RESEARCH PAPER | Engineering | Volume : 4 | Issue : 7 | July 2014 | ISSN - 2249-555X

Role based Access Control using CP-ABE Algorithm

KEYWORDS: Abstract syntax tree, Cipher text policy attributes based encryption, Role based access control.

Shuriya.B

Phd Scholar, Department of Computer Science and Engineering, RVS Technical campus coimbatore

ABSTRACT *Security is an important property in role based access control system. To preserve the confidentiality and integrity we need certain policies. In this paper we enhance abstract syntax tree (express the user role and permission) with cipher text policy attribute based encryption technique. This will provide the security policy for the administration. The cipher text policy attribute based encryption is much more flexible than plain identity-based encryption.*

INTRODUCTION

The access control to system resources must be provided efficiently and confidentially. The security policy such as Organization policy and Government policy can be made. Requirements includes such as Restrict read access (confidentiality), Restrict write access (integrity)and Restrict execute access (for application systems).

In this work, we construct the role based access structure and also provide security policy using Cipher text policy-attribute based Encryption. When creating a role access structure, the assignment of permissions to each role must be verified. The two or more permission can also be given to the single user. Here, clustering can be performed by classifying user groups. The similar permissions sets are avoided in our work for obtaining throughput.

The CP-ABE is much more flexible than plain identity-based encryption, in that it allows complex rules which specify private keys can decrypt cipher text. The identity-based encryption can be done by using one public key and Master Private Key used to make more restricted private keys. But there is very expressive rules for which private keys can decrypt .They are Private keys have "attributes" or labels and Cipher texts have decryption policies. CP-ABE can be viewed as a generalization of identity-based encryption. So as in identity-based encryption, there is a single public key, and there is a master private key that can be used to make more limited private keys. Using a few keys to encrypt many files may lose the fine grained control we had over access policies. However, specifically, the private keys are associated with sets of attributes or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt. To access any files in remote storage the scalable and reliability is an important property. The more we replicate our files, the more we introduce potential points of compromise and the more trust we require. For this problem CP-ABE may be useful.

ABSTRACT TREE SYNTAX

To specify RBAC policies, the abstract syntax has been extended to include set and set operations to model role-based access control requirements. A set can be used as a component itself or can be an attribute of a component. Basic set operations such as union, compliment, and intersection are allowed. It also includes membership and cardinality. A session can be represented as a component and may have active roles as an attributes. Objects are represented as components and operations performed on them are represented as its states. The membership of a user in a specified role is checked by using the set membership function in Abstract Syntax Tree.

ROLE BASED ACCESS CONTROL

To have effective access control on authorized system, DAC-MACS (Data Access Control for Multi-Authority Cloud Storage) is used. An effective and secure data access control scheme for storage systems can be modeled.

Role based access structure for an organization; the fine grained permission assignment should be created. The important functions for our implementation are user assignment for role and Permission assignment for user.

User assignment for role

The user assignment for role is a function to identify a user for a particular role. The operations such as union, intersection and compliment are allowed. It includes membership and cardinality.

Permission assignment for user

The permission assignment for role is a function used for assigning permission sets for each role in an organization. There may be two or more permission sets for important roles.

Access structure

Consider the set of attributes (A1, A2,..,An), where $A \subseteq 2^{(A1,A2,...An)}$ is specified as monotone. For all $B \in C$, if B C A and $B \subseteq A$ then $C \in A$. An access structure is an collection of non empty subsets with the authorized sets. It also includes that are not in set A is unauthorized sets.

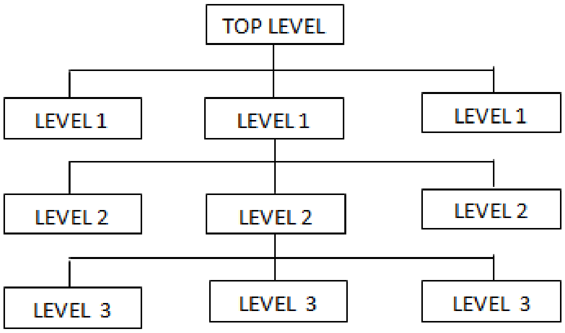

Fig 1: Access structure

The access structure for an organization will have several levels. Each level will have different roles. Each roles will have different permission in access structure. The CP-ABE scheme with efficient encryption/decryption is used for both forward and backward security.

