ISSN:0975-9646

CIPHER-Text Policy Attribute Based Access to Cloud

Venkateshprasad.Kalluri[1], D.Haritha[2]

[1]*Student, Department of ECM, KL University, A.P, INDIA*
[2]*Assistant professor, Department of ECM, KL University, A.P, INDIA*

***Abstract---* Cloud computing, is the significant computing paradigm which allows the users to store their data into cloud This paper presents a Attribute-Based access to the media in the cloud where it uses cipher-text policy Attribute-Based Encryption (CP-ABE) technique to create an access control structure.by using the algorithms in the access policy the attributes are used to generate a public key in order to encrypt the data and a secret key consisting of user attributes to decrypt the data and is used as an access policy in order to restrict the access of the user. . By using ABE technique the encrypted data is trustworthy even on the untrusted server. This requires flexible and accessible cryptographic key management to support difficult access policies. The policy is to assign a key to each user attribute and encrypts the data based on the appropriately distributed keys to corresponding user.**

***Keywords*---Cloud computing, CP-ABE, Access Control, Attribute**

I. INTRODUCTION

Cloud computing offers the abstract view to the users and developers.it hides much of the implementation details.it is mainly used in content sharing networks. Examples for these networks are social networking where they are dynamic in terms of storage requirement. However due to the weak security issues the use of cloud is not very fast in content sharing networks.

Access policy is a mechanism that provides security facilitates the data to user in a controlled manner. The traditional mechanism is that the data is encrypted with the user's public keys. The data owners encrypt the data using this users public key and then uploads the file to the cloud. The user whenever wanted to download the file should decrypt the file with his generated secret key. By doing this there are a few problems like the owner has to get the public key of the user and the same data is encrypted with different public keys this results in storage overhead. For example cryptic text c=E(E(m,sk1),sk2) here encrypting multiple times with the key pair(sk1,sk2) here one user has an attribute key sk1 and another user has an attribute key sk2 this may collude to decrypt the data. Hence for a particular shared data among the multiple users we need to encrypt the data with every user's public key in order to provide security hence an ordinary encryption is unsatisfactory. Instead if the cipher text consists of the set of attributes then by using the key and access policy we can decrypt the data i.e. the key works only when the attributes in the cipher text satisfies the access policy.

The access policy here is completely based on permission relationship where the relationship is between user attributes and resource attributes. The attributes may be any information of the user's profession, job roles that is provided and is used to grant the access. However in order to design an access policy mechanism there are many challenges to overcome some of them are (1)user can upload any kind of data like text, media etc.(2) any can give any number of attributes and hence two or more users may have same attributes. (3) any individual may grand any kind of access to any number of users.

This approach allows the user to implement the access control on their data directly in content sharing service rather than through a central administrator. In order to provide a complex access policy mechanism we need flexible and scalable cryptographic key management algorithms. For improving these disadvantages we are using attribute based encryption .hence we employee CP-ABE(cipher text policy – attribute based encryption) technique as a remedy to the above mentioned problem.in CP-ABE the recipient can decrypt the data only when the user attribute satisfy the access policy and this can be seen as one-to-many public key encryption and the data owner provides access to many users. In this system the users private key is associated with the user attributes and on the other hand the party that is encrypting the data specifying an access policy.

Organization

The paper is organized as follows. Section II give the related work done. Section III gives the background and bilinear maps and we then discuss the cryptographic and security primitives in section IV. Finally we give the conclusion in section V.

