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, Issue 5, May 2014

Privilege Based Attribute Encryption System For Secure and Reliable Data Sharing

T.Balasathuragiri, Prof. A.Suresh

Assistant Professor, Dept of CSE, Asan Memorial College of Engineering and Technology, Tamil Nadu, India.

Professor & Head Computer Science and Engineering, Asan Memorial College of Engineering and Technology. Tamil Nadu, India.

ABSTRACT – The secured data sharing is provided between the data owner and user based on the user's attributes. It achieves more secure and fine grained data access control in the data sharing system. Data security is the key concern in the distributed system. Cryptographic methods are used to enforce the access policies of users. But here the key generation center (escrow) can obtain the messages sending between the users by generating the private key. This is referred as Key escrow problem. This problem can be solved by escrow free key generation using 3PC (Three Party Computation). Thus the proposed system gives the greater performance and security to the distributed data sharing system.

KEYWORDS - Data sharing, attribute-based encryption, revocation, access control, removing escrow

I. INTRODUCTION

RECENT development of the network and computing technology enables many people to easily share their data with others using online external storages. People can share their lives with friends by uploading their private photos or messages into the online social networks such as Facebook and MySpace; or upload highly sensitive personal health records (PHRs) into online data servers such as Microsoft Health Vault, Google Health for ease of sharing with their primary doctors or for cost saving. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their 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 crypto- graphic approach that achieves a fine-grained data access control]. It provides 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 (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access, which is the traditional access control approach of such as the reference monitor.

II.PROPOSED SYSTEM

In existing system, a major issue is the Key-Escrow problem the key generation center and the user doesn't have any control/preferences or specification of deciding the key based on user's attributes. In CP-ABE (Cipher text Policy - Attribute Based Encryption), the key generation center (KGC) generates private keys of users. The revocation of any single user in an attribute group would affect all users in the group.

- The data sharing is not much secure; the other user can easily access the data in data store.
- The system won't distribute the data based on the attributes of the user Loss of data

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

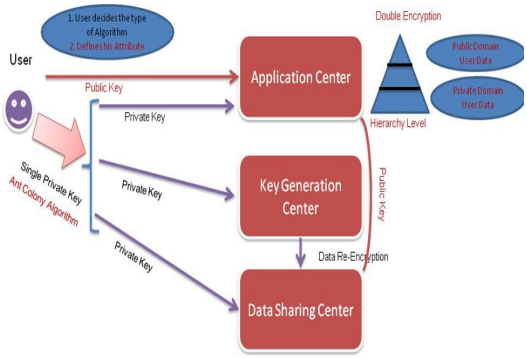
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

In Proposed system the key escrow problem is resolved by a key issuing protocol. The key issuing protocol generates a three party computation (3PC) protocol (key generation center, data sharing center, and application center) and the keys will be merged using Ant-Colony Algorithm. Triple DES algorithm is used for sharing the secured data to the user. Due to partial disclosure algorithm, the data will be retrieved based on the hierarchy.

- Data shared between the data owner and the users based on the attributes.
- The escrow problems are solved in the existing system.



Data sharing System architecture

III. SYSTEM DESIGN

A. Attribute Define Module/User Creation Module

Attributes of the user will be taken as an input in the system. For example, the position / designation of the user will be taken into consideration. Fetching the designation is used to get the data retrieval in the hierarchical manner. It is mainly used to create a multi location based key generation associated with hierarchical based data distribution and hiding.

B. Escrow-Free Key issuing Protocol Module

The KGC is responsible for issuing attribute keys to user and the secret key is generated through the secure 2PC protocol between the KGC and the data sharing center. To decrypt the data the user needs the keys from the data storing center and KGC. Thus we overcome the escrow technique by using this protocol. Our proposed system incorporated 3PC protocol where the key will be generated in Application center too and the keys will be merged using Ant-Colony Algorithm.

C. Authentication Module

It describes the interface between the user and system and the admin provided the type of authentication. Option of Security questions and answers were added in the system. It provides an interface to the permission system inside the Application. It contains views that make it possible to log users in and out, register and activate new users, password changing, etc.

