International Journal of Pure and Applied Mathematics
Volume 119 No. 14 2018, 75-78
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Access Structures used for the Implementation of Attribute Based Encryption: A Survey

J. Joshua Daniel Raj[1], P. Karthik[2], Samson Immanuel J[3]

[1]Research Scholar, Dept. of ECE, KSSEM, Bangalore.
[2]Professor, Dept. of ECE, KSSEM, Bangalore.
[3]Assist. Professor, Dept. of ECE, Karnuya University, Coimbatore

Abstract

We generate the data and store it or share it in the internet for our convenience and also we would like to embed access settings to the data. One of the most convenient methods used for the decades is to set the access privileges using the probable user attributes is attribute based encryption. In this paper we survey the different access structure that is being used for the implementation of attribute based encryption systems in the modern world. We also have presented the comparisons of the access structures in terms of threshold gates, proof of security and computation cost.

1. Introduction

In the modern era the data is generated at higher rate due to the availability of compact and handheld devices, when the data is transferred to other person using internet, it get stored into the cloud drives and anyone who has a link can have an access to the data. If the data is private and sensitive and we do not want to give access to others, then the normal practice is to encrypt the using cryptography techniques and store it in the cloud. In the private key cryptosystems the owner of the data uses a private key to encrypt the data; the key is communicated to the sender in a very secured way. Only the person who has the same key can access to the data. In some situations where we want to store the data and restrict the access to it, then we use a public key crypto systems, there are many public key crypto systems evolved over the period time among these the one of the most widely used modern public key cryptographic systems is attribute based encryption.

1.1. Attribute based encryption

One of the most widely used encryption scheme to implement the data centric security is to use attribute based encryption[1]–[7], this is a public key encryption, in this the user attributes (eg: role, position, designation) are used to construct a cipher text and secret key. Hence only the user key that matches with the described attributes in the cipher text can decrypt the data. The major two types of ABE schemes are Key-policy ABE (KP-ABE) and Ciphertext-policy ABE (CP-ABE).

1.1.1. Key Policy and Ciphertext Policy Attribute Based Encryption

In KP-ABE[8] shown in figure 1 the owner uses the set of attributes to construct a ciphertext and the private keys are mapped with an access structure. The access structure specifies which type of ciphertext the private keys can decrypt.

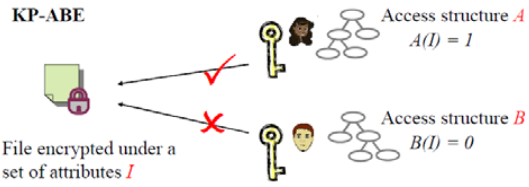

Fig. 1 Key Policy Attribute Based Encryption

In CP-ABE[9] shown in figure 2 the owner uses the user attributes to construct a secret key and access structure is used to construct a ciphertext. In this section we give the background operational details of ABE. The ABE allows monotonic or non-monotonic access structure .

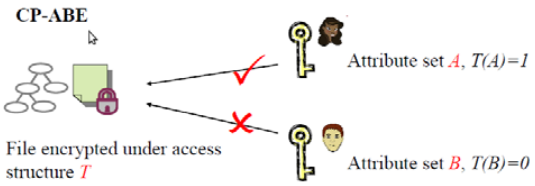

Fig.2 Ciphertext Policy Attribute Based Encryption

1.2 Back ground

In this section we shall discuss an important mathematical detail that comprises the ABE method and the assumptions for implementing data centric security.

A. Bilinear Maps

A Bilinear map is a mathematical function that combines two vector spaces and produces a third vector space and it is linear in operation.[9]

Let $\mathbb{G}$ and $\mathbb{G}_T$ be cyclic groups with the same large prime order q. Then the bilinear map e is defined as: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

Let $\mathbb{G}_0$ be a bilinear group of prime order p, and let g be a generator of $\mathbb{G}_0$. In addition let $e: \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ denote the bilinear map. A security parameter, k will determine the size of the groups. The Lagrange coefficient $\Delta_{i,S}$ for $i \in \mathbb{Z}_p$ and a set, $\mathbb{S}$, of elements in $\mathbb{Z}_p$; $\Delta_{i,S(x)} = \Pi_{j \in S, j \neq i} \frac{x-j}{i-j}$. additionally it employs a hash function $H: \{0,1\}^* \rightarrow \mathbb{G}_0$ that will model as a random oracle.

The properties of bilinear map is as follows

Bilinearity: $\left(g_1^a, g_2^b\right) = e(g_1, g_2)^{ab}$. where g_1 and g_2 are the generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, $a, b \in Z$. (Note that $\mathbb{G}_1$ and $\mathbb{G}_2$ is called the source group and $\mathbb{G}_T$ is called the target group. When $\mathbb{G}_1 = \mathbb{G}_2$, we call it a symmetric bilinear map.
Computability: The bilinear map e is efficiently computable for any pairs given by $\mathbb{G}_1 \times \mathbb{G}_2$.
Non-degeneracy: $e(g_1, g_2) \neq 1$. It means that the map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_2$ to the identity in $\mathbb{G}_T$.

