www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12449-12452

Design secure sharing protocol

Kamini H. Gonnade, Fazeel Zama

(Student)
Computer Science and Engineering
Nagpur University
Nagpur, India
kaminigonnade12@gmail.com

(Assistant Professor)
PG Computer Science and Engineering
Nagpur University
Nagpur, India
fazeel.zama20@gmail.com

Abstract— ***In this paper, our main issue is an authorization and providing the data security for various applications in web services in a network. Cloud Computing is a revolutionary IT field and we are using this technology for various purposes. With the increasing use of the data sharing in distributed systems such as online social networks or cloud computing, there is increasing in concerns for data security while distributing or sharing data. Here, Ciphertext policy attribute-based Encryption(CP-ABE) is becoming cryptographic solution to above issue of secured data sharing among network. Also, we will have these achievements :1) key escrow problem could be solved by escrow-free key issuing protocol, where key is generated using the secure two-party computation between the key generation center and the data-storing center 2) fine-grained user revocation per each attribute could be done by using anonymous id algorithm where sharing of data will be done on attribute basis.***

Keywords- Data integrity, Data sharing, attribute-based encryption, removing escrow, privacy protection.

1. INTRODUCTION

Cloud Computing is a revolutionary IT field in today's world. With the recent development in network and computing technologies, people can share their private data with their closed one's among network. So, for sharing data, the use of cloud computing is increasing. People can share their data through online social media like Facebook, what's app, etc. In this way, due to the development and increasing use of internet, people from various parts of world are coming closer. Also, while sharing the data among network, some security problems and access control problem may arises, which we have to handle in this paper. Improper use of the data by the storage server or unauthorized access by outside users could cause threats to data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Attribute-based encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control. A Ciphertext policy attribute-based Encryption (CP-ABE) is cryptographic solution to the issue of secured data sharing among network. This will enable data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed or shared among different people in network. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy.

Also, while using CPABE , some problems may occurs. The key generation center (KGC) generates private keys of users by applying the KGC's master secret keys to users' associated set of attributes. As there is only one person who is responsible for making key, we cannot trust on that person. Because KGC is generating key, so if possible KGC can also decrypt it and we can loose security while sharing data.So, we have to solve this problem. Another challenge is key revocation. some users may change their attributes at some time, and some private keys might be compromised, so the key revocation or update for each attribute is necessary in order to make systems secure.

2. OVERVIEW

In this paper, we propose a novel CP-ABE scheme for a secure data sharing, which features the following achievements and here, we are representing the overview of operations which will perform in this paper. Data confidentiality and secure data sharing is important concept, which will discuss further.

Data confidentiality: The delivered contents cannot be viewed by unauthorized entities, including unauthorized proxies and other users besides the requester. Proxies authorized by the publisher to process the contents can view the data.

Data sharing: Data will be shared securely by using 2PC protocol among network. Our model will include encryption and decryption of data to share data securely and that data should reach to correct user.

3. EXISTING SYSTEM

In existing system, they have used following methods:

3.1. Two Party Computation(2PC) protocol:

The Two party computation protocol helps to share data securely.Following things are achieved in existing system.

3.1.1. Key Escrow Problem:

The very first problem occurs is key escrow problem which is resolved by a key issuing protocol. The main task of the key issuing protocol is that the key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC (Key Generation Centre) and the data-storing center with their own master secrets. The 2PC protocol restricts them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Hence, users are not required to fully trust on either the KGC or the data storing center in order to protect their data to be shared. Data confidentiality and privacy can be cryptographically enforced against any curious KGC or data-storing center.

3.1.2. Fine grained user revocation:

The immediate user revocation can be done via the proxy encryption mechanism along with the CP-ABE algorithm. Here, the attribute group keys are selectively distributed to the valid users in each attribute group, which then are used to re-encrypt the cipher text encrypted under the CPABE algorithm. The immediate user revocation enhances the backward/forward secrecy of the data on any membership changes. Data owners need not be concerned about defining any access policy for users, but data owner just need to define only the access policy for attributes as in the previous ABE schemes. Therefore, the proposed scheme is the most suitable for the data sharing scenarios where users encrypt the data only once and upload it to the data-storing centers and leave the rest of the tasks to the data-storing centers such as re-encryption and revocation.