D. Data Re-Encryption Module

The data owner uploads the data in data sharing center after encryption. Before sending those cipher text to the users, the data sharing center re-encrypt it by using re-encryption algorithm .If the user needs to access the data means they need to decrypt the data twice.

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, Issue 5, May 2014

E.Hierarchical / Partial Disclosure Module

.

The Data in the system will be stored in a Hierarchical manner. Same data will store in a different format based on the designation / Hierarchy. Due to partial disclosure algorithm, the data will be retrieved based on the hierarchy

. .

IV. RELATED WORK

In [1], ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into users' keys; while in CP-ABE, the attributes are used to describe users' credentials, and an encryptor determines a policy on who can decrypt the data. Between the two approaches, CP-ABE is more appropriate to the data sharing system because it puts the access policy decisions in the hands of the data owners.
In [2], Removing Escrow:-Most of the existing ABE schemes are constructed on the architecture where a single trusted authority or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the KGC can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time.

In [3], presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets

In [1], ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into users' keys; while in CP-ABE, the attributes are used to describe users' credentials, and an encryptor determines a policy on who can decrypt the data. Between the two approaches, CP-ABE is more appropriate to the data sharing system because it puts the access policy decisions in the hands of the data owners.
In [2], Removing Escrow:-Most of the existing ABE schemes are constructed on the architecture where a single trusted authority or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the KGC can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time.

In [3], presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this kind of fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with the other authorities in the system to generate a user's secret key and decryption (hence the use of the term symmetric).

.

In [4], proposed an anonymous private key generation protocol in identity-based literature such that the KGC can issue a private key to an authenticated user without knowing the list of users' identities. It seems that this anonymous private key generation protocol works properly in ABE systems when we treat an attribute as an identity in this construction.

In [5], Revocation: - In proposed first key revocation mechanisms in CP-ABE and KP-ABE settings, respectively. These schemes enable an attribute key revocation by encrypting the message to the attribute set with its validation time. These attribute-revocable ABE schemes have the security degradation problem in terms of the backward and forward secrecy. They revoke attribute itself using timed rekeying mechanism, which is realized by setting expiration time on each attribute.

V. TECHNIQUES AND ALGORITHM USED

A. CP-ABE (Cipher text Policy- Attribute Based Encryption)

Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys while in our system attributes are used to describe a user's credentials, and a party encrypting data

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, Issue 5, May 2014

determines a policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).In addition;we providen implementation of our system and give performance measurements.

VI. CONCLUSION

Thus the overall the system architecture and their modules are described and their purpose is clear. These sub modules and their function provides more secure and fine-grained data access control in the data sharing system.

REFERENCES

1 A. Lewko, A. Sahai, and B. Waters, Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, pp. 273-285, 2010.

2 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.

3 L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Cipher text-Policy Attribute-Based Encryption and ItsApplication", Proc. Int'l Workshop Information Security Applications (WISA '09),pp.309-323, 2009.

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

5 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.

6 A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption withficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

BIOGRAPHY

Mr. T. Balasathuragiri., B.E.,M.E.,(Ph.D) works as the Assistant Professor of the Computer Science and Engineering Department in ASAN Memorial College of Engineering & Technology, Chengalpet, Chennai, TamilNadu, India. He has more than 3 years of experience in teaching and his areas of specializations are Image Processing and Neural Networks. He has published many of her papers work in national and international conferences.

Dr. A. Suresh., B.E.,M.Tech., Ph.D works as the Professor & Head of the Computer Science and Engineering Department in ASAN Memorial College of Engineering & Technology, Chengalpet, Chennai, TamilNadu, India. He has more than 16 years of experience in teaching and his areas of specializations are Data Mining, Artificial Intelligence, Image Processing, Neural Networks and System Software. He has published many of his research work in national and international journals & conferences and he has published one book in the name of Data structures & Algorithms in DD Publications.