ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Cipher text Policy Attribute Based Encryption Using 2Party Computation Protocol in Data Sharing

G.K.Kartika

Assistant Professor, Dept. of I.T., V.B.I.T, Ghatkesar, R.R.Dist, Telangana, India

ABSTRACT: Data sharing paradigm in distributed systems like online social networks or cloud computing demands and concerns for distributed data security. The most challenging issues in data sharing systems is the impulsion of access policies and the support of policies updates. The promising cryptographic solution to this issue is Cipher text policy attribute-based encryption (CP-ABE). It allows data holders to define their own access policies over user attributes and impose the policies on the data to be distributed. But the major drawback in this technique is the key escrow problem where the key generation center(KGC) decrypts the messages addressed to specific users by generating their private keys which is not suitable for data sharing scenarios where the data holders would be interested to make their private data accessible to designated users only. The other issue that arises after applying CP-ABE technique in the data sharing system is the user revocation since the access policies are defined only over the attribute groups. Therefore in this paper, we propose a contemporary CP-ABE scheme for overcoming the first issue of key escrow problem in data sharing systems. The proposed scheme looks forward for the following achievement- the key escrow problem is solved using the secure two-party computation protocol between the key generation center and the data-storing center, The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.

KEYWORDS: Cipher text Policy, Data sharing, attribute-based encryption, removing escrow.

I. Introduction

In Attribute based Encryption, attributes are focused for important role as a part of which they are segregated to generate a public key for encrypting data and also used as access policies to control user access.This access policy is flavoured in two---First is the key policy and second is the Ciphertext Policy.Key Policy attributes are used for describing encrypted data and policy implemented in user's key. Whereas Ciphertext policy attributes describe the access structure on the cipher text. Some of the benefits that the users get out of it are: Essentially decreasing the communication overhead of the internet along with a fine grained access control which resolves the issue of untrusted storage of secure data and sharing of data. In Ciphertext Policy, the key generation center (KGC) generates private keys of users by applying the KGC's master secret keys to associated set of user attributes. Thus, the major advantage of this approach is to largely reduce the need for processing and storing public key certificates under traditional public key infrastructure (PKI). However, one of the major drawbacks of this approach is the key escrow problem. The KGC can decrypt the ciphertext that is addressed to the distinct users by generating their attribute keys. This could be a possible threat to the data confidentiality or privacy in the data sharing systems as shown in Fig.1.

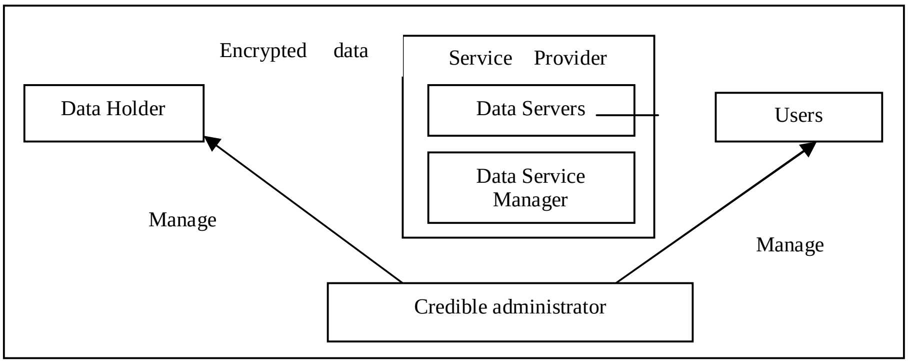

Fig.1: Overall Architecture of Data Sharing systems.

Attribute based Encryption (ABE) is one of the techniques which suits the data sharing with encryption concept by providing a way of defining access policies based on different attributes of the requester environment (or) the data object. Especially cipher text policy attribute based encryption enables Data Holders to define their own access policies over user attributes and enforce the policies on the data to be distributed[5][6]. The major drawback is that the key generation center (KGC) can decrypt any message which is addressed to a specific user by generating his/her private key. This is not suitable for data sharing scenarios where the Data Holder would like to make their private data only accessible to designated users. This problem is known as Key Escrow problem [7][8]. The other problem to be solved is key revocation where the users change their associate attributes at same time (or) private keys may be disclosed and each attribute in the system makes it insecure. This issue is creating more problems in ABE, since each attribute in the system is shared by group of users. And the revocation of any attribute (or) a user in that group, would affect all the other users existing in that group which in turn results in vulnerabilities during rekeying procedure.

