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.2, Special Issue 4, September 2014

Removal of Escrow Problem and Revocation Problem in Distributed Data Sharing

D.Saroja, P.Lakshmi

M.Tech, Department of Computer Science and Engineering, S.V. Engineering College for Women, Tirupati, India

Assistant Professor, Department of Computer Science and Engineering, S.V. Engineering College for Women, Tirupati, India

ABSTRACT: Distributed data sharing has became an increasing challenge in modern distributed systems like cloud computing and online social networks etc., due to its data sharing archetype. The implementation of accessing policies and maintaining the policy updates has become a challenging issue in our Data sharing archetypes. Cipher text policy attribute-based encryption (CP-ABE) is appropriate a capable cryptographic solution to this problem. Our CP-ABE facilitates the data owners to characterize their individual access policy over user attributes and implement the policies on the data to be distributed. Beside its advantage, on the other hand our CP-ABE have main disadvantage called a key escrow or written agreement problem. The key generation center possibly will decrypt whichever messages addressed to particular users by generating their confidential personal or private keys. This is not appropriate for data sharing situations where the data owner would like to make their private data only easy to get to chosen users. As the access policies are defined only over the attribute universe user revocation or cancellation has become another challenging issue in applying CP-ABE in data sharing system.

As a result in our paper, we propose a new CP-ABE method for a data sharing system by developing the feature of the system architecture. The proposed method will achieve the following features: 1) By constructing the secure two-party computation between the key generation center (KGC) and the data storing center (DSC) we achieve escrow-free key issuing protocol through which key escrow or written agreement problem is solved and 2) On the top of ABE for alternative encryption we use selective attribute group key distribution to get elegant user revocation for each attribute. The performance and security analysis signify that the anticipated system is able to securely manage the data distribution in the data sharing system.

KEY WORDS: access control, CP-ABE, Data sharing Systems, KGC, revocation, removing escrow.

I. INTRODUCTION

Many people are using latest advances of the network and computing technologies to share their data with others in online external storages. By uploading their private photos or messages into the OSNs such as Facebook and Twitter people can share their lives with friends or uploading highly sensitive personal health records (PHRs) into online data servers such as Google Health for effortlessness of sharing their reports with chief doctors or for saving cost. The latest technologies and services are utilized by the people unlimitedly, at the same time several issues like data security and access control are raised in those technologies regarding to people.

