International Journal of Computer Applications (0975 - 8887)
Volume 131 - No.15, December 2015

Review on Fuzzy Authorization for Cloud Storage

Arya Vijayan
PG Scholar
Dept. of Computer Science
College of Engineering Perumon

Devi Dath
Assistant Professor
Dept. of Computer Science
College of Engineering Perumon

ABSTRACT

Cloud computing is a widely accepted technology that delivers many services over internet. The services includes storage, easy access from anywhere at any time and also minimum device memory utility. Inorder to provide security and privacy of data many authorization schemes are used. OAuth scheme is one of the most commonly used authorization scheme. But it cannot be used in the case of heterogeneous clouds. To overcome this difficulty, Fuzzy Authorization scheme was proposed. In this scheme, modified Ciphertext Policy-Attribute Based Encryption (CP-ABE) and OAuth schemes are used. This scheme provides the facility for an application that is present in one cloud party to access data that is stored in another cloud party. Fuzzy Authorization is a reading authorization scheme and data modification can only be done by data owner. When a data is modified, the application's right of accessing the data will be automatically canceled. By making use of Linear Secret Sharing Scheme and GRS code this scheme has become more scalable and flexible. The implementation is done by using simulator OMNET++4.2.2 and cryptographic part is done by using Pairing Based Cryptographic(PBC)library. Simulation results shows that this scheme is more secure and efficient. Different access control schemes are compared in this paper based on many parameters.

Keywords

Ciphertext Policy-Attribute based Encryption, Fuzzy Authorization, Cloud Storage Provider, Application Service Provider

1. INTRODUCTION

Cloud computing [1]is an emerging technology that provides both Software as service and Hardware as service. Some of the important features of cloud computing are, the data stored in the cloud storage can be accessed easily and only less amount of physical space is used for storing data. So more people are attracted to this technology. This makes the authorizations and operations between the Cloud Storage Providers(CSP) and Application Service Providers(ASP)[2] more urgent.

For example consider the case of an application called PDFMerge[3] which is registered to an Application Store(AS) called Google Chrome Web Store. And there is a data owner who stores his data into a CSP called JustCloud. One option is that the data owner has to download the pdf files from JustCloud and upload it to the application. Second option is to provide direct authorization[4] which is more efficient than the first method. Building trust between the owner and application is one of the most important issue here, as both of them are residing at different clouds. Second issue is that, if the data owner has to grant access for more than one file, multiple access tokens and secret keys should be provided.

OAuth[5][6] is the most commonly used authorization scheme. If both the data owner and application are in the same cloud this authorization scheme can be used. But here it is case of heterogeneous cloud, so this scheme cannot be used. In AAuth authorization scheme proposed by Tassanaviboon, the owner and application are at different clouds but the drawback of providing multiple access tokens for accessing multiple files are not solved. Inorder to solve both the above mentioned issue, Fuzzy Authorization[2] scheme was proposed by Shasha Zhu and Guang Gong.

Fuzzy Authorization is a secure file sharing scheme[7] that has high flexibility and scalability. This is developed by using the modified CP-ABE[8] and OAuth. Another important feature of Fuzzy Authorization is that it is a reading authorization scheme,that is the application can only access the data and cannot make any modifications to the data. Only data owner can do modifications to his data. So if the owner makes any modifications to his data, the applications right of accessing the data will be automatically revoked[9].

2. LITERATURE SURVEY

A modified version of Ciphertext Policy-Attribute Based Encryption(CP-ABE) and OAuth is used in Fuzzy Authorization. This CP-ABE, proposed by John Bethencourt, Amit Sahai, B Waters is a type of identity based encryption. It is an important cryptographic primitive for access control. In this system there will be one public key and a master private key. This master private key can be used to make more restricted private keys. In this scheme the attributes describes the user's credentials and the party who is encrypting the data determines the policy for who can decrypt the data. A user can decrypt the ciphertext only if the attributes of the user passes through the access structure of the ciphertext.

The OAuth scheme proposed by Tassanaviboon provides authorization to an application to access a data when both the data owner and the application resides in same cloud party. This cannot be applied in untrusted cloud. So a new authorization scheme AAuth was proposed. This scheme is based on OAuth standard and CP-ABE. Main advantage of this scheme is that users can share the resources in a secure manner in semi trusted cloud environment. In this for each access grant an ABE[11] token is provided.