The bilinear maps that satisfy the above mentioned properties are called admissible bilinear maps; this is in fact used in ABE systems.
The remaining part of this paper details the different access structures that have used and its implementation techniques and comparison results.

2. Attribute Based Encryption using Monotonic Access structure

This is a most widely used access structure in the implementation of attributed based encryption algorithm[8], [9]. The access structure is are composed of threshold gates and leaves describe attributes[10]. The AND gate can be constructed as n-of-n threshold gates and OR gates as 1-of-n threshold gates[11], [12]. The access structure is defined as Let $\{P_1, P_2, P_3, \ldots P_n\}$ be set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1, P_2, P_3, \ldots P_n\}}$ is monotone if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. An access structure is a collection A of non-empty subsets of$\{P_1, P_2, P_3, \ldots P_n\}$. The sets in $\mathbb{A}$ are called the authorized sets and the sets not in $\mathbb{A}$ are called the unauthorized sets. The access structure $\mathbb{A}$ contains the set of authorized sets of attributes. This encryption method uses four algorithms [10], [13]

Setup : this algorithm uses implicit security parameter and produces master key and public parameters.
Encryption: this algorithm uses public key, message and access structure as input and generates the ciphertext
Key generation: this algorithm uses the master key and a set of attribute as input and generates secret key.
Decrypt: this algorithm uses the public parameters, ciphertext and secret key for a set of attributes and reproduces the plain text as output.

3. Attribute Based Encryption using Non-Monotonic Access Structure

The non monotonic access structure uses AND, OR and NOT gates, using these gates the negative constraints can be used for key access and generation[14]. The non-monotonic access structure can be well explained with a following example. A project manager of a company is sending a secret message to his team, if he uses the access structure Team Leader AND Bangalore, when anyone who is a team leader and working in a Bangalore location trying to access, the private key would be generated in the monotonic access structure. If the secret information is need to be read only by the Team Leader in the Bangalore project, not by a team leader of other location, it can be specified by using the access formula "Team Leader" AND "Bangalore" (NOT "Chennai"). This will prevent data being accessed by team leaders of other locations.

The non-monotonic access structure is derived from monotonic access structures, initially universal set of attributes are selected, from this set of d attributes are selected for encryption process by the authority. Among these the attributes that are present in this set is called positive attributes and the remaining attributes are called negative attributes. To decrypt the cipher text the user must posses minimum of $d + 1$ attributes.

Let us assume we have a set of attributes $\mathcal{P}$, it consists of both positive and negative attributes. $\mathcal{A}$ is a group of monotonic access structure over $\mathcal{P}$ for which it given as$LSSS\ \{\Pi_{\mathbb{A}}\}_{\mathbb{A} \in \mathcal{A}}$. $\tilde{\mathcal{A}}$ is a non-monotonic access structure over $\mathcal{P}$. The non-monotonic access structure $\tilde{\mathbb{A}}$ is present for$\forall \mathbb{A} \in \mathcal{A}$. Let $\tilde{S} \subset \tilde{\mathcal{P}}$, $\mathcal{N}(\tilde{\mathcal{P}}) \subset \mathcal{P}$, namely, the positive attributes are in $\tilde{S}$, whereas the attributes in $\mathcal{N}(\tilde{S})$ may be positive or negated. Then let $\tilde{S} \subset \mathcal{N}(\tilde{S})$. For every attribute $x \in \tilde{\mathcal{P}}$ but $x \notin \tilde{S}$, we have $x' \in \mathcal{N}(\tilde{S})$. Hence $\mathcal{N}(\tilde{S})$ consists of all attributes in $\mathcal{S}$ and the other attributes are not in $\mathcal{S}$. Hence there is a non-monotonic access structure $\tilde{\mathbb{A}}$ over $\tilde{S}$. This scheme uses four algorithms

Setup : it uses implicit security parameters and provides the public parameters PK and a master key MK.
Encryption: it takes message, set of attributes and the public parameters PK as input and generates ciphertext E.
Key generation: it takes the access structure, master key MK, and the public parameters PK, it provides the decryption key as in output.
Decryption: it takes ciphertext, and the decryption key, public parameters as input and decrypts the ciphertext into a plain text.

4. Attribute based encryption using Hidden Access Structure

This scheme allows the owner of the data to hide the access structures and encrypt it for secure communication. In this the encryptor can use wildcards $\mathcal{W}$ in a hidden manner[15]. To develop an access structure , it uses the notation $\mathcal{W} = [\mathcal{W}_1, \ldots, \mathcal{W}_n]$= [1,1,*,* ,0] where n = 5, it is called as ciphertext policy. The wild card $*$ represents don't care value. This would be considered as an AND gate in the access structure. In order to decrypt the ciphertext the secret key must be associated with 1 for $\mathbb{A}_1, \mathbb{A}_2$ and $\mathbb{A}_5$. And any value for $\mathbb{A}_3$ and $\mathbb{A}_4$.