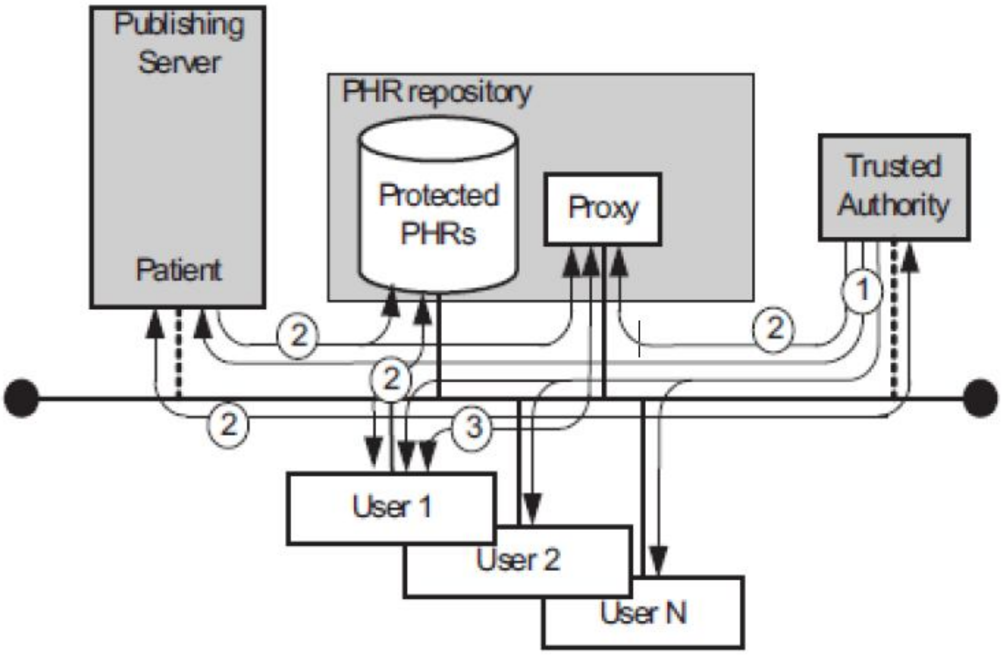

Fig 1: Security management in PHRs

There are possibilities of threats to data like offensive use of the data by the storage server or illegal access by outer users. Users may wish to visible their private data to specified persons by giving some credentials. A potential cryptographic advance that achieves an elegant data access control is Attribute-based encryption. Depending on the attributes of the requester and data object it defines access policies. Particularly, cipher text policy attribute-based encryption allows encryption of attribute set and decryption needs to have in order to decrypt the ciphertext, and impose it on the data. Therefore, each user with a diverse set of attributes is permitted to decrypt dissimilar pieces of data for each security policy. To prevent unauthorized data access our CP-ABE reduces the need to depending on data storage server (DSS).

On the other hand, the advantage of the CP-ABE comes with a most important disadvantage which is known as a key escrow or written agreement problem. By generating their attribute keys the KGC will decrypt every ciphertext addressed to specific users which is a potential hazard to the data privacy or secrecy in the distributed data sharing systems. One more challenge in Distributed data sharing system is the key revocation. In order to make systems secure, update of each attribute is necessary as a few users may alter their attributes at some time or few private keys might be negotiated. This matter is still more complicated particularly in ABE, as each attribute is possibly shared by multiple users. The cancellation of any attribute or single user from an attribute group or set of users will influence all users in that group. As a consequence, there may be a constrained access during rekeying procedure or security ruin due to the windows of defenselessness.

II.PROPOSED WORK

We have two different Attribute based Encryption systems. They are:

- key-policy ABE and

- Ciphertext-policy ABE.

In Key Policy ABE, attributes are used to illustrate the encrypted data and policies are constructed into users' keys; whereas in Cipher Policy ABE, the attributes are used to illustrate users' recommendations, and an encryptor find outs a policy such that who can decrypt the data. among the two Attribute based Encryption systems, CP-ABE is more suitable to the data sharing system as it puts the access policy conclusions in the hands of the data owners.

ELIMINATION OF ESCROW OR WRITTEN AGREEMENT:

The majority of the presented Attribute-based Encryption schemes are builds on the architecture where a single trusted authority (KGC) has the authority to create the whole private keys of users with its master secret information. As a result, the key escrow or written agreement difficulty is inherited such that the KGC can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. In KP-ABE system, all disjoint attribute authorities are partaking in the key generation protocol in a distributed way such that they cannot group their data and link numerous attribute sets fitting in to the same user.

One of the disadvantages of KP-ABE system is totally distributed approach is decrease in the performance. All attribute authorities will communicate with other authorities in the system to generate secret keys due to lack of centralized authority with master key information.

In our approach, we propose ***an Escrow Free Key Issuing Protocol for CP-ABE*** to resolve escrow problem which utilizes the feature of the data sharing system architecture. By performing a secure two-party computation (2PC) protocol among the KGC and the DSC with their own master secrets key issuing protocol generates and issues user secret keys. The 2PC protocol prevents them from acquiring any master secret information of each other such that none of them could generate the whole set of user keys on their own. Therefore, users are not necessary to completely belief the KGC and DSC in order to protect their data to be shared. Through our proposed system the data confidentiality and privacy can be cryptographically imposed in opposition to any inquiring KGC or data-storing center (DSC).

