International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 2, May 2014, PP 126-130

Secure and Efficient Ciphertext Policy Attribute Based Encryption without key Escrow Problem

A.MeenaKowshalya, Dr.M.L.Valarmathi
Assistant Professor, Dept of CSE,
Government College of Technology,
Coimbatore, India.

Abstract: *Online data sharing systems such as Microsoft health vault, Google+, Facebook etc., renders security through promising cryptographic solutions via Ciphertext policy Attribute Based Encryption (CPABE). The CPABE scheme is well suited for distributed data sharing systems because the data owner has full control in enforcing access policies and updating the policies. Though the CPABE scheme is advantageous it comes with a major drawback known as the key escrow problem. In this paper, the key escrow problem is resolved by using a Modified Escrow free Key generation Protocol (MEKGP). The modified escrow free key generation protocol ensures that neither the Key Generation Center (KGC) nor the Data storing center can generate the secret keys individually. The KGC and Data storing center generate parts of secret key which are then integrated by the user. In this paper, the KGC need not be assumed to be trustworthy unlike the existing systems. The results show that the modified escrow free key issuing protocol completely eliminates key escrow problem and is efficient. This protocol hasn't been used in the literature and is the newly proposed approach to the best of the author's knowledge.*

Keywords: *Attribute based Encryption (ABE), Ciphertext policy ABE (CPABE), Key escrow problem, Key generation center (KGC), Data storage center, Data Owner (DO).*

1. INTRODUCTION

With the recent data sharing systems users are able to share their lives to the outside world. Every user is tagged with several attributes. A person may wish to publish his personal health record into the social network for expert diagnosis, guidance and to save cost. The name, the type of his alignment becomes his attributes. Since users are defined over their attributes, tradition public key cryptography has gone obsolete. This paved the way for Attribute Based Encryption (ABE) [13]. ABE allows an encryptor to encrypt a document with set of attributes. One can decrypt the same document belonging to the group only if his set of attribute (partially or fully) matches that of the encryptor. ABE comes in two flavors. Key Policy Attribute Based Encryption (KPABE) and Ciphertext Policy Attribute Based Encryption (CPABE). In KPABE, the attributes are associated with the encrypted data and in CPABE the attributes are associated with user credentials. Hence, CPABE is suited for distributed systems because the data owner has full control over enforcing set of attributes over attribute universe [14]. Enforcement of access policies and updating the same is done by the data owner. The system is comprised of a Key Generation Center (KGC), the Data Owner (DO), the data storing center and number of users. The KGC generates its master secret key (MSK) and a public key. With its MSK, the KGC generates the private keys of the users and hence the KGC can decrypt all possible data of the users. In the tradition cryptographic systems, the KGC is assumed to be trustworthy [15]. Considering the distributed data sharing environment the Data Owner may intend only designated users decrypt the data. Such a problem is known as the Key Escrow problem [12].Figure 1 depicts the typical architecture of the data sharing system.

