Research Article

ACCENTS Transactions on Information Security, Vol 2(7)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2017.27003

Time domain attribute based encryption for big data access control in cloud environment

Shobha. K[1] *and S. Nickolas[2]
Research Scholar, Department of Computer Application, National Institute of Technology, Tiruchirappalli, Tamil Nadu, India[1]
Associate Professor, Department of Computer Application National Institute of Technology, Tiruchirappalli, Tamil Nadu, India[2]

Abstract
Due to high volume, variety and velocity of big data, organizations apprehend to store these huge data on the cloud environment, because of its scalability and processing power services in terms of pay as you use. Due to the security demand of data in terms of storage and access structure, data owner cannot store data on cloud in plain text format and hence has to define the encryption algorithm and access structure for the data that has to be stored in the cloud infrastructure. In this paper we propose a new way of encryption method called as a time domain attribute based encryption by embedding time into both cipher text and keys to achieve an end to end security of big data in cloud. The proposed time domain attribute based access control (TDAAC) algorithm shows how ciphertext policy attribute based encryption (CP-ABE) with time domain and access rights can assist in protecting data against adversaries or deliberate unauthorized access to data that is stored in cloud.

Keywords
Terms-Big data, Cloud computing, CP-ABE, Time domain, TDAAC.

1.Introduction
With the rapid development of technologies and social network sites, data generation has increased in our daily life and this enormous data is called as the big data. The ever increasing data pose many challenges from storage to computation, since traditional tools cannot manage this large amount of data. Cloud computing, due to its flexible, scalable and economic resources, is a natural fit for storing, processing and sharing the data contents.

When outsourcing data contents into the cloud, it is not easy to achieve fine-grained access control especially in time-domain, as the owners of the data are not able to control their data as on their own servers. The untrustworthy cloud servers further makes this issue more challenging: 1) cloud servers may not be fully trusted by the owners to control the access of their data 2) cloud servers may also be curious about the stored data contents. Thus existing server based access control methods are not applicable for cloud-based content sharing.

A possible approach is to encrypt data contents and only authorized users are given decryption keys.

However, due to large volume of data contents and the performance requirements traditional encryption methods like AES, DES, RSA, etc. may not be suitable for data encryption. To solve this problem attribute based encryption (ABE) can be used. However existing ABE and variants of ABE such as KP-ABE and CP-ABE methods do not take the time into consideration, hence the main challenging issue in our proposed time-domain cipher text attribute based encryption is how to embed time into the cipher text and the keys.

Another challenging issue to control data sharing in time-domain is the dynamic change of attributes. In each time period, a user may be entitled some new attributes, or revoked some attributes, or re-granted some previously revoked attributes. Existing attribute revocation methods [1-4] need to re-encrypt all the previously encrypted data so that all the new coming users may still be able to decrypt the previous data if their attributes satisfy data access policies. Hence, these methods may not be suitable for fine-grained data sharing within certain time period.

*Author for correspondence

In this paper, we focus on how to securely share data contents to a certain group of people during a particular time period in cloud-based systems, and propose a cryptographic approach, a provably secure time-domain attribute based access control (TDAAC) scheme, to control the access of session keys that are used to encrypt data contents. This proposed model is based on multi authority ciphertext policy attribute-based encryption (CP-ABE) scheme proposed by Lewko and Waters [5], so that TDAAC can support attributes issued from multiple authorities as well.

The remainder of this paper is organized as follows. We first review some existing works that are related to attribute based encryption and its methods in section 2. Then, we describe the proposed system and security model in section 3 and in section 4 we describe the frame work of TDAAC. Finally, the conclusion of this paper is drawn in section 5.

2.Related work

The literature survey gives descriptions of different schemes available in attribute based encryption along with its advantages and disadvantages.

2.1Attribute based encryption(ABE)

An attribute based encryption scheme was introduced by Sahai and Waters [7] in 2005 with the intention of providing security and access control. Attribute-based encryption (ABE) is a public-key based encryption that allows users to encrypt and decrypt data based on user attributes. In this scheme the secret key of a user and ciphertext are dependent upon attributes (e.g. the unique ID of a person). In such a system, the decryption of a ciphertext is possible only if the set of attributes matches the attributes of ciphertext and the number of matching is at least a threshold value *d*. Attribute-based encryption (ABE) proves the collusion resistance as it is important in the systems where revocation, re-granting of access policies and users are present. An adversary that holds multiple keys should be able to decrypt the data only if at least one individual keys among the keys that forms the threshold key *d* grants access.

The drawback with attribute based encryption (ABE) scheme is that the data owner has to use every authenticated and authorized user's public key to encrypt data. Because of the use of monotonic attributes to control user access, this system usage in different application is restricted.