KEY REVOCATION:

The need of attention towards user revocation can be done using the alternative encryption method jointly with the CP-ABE algorithm. To re encrypt the cipher text encrypted under the CP-ABE algorithm, attribute group keys are selectively distributed to the authorized users in each attribute group. In order to make systems secure, update of each attribute is necessary as a few users may alter their attributes at some time or few private keys might be negotiated. This matter is still more complicated particularly in ABE, as each attribute is possibly shared by multiple users. The cancellation or revocation of any attribute or single user from an attribute group or set of users will influence all users in that group. Yet a user is withdrawn from some attribute groups, he would still be able to decrypt the shared data as long as the other attributes that he holds assures the access policy of the cipher text.

Data owners need to define only access policy for attributes only not to be concerned defining any access policy for users. In our proposed system, we assign most difficult tasks such as membership management and user revocation to the data storing center (DSC) whereas the KGC is in charge for the attribute key management devoid of revealing any private information to the other parties. Hence, the proposed system is the for the most part appropriate for the data sharing systems where users encrypt the data only once and upload it to the data-storing centers (DSC). The remaining tasks such as re encryption and revocation are performed by the DSC.

III. A DISTRIBUTED DATA SHARING SYSTEM

In this segment, we illustrate the Distributed data sharing architecture and characterize the security model.

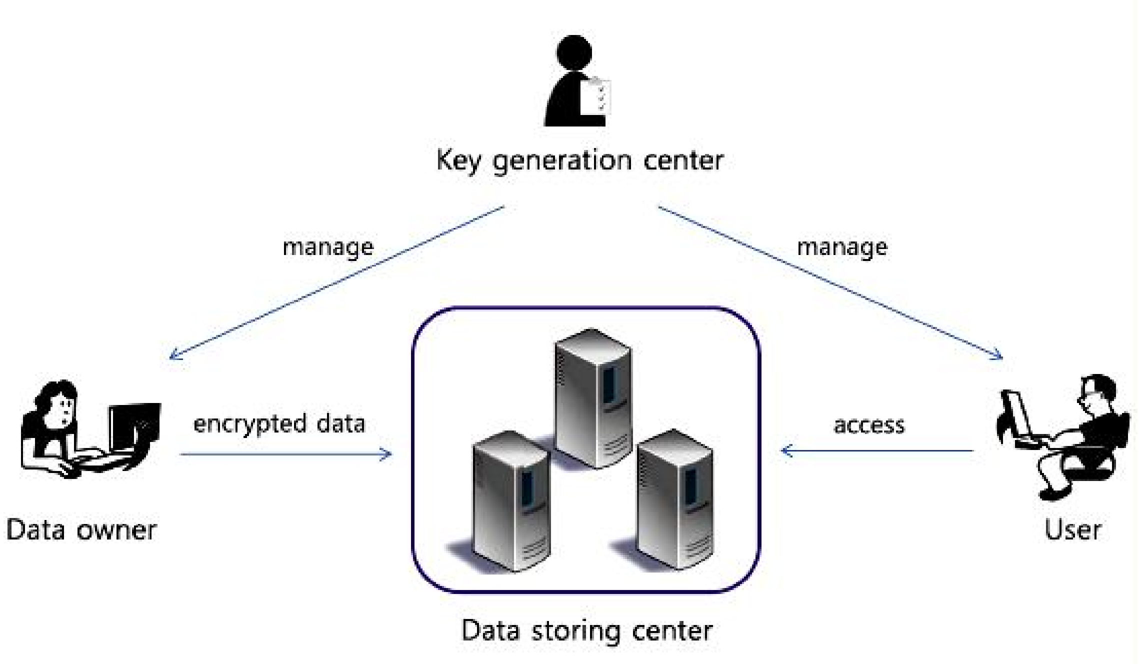

Fig. 2. Architecture of a distributed data sharing system.