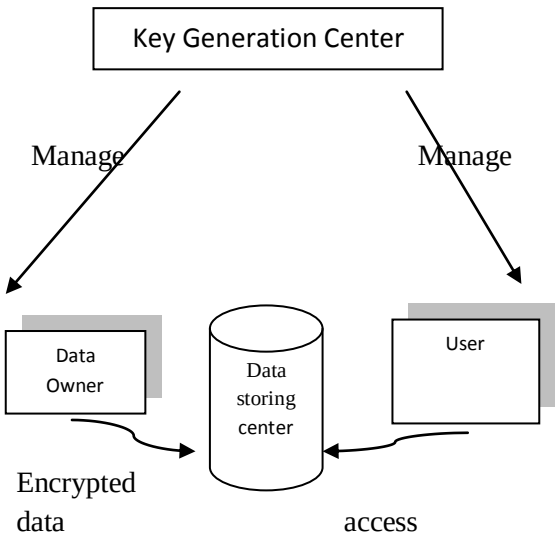

Figure 1. *Components of a data sharing system*

2. RELATED WORK

Several solutions to the key escrow problem have been stated in the literature. Most of the existing CPABE schemes were constructed on an architecture where a single trusted authority or the KGC generates the secret keys of the users [3] [5] [6] [8] [9] [10]. Guoyan Zhang, Lei Liu, Yang Liu [2] proposed a solution to resolve key escrow problem. The authors introduced another secret key that the KGC cannot obtain. This solution doesn't increase length of the public key and the Ciphertext but the overhead in terms of rekeying and the number of messages increased dramatically in the order of $O(n^2)$. Chase and chow [4] proposed a distributed KPABE scheme where all disjoint attributes take part in key generation. They cannot pool their data and link multiple attributes belonging to the same set of user. This solution was effective in resolving the key escrow problem but the communication overhead rose up to $O(n^2)$ since all attribute authority must communicate among each other for key generation. An additional $O(n^2)$ key components need to be stored besides attribute keys, where n is the number of authorities. Chow [7] proposed an anonymous private key generation protocol where the KGC issues a private key to an authenticated user without knowing the list of identities. This kind of scheme works well if attributes are treated as identities i.e., Chows key generation protocol is suited only for Identity Based Encryption (IBE). IBE is a generalization of ABE. This scheme cannot be adopted for CPABE since user's identity is attributes which are not public. Junbeom Hur [12] proposed a secure two party computation protocol for resolving the key escrow problem. The secure 2PC protocol ensures that none of them (KGC and the data storing center) could generate the key all alone. In Hur's proposed system the KGC need not be assumed to be trustworthy. The secret key generation is done by the KGC and data owner. The issue with Hur's approach is that the user has to contact the KGC and the data storing center before getting set of keys. The KGC is responsible for authenticating the user and issue attributes to him if he is entitled to the attributes. The KGC and the data storing center generate parts of secret keys for the user. None of them could generate the entire secret key all alone and thus the key escrow problem is resolved. The drawback with this approach is that the data owner who is responsible for enforcing and updating access policies doesn't take part in issuing attributes. In the proposed system, the data owner, the data storing center and the KGC can issue attributes to the users. By any means the system becomes well defined over a set of user attributes.

The rest of the paper is organized as follows: Section 3 depicts the cryptographic background required for CPABE. Section 4 describes the proposed system. Section 5 shows the experimental results and Section 6 concludes the paper.

3. PRELIMINARIES

3.1 Cryptographic Background

3.1.1 Access Structures

Let $\{P^1, p^2, p^3 \ldots P^n\}$ be set of parties. A collection $A \subseteq 2^{\{P1, p2, p3 \ldots Pn\}}$ is monotone if $\forall$ B,C: if B ε A and B $\subseteq$ C, then C ε A. A monotone access structure is a collection of A non empty subsets of $\{P^1,, p^2, p^3 \ldots P^n\}$ i.e., A ε $\{P^1, p^2, p^3 \ldots P^n\} \setminus \{\emptyset\}$. The sets in A are called authorized sets and the sets not in A are called unauthorized sets.

3.1.2 Bilinear pairings

Let G_0 and G_1 be a multiplicative cyclic group of prime order p. Let g be a generator of G_0. A map $e : G_0 \times G_0 \rightarrow G_1$ is said to be bilinear if $e(P^a, Q^b) = e(P,Q)^{ab}$ for all P,Q ε G0 and all a, b ε Z_p^* and non degenerate if $e(g, g) \neq 1$ for the generator g of G^0. We say that G_0 is a bilinear group if the group operation in G_0 can be computed efficiently and there exists G_1 for which the bilinear map e: $G_0 \times G_0 \rightarrow G_1$ is efficiently computable.