4. DATA SHARING ARCHITECTURE

4.1. System Description and Key Management:

4.1.1. Key generation center:

It is a key authority that generates public and secret parameters required for CP-ABE and it is in charge of issuing key, revoking key and updating attribute keys for users. It also grants differential access rights to individual users based on their attributes. This key generating center is quite honest in doing their task, but we have to prevent encrypted data so that security should be maintained.

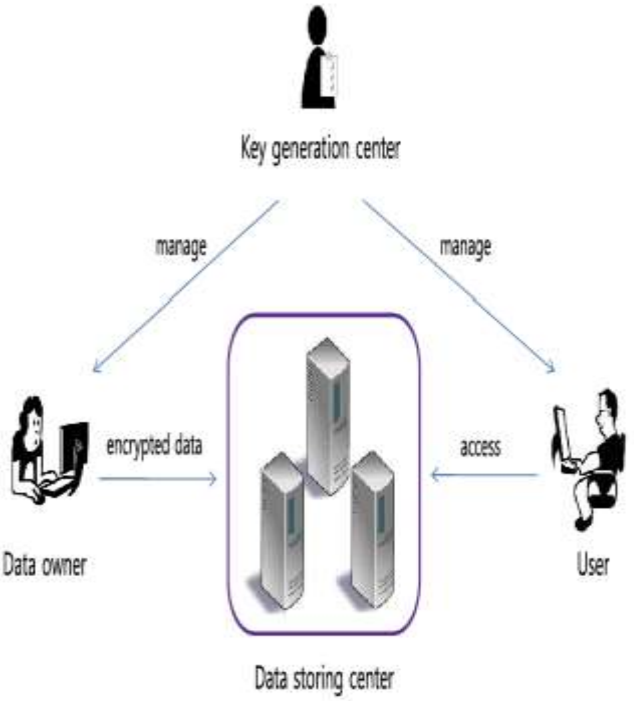

Fig 1: Architecture of data sharing system

4.1.2. Data-storing center:

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 some contents services. Also, the data-storing center is another key authority that generates personalized user key with the help of KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce fine-grained user access control. The data storing center is also trustworthy like KGC.

4.1.3. Data owner:

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 owner can send any type of data, whatever data he wants to send to other person. A data owner is responsible for defining (attribute-based) access policies, and enforcing it on its own data by encrypting the data under the policy before distributing it.

4.1.4. User:

It is an entity who wants to access the data from owner. If a user possesses a set of attributes satisfying the access policy of the encrypted data and is not revoked in any of the valid attribute groups, then user will be able to decrypt the cipher text and obtain the data. So the user will get the data securely and here sharing of data will occurs.

4.2. Threat Model and Security Requirements:

4.2.1. Data confidentiality:

Unauthorized users who do not have enough attribute satisfying the access policy should be prevented from accessing the plaintext of the data. So, we can prevent data to be accessed by every user.

4.2.2. Collusion resistance:

Collusion resistance is one of the most important security property required in ABE systems. As the number of users increases, there may be chances of collusion in network. We should handle it properly.

5. PROPOSED SYSTEM

We have added some points in existing system.

5.1. Two Party Computation(2PC) protocol:

5.1.1. Escrow-Free Key Issuing Protocol for CP-ABE:

The KGC and the data-storing center are involved in the user key issuing protocol. In this protocol, a user is required to contact the two parties before getting a set of keys and the secret key is generated through the secure 2PC protocol between the KGC and the data-storing center. Both KGC and data storing center generates their own master key's and issue independent key components to a users. Then, the user is able to generate the whole secret keys with the key components separately received from the two authorities, here KGC and data storing center. The secure 2PC protocol restricts them from knowing each other's master secrets so that none of them can generate the whole secret keys of a user alone. As none of them will be able to know each other's master key, so security will be maintained while sharing the data among network. To make the key issuing protocol escrow free, the CPABE works as follows.

5.1.1.1. Key generation:

The KGC and the data-storing centre both are involved in the following key generation protocol.

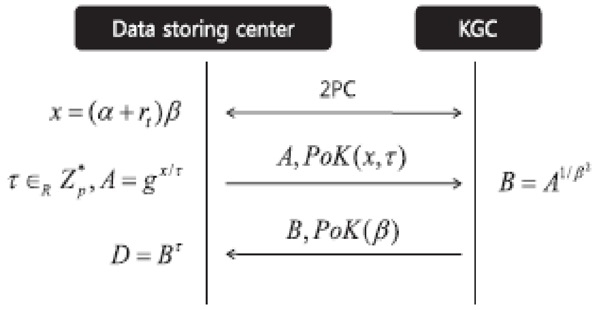

Fig. 2 Key generation protocol.