The above figure shows the architecture of the distributed data sharing system, consisting of the following system entities:

Key generation center (KGC):

For CP-ABE, it generates public and secret parameters acting like a Key authority. KGC issues, revokes, and updates the attribute keys for users. Based on their attributes it grants differential access rights to individual users. KGC is assumed to be honest in executing the assigned tasks in the system but sometimes curious to learn the information of encrypted contents. As a result, KGC be supposed to be disallowed from accessing the plaintext of the encrypted data still it is honest.

Data storing center (DSC):

The Data storing center provides a data sharing service, which is in charge of controlling the accesses from outside users to the storing data and providing consequent contents services. It is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users for each attribute, which are used to implement an elegant user access control. The data-storing center is also assumed as semi trusted like the Key Generation Center.

Data owner (DO):

Data owner is a user who owns data, and desires to upload it into the external data storing center for effortlessness of sharing or for saving cost. DO is responsible for defining (attribute-based) access policy, and implementing it on its own data by encrypting the data underneath the policy before distributing it.

User:

The individual who wants to access the data are called user. If a user is having a set of attributes fulfilling the access policy of the encrypted data, and is not withdrawn in any of the attribute groups, then he has the right to decrypt the cipher text and access the data.

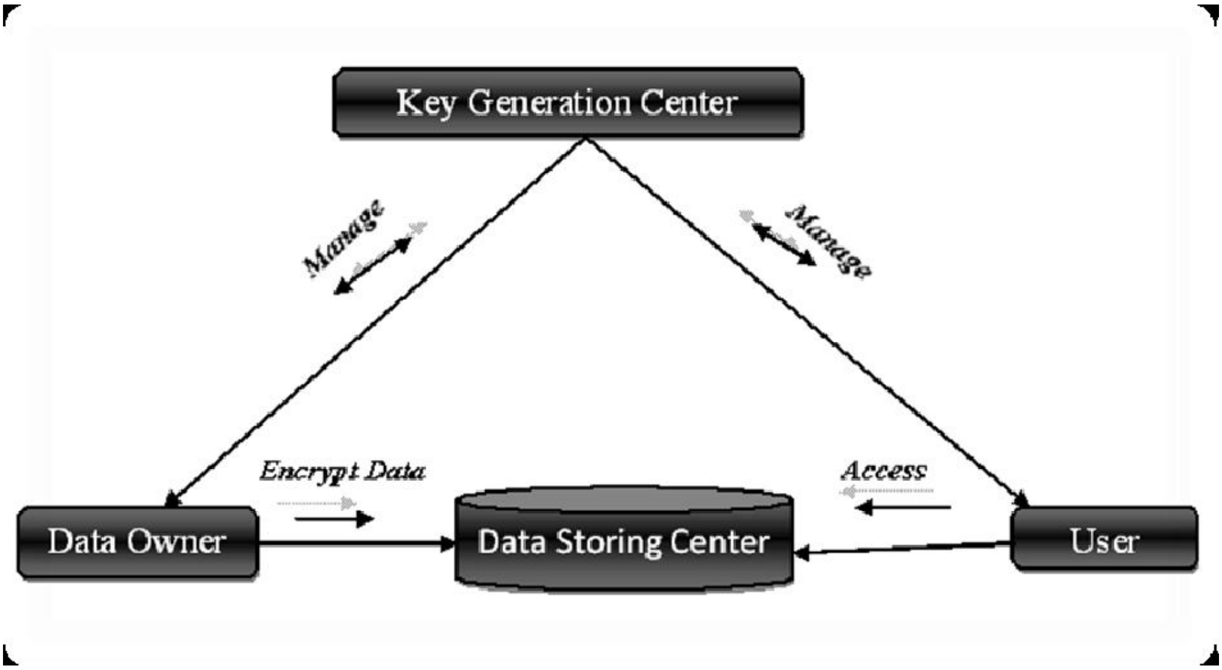

Fig.3: Node structure of the distributed data sharing system

In our approach, both the key managers, the KGC and data storing center (DSC), are semi trusted. They should be prevented from accessing plaintext of the data to be shared; for the time being, they should be still able to issue secret keys to users. To understand this problem, it is somewhat difficult, so the two parties employ in the arithmetic 2PC protocol with master secret keys of their own, and issue independent key components to users all through in the key issuing phase. The 2PC protocol prevents them from knowing each other's master secrets so that none of them can generate the complete set of secret keys of users independently. As a result, we assume that the KGC does not get together with the data storing center (DSC) as they are honest .