3.1.3 Bilinear Diffie-Hellman (BDH) Assumption

Using the above notations, the Bilinear Diffie-Hellman problem is to compute $e(g, g)^{abc}$ ε G1 given a generator g of G0 and elements g^a, g^b, g^c for a, b, c ε Z_p^*. An equivalent formulation of the BDH problem is to compute $e(A,B)^c$ given a generator g of G0, and elements A,B and g^c in G0.

4. MODIFIED ESCROW FREE KEY GENERATING PROTOCOL (MEKGP)

The KGC and the data storage center generate parts of the secret key. These parts are combined into a single secret key by the user. Before key generation the user authenticates himself from the KGC. The data owner, the KGC and the data storing center take part in providing attributes to the user if the user is entitled to the set of

attributes over a universe. This is the first approach where the data owner also takes part in providing attributed to user. The secure two party computation 2PC protocol deters the KGC and the data storing center from generating the secret key all alone i.e., none of them could generate the secret key by themselves. The secure 2PC protocol also prevents the KGC from decrypting the Ciphertext of users since the identity of the users are not public. Only the data owner has the entire access control over users. The secure 2PC protocol consists of the following algorithms.

1. Setup:

pp ← setup( ) (1^{λ}). The setup phase outputs the system public parameters pp.

2. (PK_k, MK_k) ← KGC Keygen( ), the KGC outputs the public and the private key pairs.

3. (PK_d,MK_d) ← DSC Keygen( ), the data storing center outputs the public and the private key pairs.

4. S ← DO(ID_t), the data owner outputs the set of attributes to the user.

5.$KCom_d(MK_d,ID_t,$ ⟷ $aux_t)$ $KCom_k(MK_k,ID_t,aux_t)$

$KCom_d$ and $KCom_k$ are two key generation algorithm that execute the user secret key between the KGC and the data storage center.

6. $SK_{k,\ ut}$ ← $Issuekey_k(aux_t, S)$. The KGC takes as inputs the auxiliary key and set of attributes S of the user and outputs a secret key $SK_{k,\ ut}$

7. $SK_{d,\ ut}$ ←$Issuekey_d$ ( ). The data storing center takes nothing as input and outputs a secret key $SK_{d,\ ut}$

The KGC and the data storing center generate their public and private key pairs. After the user is authenticated by the KGC, the KGC and the Data storing center starts the secure 2PC protocol. The user receives two secret key components. One from the KGC $SK_{k,\ ut}$ and another from the data storing center $SK_{d,\ ut}$. The user derives the whole secret key from the two components. The data owner and the data storing center also take part in the definition of attribute set for the user. Unlike the existing schemes where only the KGC and partially the data storing center defines the attributes of a user.

5. EXPERIMENTAL RESULTS

The CPABE toolkit from the Stanford crypto was used for simulation. The dataset was collected from Amazon sports review which consists of 510,991 user reviews from June 1995 to March 2013. The set up phase, key generation phase and the re-keying phase shows a complexity of O(log n). The proposed method was compared with three other schemes namely Betherncourt, Sahai, Waters (BSW) scheme [5], Attarpadung and Imai (AI) scheme [1], Yu, Wang, Ren, Lou (YWRL) scheme [11] and the Junbeom Hur (JH) scheme [12]. The comparative results of various approaches are listed in the following table 1. Each cryptographic operation was performed using the Pairing Based Cryptography (PBC) library version 0.5.14 Table 1 show that the proposed scheme resolves the key escrow problem completely and has the lowest complexity. Table 2 depicts the computational cost involved in the pairing operation, exponentials in G0 and G1. The table show that the modified escrow free key generational protocol (MEKGP) is efficient and secure when compared to [12] [5] [1] and [11]. The public key parameters were selected to provide a 60 bit security level. The implementation uses a 160 bit elliptic curve group based on the super singular curve $y^2=x^3+x$ over a 512 bit finite field. The computational cost is analyzed with respect to pairings, exponentiation in G0 and G1.the hash operations are negligible and hence ignored in the result. We assume a binary tree as an access tree.