3. REVIEW ON FUZZY AUTHORIZATION

3.1 System Model

This system consists of 4 entities. They are Data Owner(O), Application Service Provider(ASP), Cloud storage Provider(CSP) and an Application Store(AS). The data owner registers to the Cloud Storage Provider and then login to it inorder to store his data by uploading it, access the stored data and to provide authorization for accessing his data. Some cloud application services are used to process the data. The Application Service Provider is an entity that needs authorization to access owner's data that is stored in cloud storage. PDFMerge is an example for an ASP.

Another entity is the Cloud Storage Provider(CSP). It provides the facility to store data of the data owner. Dropbox is an example for CSP where video and audio files can be stored. Application Store(AS) is the entity to which the Application Service Provider will be registered. Google Web Store is an example for an Application store.

3.2 Overview of Fuzzy Authorization Scheme

The scheme has two phases an offline phase and a running phase. In the offline phase, using a random symmetric key data owner encrypts his data. Then this key will be encrypted using modified version of Ciphertext Policy-Attribute Based Encryption and OAuth scheme. The ciphertext of data and ciphertext of key will be encapsulated by the owner to form an archive. The archive is represented by access tree structure and this archive will be stored in the Cloud Storage Provider.

In the running phase, when data owner want to share data with an ASP, data owner and CSP will jointly provide an indirect secret share[10][12][15] of file attributes and similarly data owner and AS will jointly provide indirect secret share of application attributes. Consider a group element g and secret share s, then the indirect secret share can be represented as g^{sr} . When ASP receives all the indirect secret shares, it will sent request to the cloud storage for the archive and it will be provided to ASP. Decryption of the archive header for the key will be performed. Using this key the ciphertext of data can be then decrypted. The implementation can be done by using simulator and cryptographic part can be done by using PBC Library[13][14].

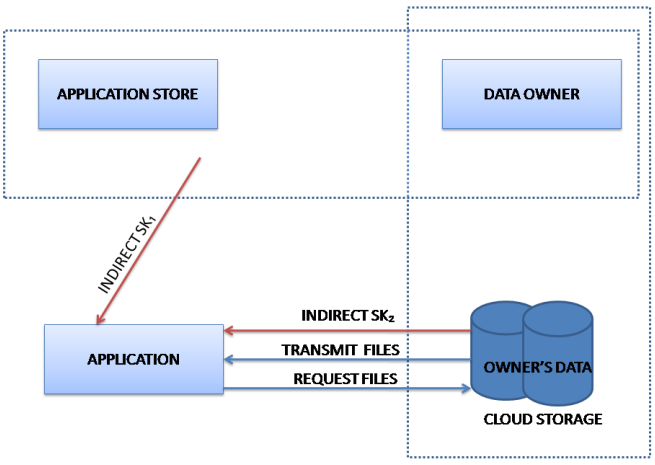

Fig. 1. System Model

3.3 Access Tree Structure

Archive files are represented using access tree structure. Access trees are constructed by using the ANDing operation. To the root node we AND the subtree of file attribute, the subtree of application attribute and timeslot attribute. Redundant checking nodes can be added to the file subtree so that the archives with the same checking nodes can be decrypted using a single access token. If the redundant checking nodes are added to the application attribute subtree, a single access token can be used by many applications.

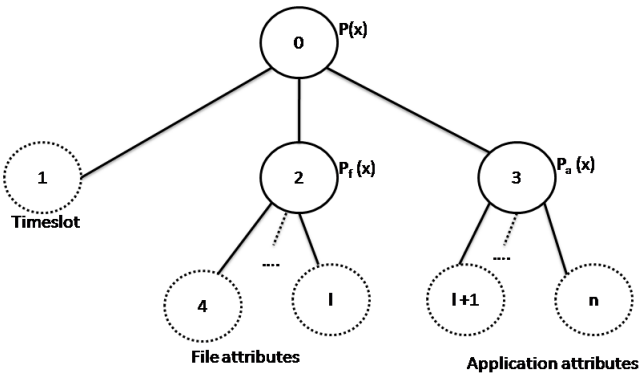

Fig. 2. Structure of Access tree

4. COMPARISON OF ACCESS CONTROL SCHEMES

Confidentiality, integrity and access control are some of the important issues that are present when data is stored in the cloud. There are many access control schemes which includes Attribute Based Encryption(ABE), Key Policy-Attribute Based Encryption(KP-ABE), Ciphertext Policy-Attribute Based Encryption(CP-ABE).Lets check these schemes in detail and compare them. Summary of comparison is as shown in Table 1.