2.2Key policy attribute based encryption (KP-ABE)

A key policy attribute based encryption scheme was introduced by Chang-Ji, Sun Yat-sen and Jian-Fa [9] in 2012 with the intention of providing security and access control with constant size cipher text. It is the modified form of ABE. In this approach users are assigned with an access tree structure. The attributes are associated by leaf nodes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. The secret key of the user defines the access tree structure. Ciphertexts are labelled with sets of attributes and private keys are associated with monotonic access structure that defines and controls which ciphertext a user is able to decrypt.

KP-ABE defines following algorithms for setup, encryption, and key generation decryption.

Setup: This Algorithm takes security parameter K as input and outputs public key PK and a system master secret key MK. Public key is used by data owners for encryption. MK is used to generate user secret keys and is known only to the authority.

Encryption: This algorithm is run by data owner and it takes a message M, the public key PK, and a set of attributes as input. It outputs the ciphertext E.

Key Generation: This algorithm is run by authority which takes input as 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 if and only if matches T.

Decryption: This algorithm is run by user 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. This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

With the above algorithms KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme.

The problem with KP-ABE scheme is the data owner cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data; it is not suitable in some application because a data owner has to trust the third party for key issuing.

2.3Cipher text policy attribute based encryption(CP-ABE)

This method is another modified form of attribute based encryption introduced by Sahai [6]. In a CP-ABE scheme, ciphertext is associated with access policy on attributes, and users private key is associated with a set of attributes. A user is able to decrypt ciphertext only if the set of attributes associated with users private key satisfies the access policy associated with the cipher text. CP-ABE works in the other way round of KP-ABE. CP-ABE algorithms are as same as KP-ABE. The access structure residing in encrypted data lets the encrypted data to choose which key can recover the data. Based on the access structure defined in attributes, messages are then encrypted such that only those whose attributes satisfy the access structure can decrypt it.

Setup: This algorithm takes security parameter K as input 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 is run by data owner and it takes input as the public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.

Key-Gen: This algorithm takes as input a set of attributes 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 tree structure T if and only if matches T.

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

CP-ABE improves the drawbacks of KP-ABE that the encrypted data cannot choose who can decrypt. It can support access control in the real environment and the users private key in this scheme is a combination of a set of attributes, so that a user can use only this set of attributes to satisfy the access policy in the encrypted data.

Drawback of most existing CP-ABE scheme is lack of flexibility and efficiency, for this reason most of the enterprises are unable to use it. CP-ABE decryption key supports attributes that are organized logically as a single set, so the users can only use all combinations of attributes in a single set issued in their keys to satisfy access policies.

2.4Attribute-based encryption scheme with non-monotonic access structures

Previous ABE schemes were limited to expressing only monotonic access structures and there is no satisfactory method to represent negative constraints in a key's access formula. Ostrovskyz [8] et al. proposed an attribute-based encryption with non-monotonic access structure in 2007. Non-monotonic access structure can use the negative word to describe every attributes in the message, but the monotonic access structure cannot. This scheme contains four algorithms:

Setup (d): In the basic construction, a parameter d specifies how many attributes every ciphertext has.

Encryption (M, γ, PK): This algorithm takes a message M ε GT under a set of attributes γ and the public parameter PK and output the ciphertext E.

Key Generation (A, MK, PK): This algorithm outputs a key D that enables the user to decrypt an encrypted message only if the attributes of that ciphertext satisfy the access structure A

Decrypt (CT; D): Input the encrypted data CT and private key D, if the access structure is satisfied it generate the original message M.

It enables non-monotonic policy, i.e. policy with negative attributes.

The problem with Attribute-based Encryption Scheme with Non- Monotonic Access Structures is that there are many negative attributes in the encrypted data, but they don't relate to the encrypted data. It means that each attribute adds a negative word to describe it, but these are not useful for decrypting the encrypted data.

It can cause the encrypted data overhead becoming huge. It is inefficient and complex because each ciphertext needs to be encrypted with system-wise constant d.

The comparison of different ABE scheme with different parameters like fine grained access control, efficiency, and collusion resistant, computational overhead is done in *Table 1*.

Table 1 Comparison of ABE

Parameter	ABE	KP_ABE	CP-ABE
Fine grained access control	Low	High if there is re-encryption technique otherwise its high	Average
Efficiency	Average	Average, High for broadcast type system	Average, Not efficient for modern enterprise environments
Computational Overhead	High	Average	Average
Collusion resistant	Average	Good	Good

3.Proposed system and security model

As the proposed model is based on the time attribute based encryption, we consider the system time and is slotted, the time space is defined as T= {t_1, t_2, t_3…}.After each time slot the system initializes it's time to t_0, and increases it by 1 for the next time slot. In order to support this time domain we embed the time into both the ciphertext and the keys in the multi-authority CP-ABE scheme, such that only those users who hold sufficient attributes in specific time period can decrypt the data.

The proposed model consists of following entities: cloud server, data owner, users, attribute authority for each user, attribute authorities bulletin board.

Cloud server: The server stores data for data owners and provides data access to users. The server is also responsible for storing attribute authority bulletin board where the update keys of the attribute are stored and then it is responsible for removing the old update keys which are based on the old time stamp.