Table 1. *Comparison of efficiency*

System	Key escrow problem	Complexity
BSW [5]	Yes	$O(n^2)$
AI [1]	Yes	O(n)
YWRL [11]	Yes	$O(n^2)$
JH [12]	No	O(n)
Proposed	No	O(logn)

Table 2. *Computational costs*

Operation	Owner	User
Pairing		2k+2
Exp in G0	2t+1	nk
Exp in G1	1	Logt
Computational ms	2t+1	(5.8+n)k+0.2 logt+5.8

6. CONCLUSION

The CPABE scheme is a powerful cryptographic solution to the issues of updates of access policies in a distributed data sharing system. In this paper, we proposed a Modified Escrow free Key Generation Protocol (MEKGP) that completely removes the problem of key escrow. This is the first and foremost paper that supports the definition of access policies by the KGC, the data storing center and the data owner. None of the approaches in literature allow the data owner to define set of attributes. The data owner could only have full access right on controlling the defining set of polices and can update them. The key escrow problem was removed by the MEKGP that establishes a secure 2P computational protocol between the KGC and the data storing center. Unlike the other existing approaches where the KGC is assumed to be trustworthy, this paper has no such assumptions. Experimental results show that the MEKGP outperforms all the other methods [5] [11] [12] [1] by completely eliminating the key escrow problem and is efficient.

REFERENCES

[1] N. Attarpadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," Proc. Int'l Conf. Palo Alto on Pairing-Based Cryptography (Pairing), pp. 248-265, 2009

[2] Guoyan Zhang , Lei Liu , Yang LiuAn "Attribute-Based Encryption Scheme Secure against Malicious KGC" Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012

[3] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt '05), pp. 457-473, 2005

[4] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy,pp 321-334,2007

[6] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007

[7] S.S.M. Chow, "Removing Escrow from Identity-Based Encryption," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography (PKC '09), pp. 256-276, 2009

[8] L. Cheung and C. Newport, "Provably Secure Ciphertext Policy ABE," Proc. ACM Conf. Computer and Comm. Security, pp. 456-465, 2007

[9] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded Ciphertext Policy Attribute-Based Encryption," Proc. Int'l Colloquium Automata, Languages and Programming (ICALP), pp. 579-591, 2008

[10] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. Int'l Symp. Information, Computer, and Comm. Security (ASIACCS), pp. 343-352, 2009

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010

[12] Junbeom Hur "Improving Security and Efficiency in Attribute based Data Sharing" IEEE Transactions on Knowledge and Data Engineering Vol:25 No:10 year 2013

[13] V Goyal, O Pandey, A Sahai, B Waters "Attribute-based encryption for fine-grained access control of encrypted data" Proceedings of the 13th ACM conference on Computer and communications, 2006.

[14] Shucheng Yu, cong Wang, Kul Ren "Attribute Based Data Sharing with Attribute Revocation", Proceeding of ASIACCS'10 April 13-16, Beijing, China, 2010.

[15] Piyi Yang, Zhenfu Cao, Xiaolei Dong "Chosen Ciphertext Secure Certificateless threshold Encryption in the Standard Model" Information Security and Cryptography,4th International Conference, Bejing, China, Inscrypt 2008

[16] The Pairing-Based Cryptography Library, http://crypto.stanford.edu/pbc/, 2012.

AUTHOR'S BIBLIOGRAPHY

Prof.A.MeenaKowshalya is with the department of Computer Science and Engineering, Government College of Technology. Her current areas of research include Information Retrieval, Information Security and Multidimensional data structures.

Dr.M.L.Valarmathi has over 30 years of experience in the department of Electrical Sciences and Computer Science Engineering disciplines. Her research interests include Image Processing, Data Mining, Optimization Techniques and Mobile Computing

[17] A. C. Yao, How to generate and exchange secrets, Proceedings 27th Symposium on Foundations of Computer Science (FOCS), IEEE, 1986, pp. 162–167.