In the proposed scenario, a unique Cipher Policy Attribute Based Encryption Technique is used for secure data sharing systems and to resolve the key escrow problem using a Key issuing protocol called 2-Party Computation (or) rather 2PC protocol that accomplishes the data sharing system characteristics. This generates secret keys for the users with their own master secret keys between Key Generation Center (KGC) & the Data Storing Center (DSC). Using this 2PC protocol, master secret information is separated from KGC & DSC in such a way that none of them could raise the whole set of user keys all alone. Thus enforcing data confidentiality and privacy against KGC & DSC individually (or) as a whole.

A. *Data Holder*

It is a client who owns data, and wishes to upload it into the external data storing centre for ease of sharing or for cost saving. A Data Holder is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it as shown in Fig.2. Data Holder to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

B. *Data Storing Centre*

It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data storing centre is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control. Data storing centre store the data. Data Storage Centers provides offsite record and tape storage, retrieval, delivery and destruction services.

C. *User*

This is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the Data Holder, and is not revoked in any of the attribute groups, then he will be able to decrypt the cipher text and obtain the data.

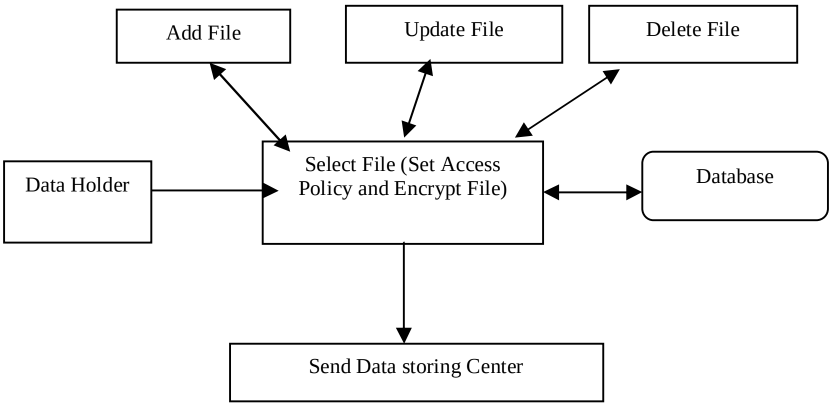

Fig.2: Data Holder (Set Access Policy, Encrypt File)

D. Key Generation Centre

It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted.

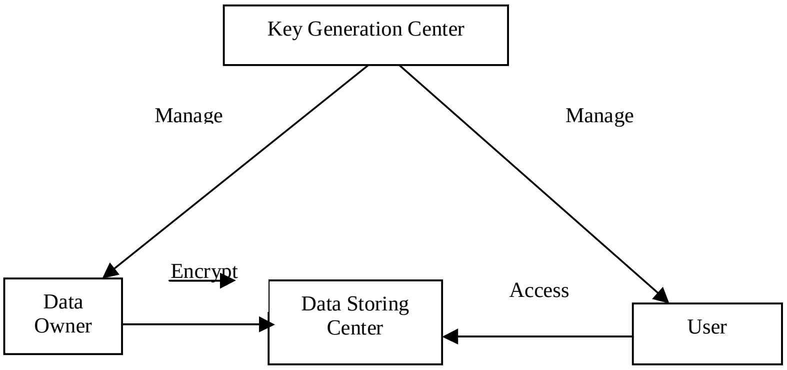

Fig 3. Nodal Structure of Data Sharing System.

The node structure of the Attribute based data sharing system is shown in Fig. 3. The nodes involved are admin and clients which stands as UI for the system. The nodes are Key Generation Centre (KGC) is a key authority that generates public and secret parameters for CP-ABE. Data storing center is an entity that provides a data sharing service. The data storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control. It is a client who owns data, and wishes to upload it into the external data storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. User is an entity who wants to access the data.

II. RELATED WORK

In this section we present the different methods those are used for ABE with their advantage and problem.

- In [3], L. Ebrahimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker proposed a mediated Cipher text-Policy Attribute-Based Encryption (CP-ABE) which extends CP-ABE with instantaneous attribute revocation.
- In [1], A. Sahai and B. Waters introduced the concept of Fuzzy Identity Based Encryption, which allows for error-tolerance between the identity of a private key and the public key used to encrypt a cipher text. They described the

scheme under the Selective ID model by reducing it to an assumption that can be viewed as a modified version of the Bilinear Decisional Diffie Hellman assumption .

