International Journal of Engineering & Technology, 7 (4.10) (2018) 396-398

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Novel method to represent Access Tree structure by Context Free Grammar with and-or graph in Key Policy based Attribute based Encryption

K.Senthil Kumar*, D.Malathi[2]

[1]*Department of CSE,SRMIST,Kattankulathur*
[2] *Department of CSE,SRMIST,Kattankulathur*
[1]*senthilkumar.k@ktr.srmuniv.ac.in*
**Corresponding author E-mail: [2]malathi.d@ktr.srmuniv.ac.in*

Abstract

Important and sensitivity data of users in a third party managed internet or cloud always pose various security as well as privacy issues. Attribute-based encryption (ABE) is a pleasant trend in the literature which addresses above problem in an efficient way, and provides data security and fine-grained access control in a decentralized manner,. Key-policy attribute-based encryption (KP-ABE) is an important type of ABE, in which user can decrypt his message with a set of attributes and private keys are embedded with a access control structure which defines which cipher text an user can be allowed to decrypt. In this paper we use a probabilistic context free grammar with an And-Or structure to represent access control structure. And-Or graph has high expressive power hence access control structure can be represented in an efficient manner.

Keywords: *Access tree structure, And-Or Graph, Attribute Based Encryption, Monotone structure*.

1. Introduction

Nowadays many important and sensitive data of users are stored by third parties on internet. Normal encryption and decryption techniques to some extend to help secure data when they are kept in individual domain, but when they are kept in cloud it always pose various risks. Key policy based Attribute based encryption try to overcome this problem in an efficient manner. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. A user is able to decrypt a cipher text if the attributes associated with a cipher text satisfy the key's access structureNormal encryption and decryption techniques to some extend to help secure data. But when the data size increases each user has to be given secret keys which also give rise to lot of traffic in the internet, and more over for same file each user will be given different secret keys to decrypt the data. This situation is not appalling. To overcome this situation Attributed based encryption (ABE) is introduced by Sahai and Waters [1].

ABE is a mechanism that specifies the access control policy to the users and data. In a typical data base environment one wants to allow different user to access their respective documents. ABE always ensures the minimal loss of data even if the storage is compromised. ABE always specifies access control policy by a collection of predicates. Access control policy defines rules that allow some kind of restrictions that is which type of users can access which type of documents, that is user's keys and cipher text are labelled with some set of attributes. So a particular key can decrypt a cipher text if they have same set of attributes.

We organize our paper as follows section 2 deals preliminary notations and definitions, Section 3 deals related work, section 4 our proposed Access tree representation by And-Or graph algorithm, section 5 conclusion.

2. Preliminary Notations and Definitions

In normal control access techniques have the assumption that server is in the domain of the data owner and owner can enforce various access restrictions. But when the server is managed by third party (like in cloud or in internet) user always faces various security risks and possible data loss. To avoid this Sahai et al[1] introduced a Attribute Based Encryption(ABE) .ABE has some interesting properties viz,

1. The ability to represent complex access control policies
2. The complete list of users not known in advance.
3. Collusion resistance (A property by which a collection of users when they combine their keys to decrypt the cipher text and they will be successful if and only if one among them can decrypt the cipher text with his own key in an individual manner) this guarantees only the correct user can access correct information.

2.1 Types of ABE

ABE can be generally classified in to two types

a. If the attributes are embedded in a cipher text and this is known as Key policy based ABE (KP-ABE).
b. If the access control structure is embedded in a cipher text and this is known as cipher text policy based ABE(CP-ABE)

KP-ABE was first introduced by Sahai etal[1] later improved by Goyal et al[2] and Ostrovisky et al[3].In KP-ABE attribute as well as data is encrypted and access structure is send along with secret key.
CP-ABE was introduced by Bethencourt et al[4] both KP-ABE and CP-ABE follows secret key sharing method of Shamir[5]. But CP-ABE is used by many [6],[7],[8] in the literature because of its compactness and efficient representation.
To understand KP-ABE one needs following definitions.

2.2 Definition: (Access Structure)

Let {p1,p2,…pn} be a collection of attributes. A collection A $\subseteq 2^{\{p1,p2,\ldots pn\}}$ is monotone if $\forall$ L,M
with L $\in$A and L$\subseteq$M then M$\in$A
2.3. 2.Secret Share Schemes (SSS)
According to [2] this is a mechanism in which a secret is distributed among n number of parties. Each piece of information is known as a share.SSS defines some specific access structure which tells which parties to combine their shares so as to reconstruct the secret.
In SSS one finds tree access structure to define control policy

2.4 Definition: Access Policy

Policies may be defined over attributes using conjunctions, disjunctions and (k,n)-threshold gates, i.e., k out of n attributes have to be present .
Example:1 To understand the meaning of access control let us consider the following example. In an university attendance entry setting (assume on line attendance entry system) we have different set of users namely professor, Teaching assistant, student, parents of the student and administrator of the online attendance entry system. We can express the access control policy as
((Professor ∧TA ∧Course code)V(Student ∧Parent ∧ Course code) V (Administrator))
Here each credential is called attributes and the whole predicate is called access structure.

