ABE strategy which will have a constant size of cipher text called Constant Cipher-text ABE (CCP-ABE) was introduced, this scheme not only maintains the cipher text's size as a constant but also supports non-monotonic data access policy[4].

1.6 Attribute based Broadcast Encryption (ABBE)

To securely send some data to a dynamically changing set of users over an unsecure channel we use Broadcast Encryption (BE) methods. In the classical BE approach the list of decryptors needs to be explicitly specified. This is not possible if the system keeps on dynamically increasing. Attribute Based Broadcast Encryption (ABBE) scheme overcomes this problem of the existing BE scheme where the exact list of decryptors is not needed4. In ABBE encryptor can generate a desirable access policy composed of one or more attributes which provides access to only the authorized set of users for the data. In ABBE scheme encryption and decryption is based only on the user attributes. The users can be associated with multiple attributes and every single attribute can be shared by multiple users. ABBE separates users into different groups based on the attributes known as revoked group and non-revoked group. The set of users who belong to the revoked group cannot use the data whereas the set of users who belong to the non-revoked group can access the data. So ABBE is suitable for large scale systems which involve more of many-to-many communications[16.]

2. Proposed System

The proposed system is the one where the data owner shares confidential data to a desirable set of users group. This can be done by explicitly selecting the decryptors list but will involve high computation and time. This system shown in Figure 1 proposes a model wherein the data owner selects the group based on the common attributes of the users. Only those users whose attributes matches the attributes chosen by the data owner can decrypt the message broadcasted. The authority takes care of the AES encryption of the file followed by the ABBE of the decryption key. Authority stores the encrypted file to the cloud and develops a header which contains the access

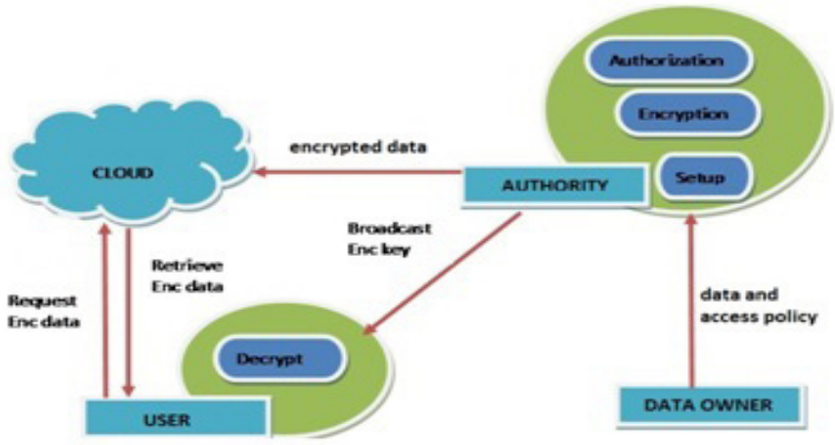

Figure 1. ABBE scheme in cloud environment.

Table 1. Performance analysis of various cryptographic systems against dynamic ABBE scheme

Schemes/Parameter	IDE	HE	ABE	KP-ABE	CP-ABE	MA-ABE	ABBE
Access Control	Less	Less	Average	Average	More	Better	More
Scalability	Average	Average	More	Average	Average	More	More
Flexibility	Less	Less	Average	More	More	More	Average
Efficiency	Less	Less	Average	Average	Average	Scalable	More

policy and then broadcasts it to the users. After broadcasting, it is not required that the header and encrypted file should be saved thus saving unnecessary storage overheads. The users receive the broadcasted message and only if they gratify the defined access control policy they will retrieve the decryption key to obtain the decrypted form of data stored in the cloud. In the proposed system, the concept of multi authority domains is also present so as to bring flexibility and to avoid key escrow issue. The proposed system also supports permanent revocation. So if the users leave the system its gets updated to the records maintained by the authority. So even if he tries to enter the system again his credentials won't meet the requirement to be part of the entire system. The proposed system doesn't involve re-keying as well as revoke users without affecting others, thus reducing computation again and flexibility of attribute organization is achieved. Since the proposed system gets changes periodically and this involves many to many communications, use of ABBE over ABE is wiser. On using this ABBE scheme for this system one can obtain a better performance than the other methods which is evident from the data given in Table 1.

2.1 Algorithm

The generalized algorithm of Attribute Based Broadcast Encryption (ABBE) is as follows:

1)Setup Phase (λ,n,B(u))

This phase takes the security parameter λ, set of users u and set of user groups B(u) chosen solely based on the attributes and outputs an encryption key EK.

2)Encrypt Phase (EK,M,B_n,B_r)

This phase takes the input as the encryption key EK, Br and Bn group along with the message M. In the process of encryption the message M will be encrypted using the encryption key EK and a cipher text C is sent along with the header information hdr

3)Decrypt Phase (dk_u,hdr,C)

This phase takes a decryption key as the input which is given to every individual user u along with the header hdr formed during the encryption phase. This will output the key K needed to decrypt the cipher text C only if the user u satisfies the following condition: $B_n \cap B(u)$ and $B(u) \cap B_r = Ø$ else it produces no result. In our scheme, the decryption keys d_{ku} is distributed beforehand (student username and password combination) and the message M is the AES decryption key encrypted using the ABBE encryption key EK formed using the attributes to form a cipher text. This cipher text C is then decrypted and the AES decryption key is obtained by the users belonging to the non-revoked group (B_n) and not by the users belonging to the revoked group (B_r) for that particular information.

2.2 Security Model

In this the security aspects of both AES and ABBE schemes are discussed. AES strategy provides security in case of known plain text attack, Differential Power Analysis attack, chosen plain text attack, and Simple Power Analysis attack. In this section, the discussion about the ABBE scheme's security proof is given briefly.