- In [2], J. Bettencourt, A. Sahai, and B. Waters presented system for Cipher text-Policy Attribute Based Encryption. Our system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt.
- In [4], Junbeom Hur specified the cause cases of corruption of KGC and corrupted data storing center, He has provided with a proof of 2pc protocol. And presented new efficient and secured method for data sharing systems. But the limitation of this system was reliability and load balancing under real time environment.

III. Proposed algorithm

Our Protocol-The 2Party Computation Protocol for Escrow Free Key Issuing:

The Key Generation Center(KGC) and the Data Storage Center(DSC) generate parts of the secret key. These parts are combined into a single secret key by the user. Before key generation the user verifies himself from the KGC. The data holder, the KGC and the data storing center take part in providing attributes to the user. This is the first approach where the data holder also takes part in providing attributes to user. The secure two party computation protocol prevents the KGC and the data storing center from generating the secret key all alone.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 holder has the entire access control over users. The secure 2PC protocol consists of the following algorithms.

1. Setup:
2. $pup \leftarrow setup\,()(1^{\lambda})$ The setup phase outputs the system public parameters pup.
   $(P_k, M_k) \leftarrow \mathrm{KGC\ Keygen}(\,)$,the KGC outputs the public and the private key pairs.
3. $(P_d, M_d) \leftarrow \mathrm{DSC\ Keygen}(\,)$, the data storing center outputs the public and the private key pairs.
4. $S_t \leftarrow \mathrm{DH}(ID_t)$, the data holder outputs the set of attributes to the user.

5.$KC_1(M_d,ID_t,KC_2(M_k,ID_t,aux_t)KC_1$ and KC_2 are two key generation algorithm that execute the user secret key between the KGC and the data storage center.

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

7.$SK_{d,ut} \leftarrow \mathrm{Issuekey}_d(\,)$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 holder 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.

IV. Simulation Results

In Ciphertext Policy, the key generation center (KGC) generates private keys of users by applying the KGC's master secret keys to associated set of user attributes. Thus, the major advantage of this approach is to largely reduce the need for processing and storing public key certificates under traditional public key infrastructure (PKI). The KGC can decrypt the ciphertext that is addressed to the distinct users by generating their attribute keys. The possible threat to the data confidentiality or privacy in the data sharing systems is Key Escrow problem as shown in Fig.1.

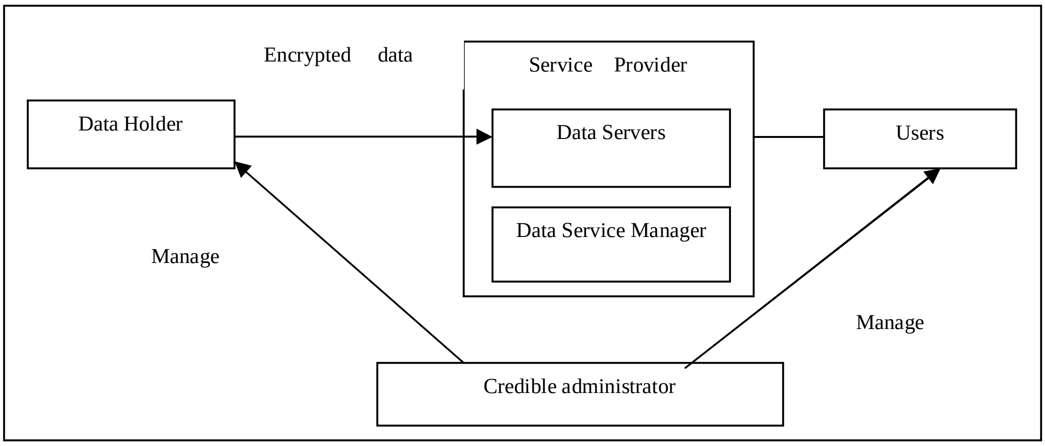

Fig.1: Overall Architecture of Data Sharing systems

It is a client who owns data, and wishes to upload it into the external data storing centre for ease of sharing or for cost saving. A Data Holder is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it as shown in Fig.2. Data Holder to get key from key generator Encrypt the file. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.