2.5 KP-ABE Background

According to Goyal et al[2] KP-ABE consists of following 4 algorithms
1. SETUP algorithm: This takes security parameter and out puts Public Key PK and a Master key MK.
2. Encryption: This is another randomized algorithm with inputs message m ,and a set of attributes γ and produces encryption message E.
3. Key Generation: This algorithm with inputs Access structure ,Public key PK,Master key generates decryption key D.
4. Decryption: This algorithm takes cipher text E and with Decryption key D decrypts the message to get original message.
2.6 Definition: Access Tree
A tree access structure is a kind of tree in which interior nodes are AND and OR Gates and leaves consists of parties or attributes
As in [16] the following example clearly illustrates access tree structure which explains access control policy
Example1:
Assume we have a top secret defense document. Let us introduce following restrictions .The allowable user should be a general in the army AND has experience 2 out of 4 operations namely Op-A, Op- B, Op-C, Op-D
We re-write the access policy as follows:
((General ∧ Army)^ (2-out-of { Op-A, Op-B, Op-C, Op-D}))
The following Fig 1 represents Access tree structure with various control policies.

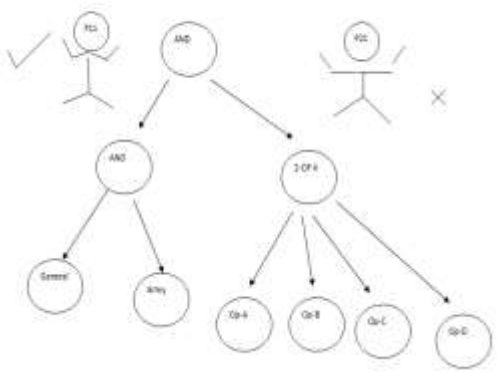

Fig1: Access Tree Structure

The following table represents a particular control access scenario.

Table 1: Control Access Policy Instance

Person	Attributes	Node at Level	Access
Person 1	General ,Army,Op-A,Op-b	At root	Allow
Person 2	Army,Op-A,Op-B	At root	Don't allow

2.7 Definition: Context Free Grammar:

As in Ullmann et al[18] a context free grammar is defined as follows
A grammar G=(N,T,P,L) where
N-A non empty set of non terminals
T-A non empty set of terminals
P-A collection of production rules
L-A special start symbol is said to be context free if production rules are of the form B→*α Where B ∈N, α∈ (NUT)*

3. Related Work

The tree based attribute encryption technique was first introduced by Goyal et al [2] .In this method they use a method of sharing secret elements across the nodes (attributes) of desired policy which in turn recomputed by using Lagrange's interpolation method. Goyal et al [2] used both AND and OR gates. Threshold policy method was used by Sahai et al [1].In this secret key and cipher text both are associated with different attribute sets. They use only AND gates for access structure. But there are some other approaches Muller et al [10] which don't permit arbitrary tree structure. According to Muller et al [10] used Disjunctive Normal Form for access tree structure. **A** Linear Secret Sharing Scheme (LSSS) is another mechanism which uses matrices to represent access policy; here the rows are labeled with attributes of the policy, to produce shares from a secret element. Lewko et al [11] used Boolean formula to produce the matrix. The Boolean formula involves both And Or structures. In normal KP-ABE cipher text size grows exponentially with the number of attributes. Wang et al[13] proposed a new method in which KP-ABE can be done with a constant size of cipher text. They used monotone access structure and proved their method security in Diffie-Hellman[14] condition. According to Delerablee[16] Identity based Broadcast encryption is a convenient method for broadcast encryption and proposed a method with constant size cipher texts with private keys. According to [15] propose a new idea to construct threshold attribute based signatures. Threshold attribute based signatures, defined by a (t, n∗) threshold predicate, ensure that the signer holds at least "t" out of a specified set of n ∗ attributes to pass the verification.

4. Proposed Method

In this paper we introduce a context free grammar with an And-Or graph model to represent access structure policy. And-Or graph has an efficient representational capabilities

4.1 And-or Graph

According to Zhu et al [9] an And-Or graph is a graphical representation which consists of three nodes namely an And node, an Or node and terminal nodes. An And representation consists of decomposition of a node to its sub nodes where as an Or node represents an alternative choice

Example:

A → BCD,

H → NO.

B → E | F,

C → G | H | I.