CP-ABE

In CP-ABE attributes play an important role because they are attached to a user's secret key. In the real world, the attributes never remain static. The attributes can be changed dynamically. The following are the requirements of the dynamic attribute-updating scheme:

1. The operations such as add/delete/update can be performed for any dynamic attribute, in any number and at any desired instance.
2. Values must be assigned to a chosen dynamic attribute.
3. The attribute values must be independent of the same to the other when values are modified.

Attribute based encryption

The Bilinear mapping is used for attribute based encryption. Consider a map ^t: Gx×Gy ! GX , from multiplicative groups (Gx, _) and (Gy._) to another multiplicative group (GX , _), with all groups of prime order s. The following are the property for a bilinear pairing:

- Linearity in the first argument
- Linearity in the second argument
- Non-degeneracy (strong)

If the pairing is defined such that Gx = Gy then it is said to be symmetric, otherwise asymmetric.

CPABE Algorithm

In this algorithm, the public parameters such as public key PK and a master key MK is used.

The encryption algorithm takes input parameter such as the public parameters PK, a message M, and an access structure A .

Encrypt (PK,M,A) which will encrypt M and yields an Cipher text . Now only the user who has Possesses a set of that particular Access structure can decrypt the M. Now we can consider A as implicit cipher text.

Key Generation (MK, S). The inputs for the key generation algorithms are the master key MK and a set of attributes S, which describe the key. It generates a private key SK.
Secret (SK, ˜ R). The Secret algorithm takes as input a secret key SK for some set of attributes R and a set ˜ R ⊆ R.It output a secret key S˜K for the set of attributes R˜.

Security model

The cipher texts are identified with access structures and the private keys with attributes in CP ABE. It follows security definition the adversary will choose to be challenged on an encryption to an access structure A* and can ask for any private key SK such that SK does not satisfy SK*

CONCLUSION

We could conclude that our paper describes the security policy for an organization. In this paper we built abstract syntax tree for a role access and to secure the process CP ABE algorithm is used. For any role which has been accessed by user is secured and prevented by CP ABE algorithm. The encryption and decryption technique is used in which key has been protected. In our future work we would like to extend our security policy.

REFERENCE

[1] David F. Ferraiolo and D. Richard Kuhn," Role-Based Access Controls" 15th National Computer Security Conference (1992) Baltimore, Oct 13-16, 1992. pp. 554 – 563. | [2] John Barkley, "Implementing Role-Based Access Control using Object Technology," First ACM Workshop on Role-Based Access Control, Gaithersburg, Maryland, November 30-December 1, 1995. | [3] T. Parker and D. Pinkas, "SESAME Technology Version 3: Overview,"http://www.esat.kuleuven.ac.be/cosic/sesame/doc-txt/overview.txt" | [4] Zhibin Z., and Dijiang H. On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption. http://eprint.iacr.org/2010/395.pdf. | [5] Luan Ibraimi, Qiang Tang, Pieter Hartel and Willem Jonker. Efficient and Provable Secure 1Ciphertext-Policy Attribute-Based Encryption Schemes. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. LNCS, vol. 5451, pp. 1–12. Springer, Heidelberg (2009) | [6] M. Chase. Multi-authority attribute-based encryption. In (To Appear) The Fourth Theory of Cryptography Conference (TCC 2007), 2007. | [7] M. Chuah, S. Roy, I. Stoev. Secure Descriptive Message Dissemination in DTNs. Proceeding MobiOpp '10 Proceedings of the Second International Workshop on Mobile Opportunistic Networking. ACM 2010. | [8] [Waters08/11] Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. PKC 2011 | [9] [LOSTW10]Lewko, A.B., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute based encryption and (Hierarchical) inner product encryption. EUROCRYPT 2010. | [10] [MKE09] Muller, S., Katzenbeisser, S., Eckert, C.: On multiauthority ciphetext-policy attribute-based encryption. Bulletin of the Korean Mathematical Society 2009. | [11] [LW11] Lewko, A., Waters, B.: Decentralizing attribute based encryption. EUROCRYPT 2011. |