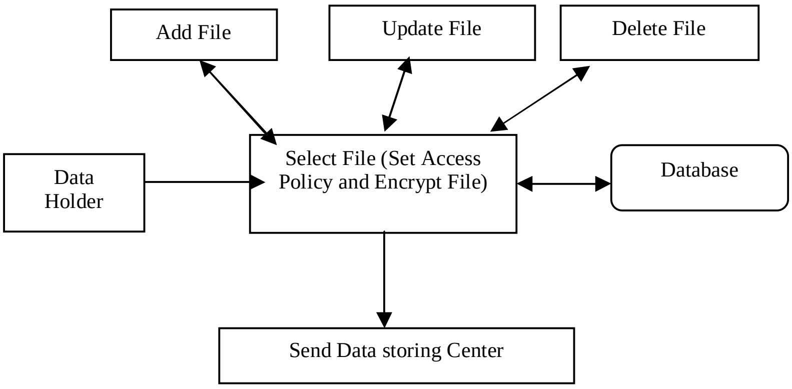

Fig.2: Data Holder (Set Access Policy, Encrypt File)

The node structure of the Attribute based data sharing system is shown in Fig. 3. The nodes involved are admin and clients which stands as UI for the system. The nodes are Key Generation Centre (KGC) is a key authority that generates public and secret parameters for CP-ABE. Data storing center is an entity that provides a data sharing service. The data storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control. It is a client who owns data, and wishes to upload it into the external data storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it. User is an entity who wants to access the data.

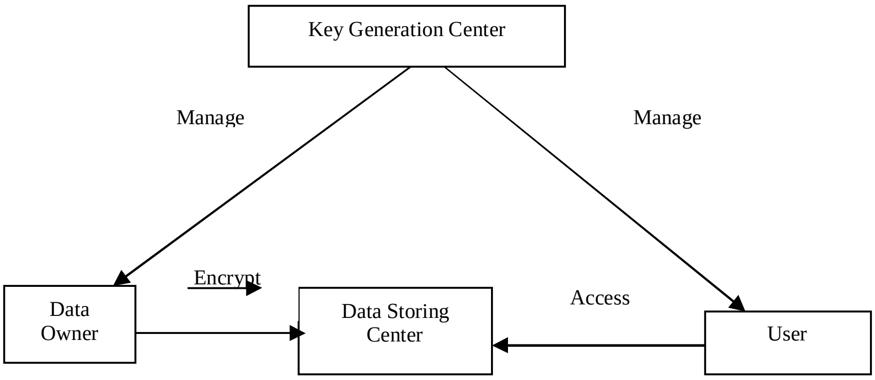

Fig 3. Nodal Structure of Data Sharing System.

V. CONCLUSION AND FUTURE WORK

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 2Party Computation Protocol that completely removes the problem of key escrow. This paper supports the definition of access policies by the KGC, the data storing center and the data holder. None of the approaches in literature allow the data holder to define set of attributes. The data holder could only have full access right on controlling the defined set of polices and can update them. The key escrow problem was removed by the 2PC protocol that establishes 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. Unlike the other existing approaches where the KGC is assumed to be trustworthy, this paper has no such assumptions. In future we can consider these solution on the multimedia files and the system is lacking reliability factor, improvement in these pin holes can be done.

REFERENCES

[1] A. Sahai and B. Waters. Fuzzy identity based encryption. In Euro crypt 2005.
[2] J. Bethencourt, A. Sahai, and B. Waters, “Cipher text-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[3] Pieter Hartel,Willem Jonker” Efficient and Provable Secure Cipher text-Policy Attribute-Based Encryption Schemes ” .
[4] Junbeom Hur “Improving Security and Efficiency in Attribute-Based Data Sharing” IEEE transactions on knowledge and data engineering, vol. 25, no. 10, October 2013.
[5] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,“Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application,” Proc. Int’l Workshop(WISA ’09), pp. 309-323, 2009.
[6] 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.
[7] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[8] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-Based Encryption with Non-Monotonic Access Structures,” Proc. ACMComputer and Comm. Security, pp. 195-203, 2007.

BIOGRAPHY

G.K.Kartika, M.Tech (Computer Science and Engineering) from Vignana Bharathi Institute of Technology, B.Tech (Information Technology) from Syed Hashim College of Science and Technology. She is having Eight years of academic experience currently working as Asst Prof at Vignana Bharathi Institute of Technology. She has guided many UG & PG students. Her research areas include Data Mining, Network security, Software Engineering, Databases.