As in Song Chun Zhu etal[9]the following Fig 2 represents And-Or graph for the above grammar

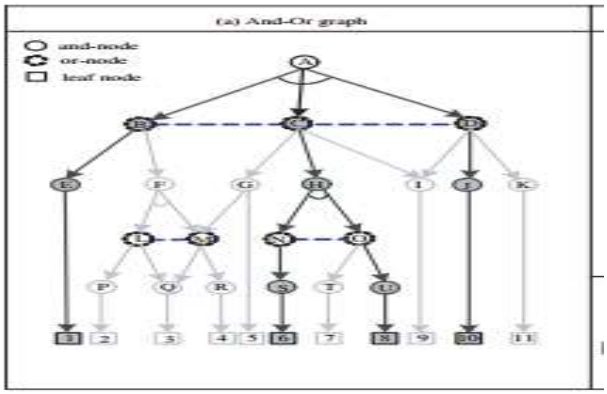

Fig2: And-Or graph

In this paper we use context free grammar for the access tree structure with combination of And-Or graph one can represent various access policy in an efficient manner. Clearly the context free grammar represents various possible access policies.

Definition: Language of Access Policy

We slightly modify the context free grammar as follows

G-{N={And,Or,K out of N threshold},T={Attributes},P,R}

Where R is the root node, P collection of production rules

For example1 The required context free grammar is given by

R-->AB

A-->ga //where g denotes general and a denotes army

B->Op-aOp-b/Op-aOp-c/Op-aOp-d/Op-bOp-c/Op-bOp-d/Op-cOpd

Clearly the language generated by the above grammar represents all possible valid users who can access the respective documents.

5. Conclusion

In this paper we present a novel Context free grammar combined And-Or graph structure to represent Control access policy when can be useful in Attribute Based Encryption. The high representational power of And-Or graph formulization helps one to represent complex control access policies in an efficient manner.

References

[1] Sahai A. and Waters B., Fuzzy identity based encryption, in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Denmark, pp.457-473, 2005

[2] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security, CCS '06, pages 89–98, New York, NY, USA, 2006.

[3] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM conference on Computer and communications security, CCS '07, pages 195–203, New York, NY, USA, 2007.

[4] John Bethencourt, Amit Sahai, and Brent Waters. Cipher text-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321–334, 2007.

[5] Adi Shamir. How to share a secret. Communications of the ACM, Volume 22 Issue 11, Nov.1979,pp 612-613.

[6] Ling Cheung and Calvin Newport. Provably secure cipher text policy ABE. In Proceedings of the 14th ACM conference on Computer and communications security, CCS '07, pages 456–465, New York, NY, USA, 2007.

[7] Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai. Bounded cipher text policy attribute based encryption. In Proceedings of the 35th international colloquium on Automata, Languages and Programming, Part II, ICALP '08, pages 579–591, Berlin, Heidelberg, 2008. Springer-Verlag

[8] Takashi Nishide, Kazuki Yoneyama, and Kazuo Ohta. Attribute-based encryption with partially hidden cipher text policies. IEICE Transactions, 92-A(1):22–32, 2009.

[9] Song-Chun Zhu, and David Mumford. A stochastic Grammar of Images. Foundations and Trends in Computer Graphics and Vision Vol. 2, No. 4 (2006) 259–362.

[10] Müller, Katzenbeisser and Eckert, Distributed attribute-based encryption. Information Security and Cryptology–ICISC 2008. Springer Berlin Heidelberg, 2008. 20-36

[11] Lewko, Allison, and Brent Waters, Decentralizing attribute-based encryption, Advances in Cryptology–EUROCRYPT 2011. Springer Berlin Heidelberg, 2011. 568- 588.

[12] Beimel. Secure Schemes for Secret Sharing and Key Distribution. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996

[13] Changji Wang and Jianfa Luo, An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Cipher text Length, Mathematical Problems in Engineering Volume 2013 (2013), Article ID 810969.http://dx.doi.org/10.1155/2013/810969

[14] W. Diffie, M. Hellman.,New directions in cryptography", IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.

[15] S Sharmila Deva Selvi, Subhashini Venugopalan, C. Pandu Rangan,On the Security of Attribute Based Signature Schemes. IACR Cryptology ePrint Archive 2012: 62 (2012)

[16] C. Delerablee.,Identity-based broadcast encryption with constant size cipher texts and private keys," in Proceedings of the Advances in Cryptology 13th International Conference on Theory and Application of Cryptology and Information Security (ASCIACRYPT '07), vol. 4833 of Lecture Notes in Computer Science,

[17] John E. Hopcroft , Rajeev Motwani, Jeffrey D. Ullman, Introduction to Automata Theory, Languages, and Computation, Addison-Wesley, 2001