Let $\mathcal{S}_i = \{\mathcal{V}_{i,1}, \mathcal{V}_{i,2}, \ldots \mathcal{V}_{i,t}, \ldots \mathcal{V}_{i,n_i}\}$ be a set of possible values for $\mathbb{A}_i$ where n_i is the possible value of $\mathbb{A}_i$. Then the attribute list $\mathcal{L}$ for a user is $\mathcal{L} = [\mathcal{L}_1, \ldots, \mathcal{L}_n]$ where $\mathcal{L}_i \in \mathcal{S}_i$ and the generalized ciphertext policy $\mathcal{W} = [\mathcal{W}_1, \ldots, \mathcal{W}_n]$ where $\mathcal{W}_i \subseteq \mathcal{S}_i$.

To encrypt the owner specifies a wildcard for $\mathbb{A}_i$, it corresponds to $\mathcal{W}_i = \mathcal{S}_i$ for $\mathbb{A}_i$. The attribute list $\mathcal{L}$ satisfies the ciphetext policy $\mathcal{W}$ iff $\mathcal{L}_i \in \mathcal{W}_i$ for$1 \leq i \leq n$. The receiver anonymity is obtained by hiding what subset $\mathcal{W}_i$ for each $\mathbb{A}_i$.

This encryption scheme uses four algorithms

Setup: it takes implicit security parameter, and produces public key PK and a master secret key MK.
Key generation: it takes master secret key, attribute list as input and produces a secret key associated with attribute list
Encryption: it takes a message, ciphertext policy as input and produces ciphertext.
Decryption: it takes ciphertext and secret key as input, and decrypts the message.

5. Performance and security analysis

An access structure is a very important part of a attribute based crypto systems. The monolithic access structure would consume less time to search whether the user possess necessary attributes, the non-monolithic access structure consumes more time to search whether the user has the necessary attributes, because it has to check all of the negated attributes also listed in the access structure. The hidden access structure consumes less access time to because most of the attributes are connected with AND threshold gate and furthermore other attributes are don't care. The other comparison results are shown in table 1.

Table 1: Comparison of access structures

Access Structure	Threshold access policy	Threshold gates	Proof of security	Security Level	Computational cost
Monotonic Access Structure	Yes	AND, OR	generic bilinear group Random oracle model	Moderate	Low
Non-Monotonic Access Structure	Yes	AND, OR, NOT	Decisional Bilinear Diffie-Hellman (BDH) assumption	Moderate	High
Hidden Access Structure.	Yes	AND, OR, Don't care	Decisional Bilinear Diffie-Hellman assumption Decision Linear assumption.	High	Moderate

6. Conclusion

In this paper we have surveyed the three most widely used access structures. Our survey reveals that although these access structures were developed a decade ago, still these access structures is being used for the implementation of attribute based encryption schemes. We believe that there is a scope for researchers to design and develop new access structures for the development of efficient attribute based encryption implementations.

References

[1] Chandrasekaran, R. Balakrishnan, and Y. Nogami, "Secure Data Communication using File Hierarchy Attribute Based Encryption in Wireless Body Area Networks," 2018.

[2] J. K. Liu, T. H. Yuen, P. Zhang, and K. Liang, "Time-based direct revocable ciphertext-policy attribute-based encryption with short revocation list," in International Conference on Applied Cryptography and Network Security, 2018, pp. 516–534.

[3] Y. Jiang, W. Susilo, Y. Mu, and F. Guo, "Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing," Future Gener. Comput. Syst., vol. 78, pp. 720–729, 2018.

[4] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, "Auditable $$\backslash$sigma $-Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 1, pp. 94–105, 2018.

[5] S. Canard, D. H. Phan, D. Pointcheval, and V. C. Trinh, "A new technique for compacting ciphertext in multi-channel broadcast encryption and attribute-based encryption," Theor. Comput. Sci., vol. 723, pp. 51–72, 2018.

[6] H. Cui, R. H. Deng, J. Lai, X. Yi, and S. Nepal, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited," Comput. Netw., vol. 133, pp. 157–165, 2018.

[7] M. P. Joshi, K. P. Joshi, and T. Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems," in International Conference on Cloud Computing, 2018.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, New York, NY, USA, 2006, pp. 89–98.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in 2007 IEEE Symposium on Security and Privacy (SP '07), 2007, pp. 321–334.

[10] M. Srivatsa and L. Liu, "Key derivation algorithms for monotone access structures in cryptographic file systems," in European Symposium on Research in Computer Security, 2006, pp. 347–361.

[11] Z. Liu, Z. Cao, and D. S. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 1, pp. 76–88, 2013.

[12] Q. Zhao, Y. Zhang, G. Zhang, and H. Wang, "Ciphertext-Policy Attribute Based Encryption Supporting Any Monotone Access Structures Without Escrow," Chin. J. Electron., vol. 26, no. 3, pp. 640–646, 2017.

[13] G. DeCandia, D. Hastorun, M. Jampani, G. Kakulapati, A. Lakshman, and A. Pilchin, "1 Secret Sharing for Monotone Access Structures."

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based Encryption with Non-monotonic Access Structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY, USA, 2007, pp. 195–203.

[15] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in International Conference on Applied Cryptography and Network Security, 2008, pp. 111–129.