Security Requirements to data sharing system:

Data secrecy:

Not permitted users, who do not have sufficient attributes fulfilling the access policy, should be disallowed from accessing the plaintext of the data. Moreover, the KGC as well as the data storing center are not honest in data sharing systems. So unauthorized access to the plaintext of the encrypted data should be disallowed.

Complicity conflict:

Complicity conflict is the most significant security property requisite in ABE systems. If multiple users collide, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text on their own. We do not want these colluders to be able to decrypt the private data in the server by combining their attributes. Since we assume the KGC and data-storing center are honest, we do not consider any active attacks from them by colluding with revoked users.

Backward and forward secrecy:

In attribute-based encryption, backward secrecy is that any user who arrives to hold an attribute that satisfies the access policy should be disallowed from accessing the plaintext of the prior data distributed previous to he holds the attribute.

forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the following data distributed after he drops the attribute, if not the other valid attributes that he is holding satisfy the access policy.

IV. IMPLEMENTATION OF CP-ABE PROTOCOL IN DISTRIBUTED DATA SHARING SYSTEMS

The following are the components involved in the implementation of attribute based encryption in distributed data sharing systems:

- Data Owner
  - Login

- Key Generation Center (KGC)
  - Data owner (set Access Policy, Encrypt File)
  - Send Data Storing Center
- Data Storing Centre
  - Store Data
- User
  - Authentication (Registration /Login)
  - User Access
  - View Available Files
  - User Get File
  - Decrypt File

Data Owner:

Login:

The user will be granted to access data only when he enters a valid username/password combination. The user is denied to access the data and considered as unauthorized person, if he enters invalid username and password.

Key Generation Centre (KGC):

For CP-ABE, it generates public and secret parameters acting like a Key authority. KGC issues, revokes, and updates the attribute keys for users. Based on their attributes it grants differential access rights to individual users. KGC is assumed to be honest in executing the assigned tasks in the system but sometimes curious to learn the information of encrypted contents. As a result, KGC be supposed to be disallowed from accessing the plaintext of the encrypted data still it is honest.

Data owner (set Access Policy, Encrypt File):

Data owner is a user who owns data, and desires to upload it into the external data storing center for effortlessness of sharing or for saving cost. DO is responsible for defining (attribute-based) access policy, and implementing it on its own data by encrypting the data underneath the policy before distributing it. By encrypting the file, the DO will get key from key generator. The encrypted data is called a cipher text which is not easily understood by unauthorized people.

Send data to Data Storing Centre: Data storing centre store the data of DO in the encrypted form as cipher text.