$\text{KeyCom}_D(MK_D, ID) \leftrightarrow \text{KeyCom}_K(MK_K, ID_t, r_t)$:

- When the KGC authenticates a user ut, it selects a random exponent rt €_R Zp for the user. This value is a personalized and unique secret to the user, which should be consistent for any further attribute additions to the user. Then, the KGC and the datastoring center engage in a secure 2PC protocol, where the KGC's private input is (rt,β) and the data-storing center's private input is α. The secure 2PC protocol returns a private output x=(α+rt)β to the data-storing center.
- The data-storing center randomly picks τ € Zp .Then, it computes A $=g^{x/\tau}$ and sends it to the KGC.
- The KGC then computes B $=A^{1/\beta2}$ and sends it to the data-storing center.
- The data-storing center outputs a personalized key component D = B^τ

5.1.1.2. Key Update:

When a user comes to hold or drop an attribute, its corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for forward or backward secrecy, respectively. Also, the key update procedure is done by the KGC when it receives a join or leave request from a user for some attributes. On receiving the request from user, the KGC notifies the data storing center of the event and sends the updated membership list of the attribute group to it. After receiving the notification from KGC, the data storing center reissues the key for that attribute group and so the sharing will be done even after updating key for attribute group.

5.1.2. Encryption and Decryption:

The encryption and decryption of data is processed using RSA algorithm. Here we are implementing RSA algorithm to encrypt and decrypt the data by particular users so that security will be maintained while sharing the data and also the data will be read by only users to which data belongs.

The RSA algorithm is as follows:

- Choose two large prime numbers p and q.
- Calculate n=p*q.
- Select the public key (i.e., encryption key) e such that it is not a factor of
  (p-1) and (q-1).
- Select the private key (i.e., decryption key) d such that following equation is true:
  (d*e) mod (p-1)*(q-1) =1
- For encryption, calculate the cipher text to the receiver.
- Send CT as the cipher text to the receiver.
- For decryption, calculation the plain text PT from the cipher text CT as follows :
  PT= CT^d mod n

5.2. Anonymous ID Algorithm:

Our next most useful task is fine grained user revocation which will be possible by implementing Authorization ID algorithm. Here, an algorithm for anonymous sharing of private data among N parties is developed. Also, this technique is used iteratively to assign these nodes ID numbers ranging from 1 to N. This assignment of ID's is anonymous such that the identities received are unknown to the other members of the group. This assignment of serial numbers allows more complex data to be shared and has applications to other problems in privacy preserving data mining and the collision avoidance in communications and distributed database access. Here, the required computations are distributed without using a trusted central authority. This algorithm is basically used to share complex data among network by creating unique Id for each user so that no other user will know the ID of each other.

CONCLUSION

The proposed scheme features a key issuing mechanism that removes key escrow problem during the key generation. This user secret keys are generated through a secure two-party computation such that any curious key generation center or data-storing center cannot derive the private keys individually. The key generation takes place by two party computation protocol between KGC and data storing center. Also, the attribute wise sharing is possible using CPABE and anonymous ID algorithm where unique id is created for each user. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing system against any system managers as well as outsiders in the network.All this work is shown in this paper by implementing it.

REFERENCES

[1] Junbeom Hur, ”Improving Security and Efficiency in Attribute- Based Data Sharing”, 2013(reference).

[2] Larry A. Dunning, Ray Kresman, ”Privacy Preserving Data Sharing With Anonymous ID Assignment”,2013.

[3] J. Anderson, “Computer Security Planning Study,” Technical Report 73-51, Air Force Electronic System Division, 1972.

[4] A. Shamir, “How to share a secret,” *Commun. ACM, vol. 22, no. 11*,pp. 612–613, 1979

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute- BasedEncryption for Fine-Grained Access Control of Encrypted Data,” Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

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

AUTHOR PROFILE

Kamini Hari Gonnade has received her B.E. in Computer Technology from Rajiv Gandhi College of Engineering Research and Technology, Chandrapur, Nagpur University in 2013. Currently, she is doing Master of Technology in Computer Science and Engineering from WCEM Nagpur, Nagpur University. Her area of interest includes cloud computing and network security.