II RELATED WORK

The relationship between the user identification and resource in content sharing applications is dynamic. there are twoforms

of access management strategies they're user attribute access management structure and Media Structure minded Access management structure

A) user attribute access management structure

Easier [9] is a design that supports fine-grained access control policies and dynamic cluster membership by victimization CP-ABE theme. a lot of works are projected to style versatile ABE schemes There are two methods to comprehend the fine-grained access management supported ABE they are KP-ABE and CP-ABE. In KP-ABE the cipher text consist of some descriptive attributes which are labeled by the sender and the trusted authority issues a user's private key and the access policy is involved in the private key which specifies the decryption of the cipher text with the key. Here the disadvantage of this encryption is that the access policy is constructed into user's personal key. So data owner does not have the option on who can decrypt the data except encrypting the data with the set of attributes. Hence it is not suitable for certain applications as the information owner must trust the authority who gives the user's key. The KP-ABE is secure beneath the final cluster model because it is monotonic access structure and additionally it cannot categorical the attributes to reject the parties with whom the knowledge owner didn't got to share the knowledge from membership. To overcome this weakness cipher text policy attribute based encryption has been created that is proved to be secured below the quality model. In CP-ABE the access policy is made within the encrypted data and also the attributes is with the user's private key. The attribute based encryption will be divided into monotonic or non-monotonic based on the sort of the access structure and based on the access policy the schemes will be classified as key policy or cipher text policy. The ideal attribute based encryption must support data privacy, scalability, fine grained access control, user accountability, user revocation and collusion resistant. But the provided access policies are not appropriate for the scalable media content.

B) Media structured access control

For a video the secure scalable streaming is the progressive encryption technique. This should be integrated with error correction technique since it may result in decryption failure due to the packet loss.an access control scheme is designed by wu et al which is highly secured and efficient and predominantly the scheme is flexible as its "*encrypt once, decrypt many ways"* is compatible with the features of jpeg 2000.

Zhu et al. [19] proposed an access management schemes for streams determined by the MPEG-4 Fine granularity scalability (FGS) normal thus on allow one encrypted stream to support each forms of scalabilities simultaneously. The organization of the media data will be ruined by the media structured access control in request to ensure the data so that the client will unscramble the separate figure content with the important keys. These plans are constrained to productive key generations furthermore ordinarily expect the presence of an online key spreading center; and they don't manage access policies, e.g., how to give user attributes to access rights

III. PRELIMINARIES

A) ONE WAY HASH FUNCTION

When we take an input string of variable length and then after applying hash function it produces an output of fixed length. The hash function is applied in one direction only and is denoted as H(.).let us assume that X is the input and by applying hash function the output will be Y i.e. H(X)=Y.it is impossible to obtain the pre image X from the image Y. An example for one way hash function is SHA-1 and MD-5.

B) BILINEAR MAPS

Bilinear maps are utilized to create a relationship around the cryptographic gatherings. Give us a chance to assume G1 and G2 be two multiplicative cyclic assemblies of prime order X and let the generator for G1 be g. the bilinear map will be e.e: G1 X G1 → G2.the following properties belongs to bilinear maps e.

Linearity: let a,b ∈G1 and c,d ∈Zx we have e (a^c, b^d) = e(a b)^c d.

Non-degeneracy: e(g, g) not equal to 1.

Where the bilinear map *e* and the assembly operation in G1 are productively processable. A point group over an elliptic (or hyperelliptic) curve is typically the input group G1 in a bilinearmap.

C) ACCESS TREE:

T - access tree

Nj - j th hub of the access trees

A - attributes of the data user or clients

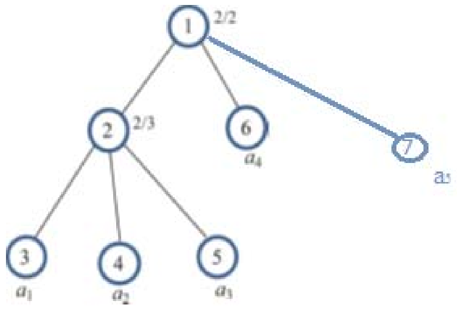
AA - Attribute authority

ai - ith attribute of the user

L - leaf hubs of the access tree

S - set of attributes of the leaf nodes belonging to a particular non-leaf node

There is an access policy established in every access control scheme which provides the access conditions and based on those conditions the user can access the information. Here is an access tree which is a representation of the access policy and this tree includes both leaf and non-leaf nodes and each leaf node consist of some attributes like age, gender etc. each non-leaf node may have a leaf node or non-leaf node or both. The root node is labeled as N1 and all the other nodes are labeled as Nj where j taken vales from 2 to some limited number successively. A Boolean function which is derived from the access policy is related with every non-leaf node and the Boolean function of the non-leaf node is represented as nj/n where n is nothing but the child nodes belonging to Nj and its Boolean value is calculated to be true if and only if it has atleast n_j child nodes. For suppose the Boolean function for the node N2 is 2/3 or equally a1a2+a2a3+a1a3 is true if a1 and a2 belongs to S and we can say nj is evaluated to be true. T(A) is evaluated to be true if the Attributes of the user satisfies the access policy and this can be explained as following. For any leaf node Nj which is accompanying with the attributes belonging to A its Boolean value is evaluated to be true and for every non-leaf node the Boolean value is the significance of its Boolean function and the T(A)= true if and only if the root nodes Boolean value is true.



Consider an example the given attributes are{a1,a2,a3,a4,a5}let the access policy be the a5,a4 and any other two attributes of the attribute set then the access is granted. then the table presents some cases where T(A) is true.

Attributes	Node N2	Node N1	Access
a1,a2,a3,a4	true	false	false
a1,a2,a4,a5	true	true	true
A3,a4,a5	false	false	false

D) CIPHER-TEXT POLICY ATTRIBUTE BASED ENCRYPTION

The CP-ABE scheme is first proposed by bethncourt et al in 2007.this CP-ABE scheme is similar to the KP-ABE(key policy attribute-based encryption).in key policy attribute based scheme the access policy is built in the users secret key where as in CP-ABE (cipher text policy attribute based encryption) the access policy is switched into the encrypted data and the attributes are linked with the public key of the user in order to decrypt the data. If the attribute set in the users secret key satisfies the access policy present in the encrypted data then the data will be decrypted.

AB-Setup

The attribute authority run an initialization algorithm by taking a security parameter () as an input. Then it outputs two keys a master key denoted as MK and a public key PK.A group G1 which is the input to the bilinear maps with a prime order of p and with a generator g and then it chooses α, β from Zp where Zp is a set of integers and produces an output PK(public key) and MK (Master key). Where PK=$G_1, g, g_1 = g^{\beta}, g_2 = e(g,g)^{\alpha}$ and MK={βg^{α}}.

AB-Encryption

Here the attribute authority runs the algorithm it will take the input as master key and the set of the attribute belonging to A and generates a private key(Sk) and distributes it to the user the attribute authority takes $r \in z_p \; and \, r_i \in z_p$.

Sk=(D=$g^{(\alpha+r)/\beta}, \{D_i = g^r H_1(a_i)^{ri}, D_i^{|} = g^{ri}\}_{\forall\, a_i \in A}$)

AB-Encrypt

The data owner runs the algorithm by taking the input message M, set of attributes and public key. The encryption happens dependent upon access tree. The data owner selects a random polynomial *f(i)* and sets its degree $d = n_j - 1$ where $n_j$is threshold such that if the Boolean value of the child nodes (n_j) is true then the Boolean value of the N_j is true. Let $f_1(0) = s$ where $s \epsilon Z_p$ select a polynomial $f_j(.)$ for every non-root nodeN_j. By letting $f_1(0)$ be$f_{parent(N_j)}$. The cipher text can be given as

CT=($B = kg_2^s = ke(g,g)^{\alpha s}$,

C=$g_1^s = \left(g^{\beta}\right)^s = g^{s\beta}$,

$\{E_j = g^{f_j(0)}, E_j^{'} = H_1(a_1)^{f_i(0)}\}_{j \in L} T$)

AB-Decrypt

The data user executes this algorithm by taking the cipher text, secret key and the set of attributes inorder to decrypt the cipher text as per the access policy.

a) Set the Boolean value of N_j is TRUE if N_j is a leaf node and the attribute$a_i \in A \cap S$.