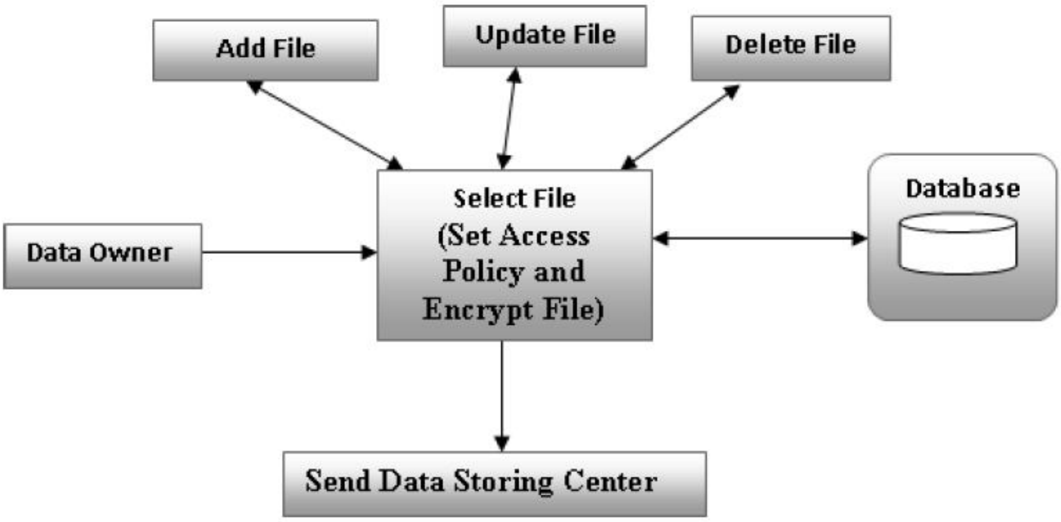

Fig. 4 Data Owner (Set Access Policy, Encrypt File)

Data Storing Centre:

The Data storing center provides a data sharing service, which is in charge of controlling the accesses from outside users to the storing data and providing consequent contents services. It is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users for each attribute, which are used to implement an elegant user access control. The data-storing center is also assumed as semi trusted like the Key Generation Center.

User:

Confirmation (Registration /Login): New user access data storing means he must be register his details by entering his name , address etc., first. The user will be granted to access data only when he enters a valid username/password combination. The user is denied to access the data and considered as unauthorized person, if he enters invalid username and password

User Access: The user checks our attributes and access policies in this module.

View Available Files: Data Storing Centre Store the number of files that files are displayed authorized user based on user access policy.

User Get File: The individual who wants to access the data are called user. If a user is having a set of attributes fulfilling the access policy of the encrypted data, and is not withdrawn in any of the attribute groups, then he has the right to decrypt the cipher text and access the data.

Decrypt File: the reverse process to Encryption is called decryption. The same Cipher is used for both Encryption and Decryption. Encryption generates a Cipher text from a Plaintext; Decryption generates a Plaintext from a Cipher text. User uses that appropriate file key to decrypt and to save that file.

V.CONCLUSION

In the data sharing systems, the enforcement of access policies and the support of policy updates are important challenging issues. In this work, we proposed an attribute based data sharing scheme to impose an elegant data access control by making use of the characteristic of the data sharing system. The proposed system removes key escrow problem during the key generation. The user secret keys are generated through a protected two-party computation (2PC) protocol such that any inquiring key generation center or data-storing center cannot get the private keys independently. Hence, our proposed system improves the data privacy and secrecy in the data sharing system in opposition to any system managers and adversarial outsiders without equivalent recommendations. by using the ciphertext policy attribute-based encryption (CP-ABE), we can do an immediate user revocation on every attribute set at the same time as taking complete advantage of the scalable access control. as a result, the proposed system achieved more secure and elegant data access control in the data sharing system.

REFERENCES

pp 41[1] J. Hur, ―Improving Security and Efficiency in Attribute-Based Data Sharing, IEEE TKDE, 2011.
[2] J. Bethencourt, A. Sahai, B. Waters,Ciphertext-Policy Attribute-Based Encryption, Proc. IEEE Symposium on Security and Privacy 2007, pp. 321–334, 2007.
[3] A. Sahai and B. Waters. Fuzzy identity-based encryption. In Eurocrypt 2005, LNCS 3494, pages 457–473. Springer-Verlag, 2005.
[4] A. Sahai, B. Waters, ―Fuzzy Identity-Based Encryption,‖ Proc. Eurocrypt 2005, pp. 457–473, 2005.
[5] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. In CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, pages 99–112, New York, NY, USA, 2006. ACM.
[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98, New York, NY, USA, 2006. ACMS.
[7] Alexandra Boldyreva, Vipul Goyal, Virendra Kumar, ―Identity-based encryption with efficient revocation‖, Proceedings of the 15th ACM conference on Computer and communications security, ISBN: 978-1-59593-810-7, 7-426, 2008.