Attribute Based Encryption was introduced by Sahai and Waters. This scheme provides security and access control. It is a type of public key encryption. It allow users to encrypt and to decrypt the data based on their attributes. That is the ciphertext and secret key are based on the attributes. The decryption is only possible if the attributes of secret key matches the attributes of ciphertext. Consider a threshold value 't'. If the number of matching is atleast t, then decryption can be done. Important feature of attribute based encryption are complex access control and no list of users is needed,just access policy is enough. The main disadvantage of ABE is that to encrypt the data ,the data owner has to use all the users public key.

The Key Policy-Attribute Based Encryption is a type of ABE. It is designed for one to many communications. In this scheme each private key will be associated with an access tree structure. This access tree will specify the type of the ciphertext the key can decrypt. Since the ciphertext are represented by a set of attributes and the key is specified using access structure,this scheme is known as KP-ABE. This scheme provides a fine grained access control and it can provide more flexibility than ABE. An important problem in this

Table 1. COMPARISON OF ABE, KP-ABE, CP-ABE

Parameters	ABE	KP-ABE	CP-ABE
Efficiency	Average	Low	Average
Computational overhead	High	Low	Average
Data confidentiality	Present	Present	Present
Scalability	Not scalable	Not scalable	Not scalable
User revocation	Absent	Present	Present
User accountability	Absent	Absent	Present
Collusion resistant	Average	Good	Good
Fine grained access control	Low	Low	Average

is that the person who is encrypting the data cannot take decision about who can decrypt the data.

The Ciphertext Policy Attribute Based Encryption works in the reverse order of Key Policy Attribute Based Encryption. This removes the main disadvantage of KP-ABE. In CP-ABE the encryptor decides the policy of who can decrypt the encrypted data. It has the disadvantage of managing the attributes of user and access policy.

5. CONCLUSION

In this paper review of a secure file sharing scheme is done, where the data of data owner stored in the cloud storage can be shared with an application in another cloud. Another important feature is that the applications access right will be automatically invalidated when ever the data owner makes some modification to the data. As an enhancement to this the writing right can be provided to the application also. The confidentiality of data is maintained by attribute based encryption and symmetric encryption. By using modified Ciphertext Policy Attribute Based Encryption the access control is implemented. And in this review paper comparison of various access control schemes are also included.

6. REFERENCES

[1] http://www.thetop10bestonlinebackup.com/cloud-storage.

[2] Shasha Zhu and Guang Gong, "Fuzzy Authorization for Cloud Storage".

[3] http://www.pdfmerge.com/

[4] "Google accounts authentication and authorization," https://developers.google.com/ accounts/docs/OAuth2Login/registeringyourapp, April 2013.

[5] A.Tassanaviboon and G.Gong,"OAuth and ABE based authorization in semi-trusted cloud computing" in Data intensive computing in clouds-DataCloud-SC'11 , second international workshop , proceedings. ACM, 2011, pp.41-50.

[6] E.Hammer-Lahav, D.Recordon, D.Hardt, " The OAuth 2.0 authorization protocol". Available at http://tools.ietf.org/html/rfc6749

[7] W.Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 55-65

[8] J.Bethencourt, A.Sahai and B.Waters, "Ciphertext Policy Attribute Based Encryption" in In proceedings of IEEE Symposium on Security and Privacy" IEEE 2007, pp.321-334.

[9] A. O. Michael Backes, Christian Cachin, "Secure key-updating for lazy revocation," in Computer Security ESORICS 2006, ser. Lecture Notes in Computer Science, vol.4189. Springer Berlin Heidelberg, 2006, pp. 41-50.

[10] R.McEliece and D.Sarwatie, "On sharing secrets and reed-solomon codes" , ACM vol 24,no.9,pp.583-584.

[11] V.Goyal, O.Pandey,A.Sahai and B.Waters, "Attribute-based encryption for fine grained access control" in Proc.13,ACM conf.comput.commun.security,2006,pp.89-98.

[12] S.Yu, "Data sharing on untrusted storage with attribute based encryption".Ph.D. dissertation, Worcester Polytechnic Institute, MA, USA, July 2010.

[13] B. Lynn, "On the implementation of pairing-based cryptosystems," Ph.D. dissertation, Stanford University, CA, USA, June 2007.

[14] B. Lynn, PBC Library Manual,http://crypto.stanford.edu/pbc/manual.pdf

[15] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, pp. 612-613, 1979. data access control in cloud computing" in INFOCOM'10 Proceedings of the 29th conference on Information communications. IEEE, 2010, pp. 534-542.