$$v_j = DeNode_1(CT, SK, j, a_i)$$
$$= e(g^r, g^{f_i(0)}) e(H_1(a_i)^{r_i}, g^{f_i(0)})$$
$$/e(g, H_1(a_i))^{r_i f_i(0)}$$
$$= e\left(g^r, g^{f_i(0)}\right) = e(g,g)^{r f_j(0)}$$

The Boolean value ofN_j is not true if the last three equations are not due to the bilinear property.

b) If N_j has child nodes then let S_j be the random set of the n_j sized set of the child nodes *z*. For suppose if the node has x child nodes then it call the DeNode(CT,SK,Z) and stores output as f_x, $f_x \neq \nabla$. If no such set exist then it is not satisfying the access policy otherwise it fulfills the access policy setting N_j value to TRUE.

$f\ _x$ =*DeNode*(CT,SK,Z)

The final result is:

$$f_x = \ e\ (g,g)^{r f_j(0)}$$

In CP-ABE the respective user's private key is used to decrypt the data where the access policy is built into the encrypted data. In CP-ABE the encrypted data can select who can decrypt it whereas this remained as the disadvantage in KP-ABE. The attributes in the user's private key plays a vital role as these are responsible to fulfill the access policy built into the encrypted data. The CP-ABE access control supports in the real time environment. The concept of CP-ABE is also used in MCB-ABE. In MCB-ABE the CP-ABE is used to encrypt the multiple messages with the same public key and the access policy is built into the encrypted data. When the user attributes satisfy the access policy then the corresponding message will be decrypted the remaining message will be in encrypted form because the multiple messages are encrypted together with the same public key.

CONCLUSION

CP-ABE primarily based access management permits a data owner to enforce access management supported attributes of data customers while not explicitly naming the particular information customers. However, CP-ABE supports just one privilege level and therefore isn't suitable for access management to ascendable media. In this paper we presented a basic development of the CP-ABE and how the access structure is built in the CP-ABE. Cloud computing is the highly adaptive technology and mobile devices are becoming widespread the above presented CP-ABE access control helps to free from the computational demanding operations on the cloud server. The experimental results show that the CP-ABE is flexible, scalable, user, accountability, collision, resistant, user revocation. With the assistance of the cloud the acceleration of the decryption increased but it is still slow in some low-end devices because a Integrated exponentiation operation is required.

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, Cipher text-policy attribute-based encryption," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 321V334, 2007.

[2] V Bozovic, D Socek, R Steinwandt, and V. I. Vil- lanyi, \Multi-authority attribute-based encryptionwith honest-but-curious central authority," Interna-tional Journal of Computer Mathematics, vol. 89, pp. 3, 2012.

[3] M. S. Hwang and I. C Lin, \Introduction to Infor-mation and Network Security (4ed, in Chinese)," in*Mc Graw Hill. In Taiwan*, 2011.

[4] A. Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technol-ogy, Technion, Haifa, Israel, 1996.

[5] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext.In R. Cramer, editor, EUROCRYPT, volume 3494 of Lecture Notes in Computer Science, pages 440–456.Springer, 2005.

[6] Waters,B, (2008) “Ciphertext policy attribute based encryption : An expressive, efficient, and provably secure realization”, Cryptology ePrint report 2008/290 .

[7] Goyal, V., Jain,A., Pandey,O., Sahai,A , (2008) “Bounded Ciphertext policy attribute based encryption”, In: Aceto, L.,Damgard,I., Goldberg, L.A., Halldorsson , M.M., INgolfsdottir,A., Walukiewicz, I .(eds) ICALP 2008, Part II. LNCS , Vol 5126, pp 579- 591, Springer , Heidelberg .

[8] Yongdong Wu, Zhuo Wei, and Robert H. Deng , Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks, IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013

[9] Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang, A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments, International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013

[10] A.Balu, K.Kuppusamy, Ciphertext policy Attribute based Encryption with anonymous access policy, International journal of Peer to Peer Networks, pp1-8,Vol 1, Number 1, October 2010