Data owner: The data owner defines the access policies on attributes from different attribute authorities and encrypts data using the session keys under these access policies before outsourcing data to cloud servers. The session keys are in turn encrypted using TDAAC algorithm. The access policies are embedded in the ciphertext and access keys. Data owners are responsible for using the global identifier for each user.

These data owners do not rely on the server to enforce the access policy.

User: Each user will be assigned with a global identity. Whenever request is made to access particular data with data owner the credentials are checked and global identity is given, using this identity user will be given a secret key to access particular data from the cloud server. However, the secret key of a user is insufficient to decrypt a ciphertext encrypted under the access policy at time t_i even when the corresponding attributes satisfy the access policy. The user has to obtain a set of update keys at each time slot t_i from the corresponding authorities who have published in attribute authority bulletin board which are stored in the cloud server.

Attribute authority (AA): Each attribute contains single attribute authority and attribute authority can manage arbitrary number of attributes. This work concentrates on multiple attribute authorities. Each attribute authority is responsible for entitling, revoking or re-granting attributes to users according to their roles or identities in its domain. *Figure 1* shows the conceptual model of content sharing. Attribute authority is responsible for generating secret keys, update keys for each user depending upon their global identity issued by data owner.

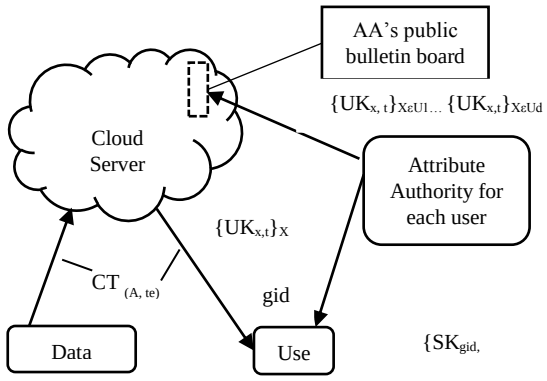

Figure 1 Conceptual model for content sharing

Attribute and user revocation: To deal with the attribute revocation problem, we follow the ideas in identity-based encryption revocation [10] and divide the time into slots. At each time slot $t_i \in T$, for any attribute and user that belongs to attribute set, attribute authority generates the update keys according to access tree and update list so that only the users who possess attributes at time slot t_i are able to obtain valid update key that belongs to attribute. Thus, by setting the update list and publishing the corresponding update key the authority can achieve dynamic change of attribute and user.

4.Conclusion

In this paper, we analyze different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, and ABE with non-monotonic access structure. KP-ABE and CP-ABE have formed the base for many other access methods depending on monotonic or non-monotonic access structure, but these methods lack in flexibility and efficiency and hence these were unable to use in enterprise. To overcome the limitations of these methods we have proposed a secure time domain ABE scheme by embedding time into both the ciphertexts and the keys, such that the users who hold sufficient attributes in a specific time period can decrypt the data and we have also proposed an method to achieve dynamic modification of access policies which supports efficient on-demand user/attribute revocation for data access permissions that are stored in cloud server. In a future work, we will implement TDAAC algorithm on real cloud based big data systems and explore the time-domain access control scheme in standard model and we prove the security of TDAAC against adversaries.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Sahai A, Seyalioglu H, Waters B. Dynamic credentials and ciphertext delegation for attribute-based encryption. In advances in cryptology-CRYPTO (pp. 199-217). Springer Berlin Heidelberg.

[2] Yang K, Jia X, Ren K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems. In proceedings of the ACM SIGSAC symposium on information, computer and communications security 2013 (pp. 523-8). ACM.

[3] Yang K, Jia X, Ren K, Zhang B, Xie R. DAC-MACS: effective data access control for multiauthority cloud storage systems. IEEE Transactions on Information Forensics and Security. 2013; 8(11):1790-801.

[4] Yang K, Jia X. Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE Transactions on Parallel and Distributed Systems. 2014; 25(7):1735-44.

[5] Lewko A, Waters B. Decentralizing attribute-based encryption. In annual international conference on the theory and applications of cryptographic techniques 2011 (pp. 568-88). Springer Berlin Heidelberg.

[6] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In 2007 IEEE symposium on security and privacy (SP'07) 2007 (pp. 321-34). IEEE.

[7] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. In proceedings of the 13th ACM conference on computer and communications security 2006 (pp. 89-98). ACM.

[8] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. In proceedings of the ACM conference on computer and communications security 2007 (pp. 195-203). ACM.

[9] Wang CJ, Luo JF. A key-policy attribute-based encryption scheme with constant size ciphertext. In eighth international conference on computational intelligence and security 2012 (pp. 447-51). IEEE.

[10] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation. In proceedings of the ACM conference on computer and communications security 2008 (pp. 417-426). ACM.

This paper is selected from proceedings of National Workshop on Cryptology-NWC 2016 organized at JNN College of Engineering Shimoga, Karnataka, India during 11-13, August 2016.