2.2.1 Semantic Proof

The ABBE strategy will be weighed secured in this given model, even if all the revoked user's keys for decryption and header information is given, it is not possible for an attacker to obtain any information related to the key[17]. The semantic security proof of this ABBE scheme is can be given with the help of a scenario involving an attacker and a challenger. Prior to the start of the game played by both attacker and challenger, the sets of users are provided to the attacker.

1. The attacker and the challenger are provided with g defined sets of users c, described by $(B(c))_{1\leq c\leq n}$.
2. Then the attacker gives an access policy and partition of two sets of groups B_n and B_r which it wants to attack.
3. In the next step challenger executes Setup (λ, n, (B(c))1≤c≤n), then provides the attacker with the key used for encryption EK, along with the keys for decryption dkuto the respective users that the attacker shall have control upon, i.e. provided this eqauation, dkuto the respective users that the attacker shall have control upon, i.e. provided this eqauation, $Bn\cap B(c) \neq B_n$ or $B_r \cap B(c) \neq Ø$ is valid.
4. The challenger runs Encrypt (EK, B_n, B_r), and receives a key K ϵ K and a header hdr.
5. In the next step, the challenger draws a random bit rb, and set K_{rb} = K, choose randomly selected K_{1-rb} in K, and finally provides (hdr, K0, K1) to the attacker A.
6. The last step is where the attacker A gives as output a bit rb'.

This game can be won by the attacker A only if rb' = rb and its advantage can be given as,

$Adv^{ind}(\lambda, n, (B(c)),A) = |2\ Pr[rb' = rb] - 1|$,

here the probability is applied on the randomly selected bit r and over all other randomly selected bits that is being is used during the first two phases of simulation. So, this ABBE scheme is thus proven to be secure against collusions which are static in nature entirely for all randomized polynomial-time.

2.2.2 Collusion of Attributes

Another big security aspect of ABBE strategies is it's resistant towards attribute collusions, i.e., if an user $u_1$possess an attribute Att_1 and an user u_2 possess an attribute Att_2 then they are not liable to decrypt the given header information if the access control is given as per this policy: Att_1 ^ Att_2. Only users who possess both the attributes Att_1 and Att_2 can decrypt the header i.e., users who satisfy the defined access policy. Other combination of broadcast encryption schemes where each key is an attribute is prone to experience attributes collusion attack[17].

3. Conclusion

The ABBE scheme in the proposed system has low encryption and decryption cost when compared with other cryptographic systems. This ABBE scheme also involves low storage and communication overhead and is highly suitable for a dynamically changing scalable environment which involves more number of many to many communications. Also in this the semantic security of a dynamic ABBE scheme is proved. In addition to this, in the proposed system no re-encryption of entire data is needed again in case of any changes to the access policy. In this system, effective immediate revocation is made possible only because the authority stays online always and handling effective immediate revocation when multi authorities stay offline is left open for discussion.

4. References

1. Sharifi AM, Amirgholipour SK, Alirezanejad M, Aski BS, Ghiami M. Availability challenge of cloud system under DDOS attack. Indian Journal of Science and Technology. 2012 Jun; 5(6):2933–7.
2. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM conference on Computer and communications security; 2006.
3. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. Proceedings of IEEE Symposium on Security and Privacy; 2007. p. 321.
4. Shaha VM, Kapadia VV. More efficient and flexible approach over traditional Cipher text Policy Attribute Based Encryption (CP-ABE) in form of Constant Cipher text Policy Attribute Based Encryption (CCP-ABE) and Attribute Based Broadcast Encryption (ABBE). Int J Adv Res Comput Sci Software Eng. 2014 Jul; 4(7):1133–5.
5. Chaudhari MB, Kapadia VV. Key generation of attribute based broadcast encryption. International Journal of Innovative Research in Science, Engineering and Technology. 2013 May; 2(5):1445–7.
6. Jeeva AL, Palanisamy V, Kanagaram K. Comparative analysis of performance efficiency and security measures of some encryption algorithms. IJERA. 2012 Jun; 2(3):3033–7.
7. Malhotra M, Singh A. Study of various cryptographic algorithms. IJSER. 2013 Nov; 1(3):77–88.
8. Rajathi A, Saravanan N. A survey on secure storage in cloud computing. Indian Journal of Science and Technology. 2013 Apr; 6(4):4396–401.
9. Kamara S, Lauter K. Cryptographic cloud storage. Proceedings of the 14th International Conference on Financial Cryptograpy and Data Security; 2010. p. 136–49.
10. Lee J-Y. A study on the use of secure data in cloud storage for collaboration. Indian Journal of Science and Technology. 2015 Mar; 8(Suppl 5):33–6.
11. Peikert C, Tripathi P. Identity-based encryption. Theoretical Foundations of Cryptography. Spring: Georgia Tech; 2010.
12. Su JS, Cao D, Wang XF, Su YP, Hu QL. Attribute-based encryption schemes. Journal of Software. 2012; 6:1299–315.
13. Sahai A, Waters B. Fuzzy identity based encryption. Advances in Cryptology V EUROCRYPT. 2005; 3494:457–73.
14. Jothi Neela T, Saravanan N. Privacy preserving approaches in cloud: A survey. Indian Journal of Science and Technology. 2013 May; 6(5):4531–5.
15. Nali D, Adams C, Miri A. Using threshold attribute-based encryption for practical biometric-based access control. Int J Netw Secur. 2005; 1(3):173–82.
16. Zhou Z, Huang D. Constructing Efficient Attribute-Based Broadcast Encryption. Proceedings of INFOCOM IEEE Conference on Computer Communications Workshops; 2010.
17. Junod P, Karlov A. An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies. Proceedings of the 10th Annual ACM Workshop on Digital Rights Management (DRM '10).