Improving Security and Efficiency in Attribute Based Data Sharing

M. Pratheepa[1], R. Bharathi[2]

[1]M.Tech Student, Department of Computer Science and Engineering, PRIST University Pondicherry, India

[2]Assistant Professor, Department of Computer Science and Engineering, PRIST University Pondicherry, India

Abstract: ***The key generation center could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users key. so overcome this problem we propose escrow problem which means a written agreement delivered to a third party and Attribute-based encryption (ABE) is a promising Cryptographic approach fine-grained data access control which is provides a way of defining access policies based on different attributes of the requester, environment, or the data object. The KGC can decrypt every cipher text addressed to specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or privacy in the data sharing systems.***

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

1. Introduction

Network and computing technology enables many people to easily share their data with others are using online external storages. People can share their lives with friends by uploading their private photos or messages into the online social networks; 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 cryptographic 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 to encrypt or to define the attribute set over a universe of attributes that a decrypt or 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 Nevertheless, applying CP-ABE in the data sharing system has several challenges. In CP-ABE, the key generation center (KGC) generates private keys of users by applying the KGC's master secret keys to users' associated set of attributes. Thus, the major benefit of this approach is to largely reduce the need for processing and storing public key certificates under traditional public key infrastructure (PKI). However, the advantage of the CP-ABE comes with a major drawback which is known as a key escrow problem. The KGC can decrypt every cipher text addressed to specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or privacy in the data sharing systems. Another challenge is the key revocation. Since some users may change their associate attributes at some time, or some private keys might be compromised, key revocation or update for each attribute is necessary in order to make systems secure. This issue is even more difficult especially in ABE, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a set of users as an attribute group).This implies that revocation of any attribute or any single user in an attribute group would affect all users in the group. It may result in bottleneck during rekeying procedure or security degradation due to the vulnerability of windows.

1.1 Related Work

The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data storing center, fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.

2. Literature Survey

We create public key revocation encryption systems with small cryptographic private and public keys. Our systems have two important features relating respectively to public and private key size. First, public keys in our two systems are short and enable a user to create a cipher text that revokes an unbounded number of users. This is in contrast to other systems where the public parameters bound the number of users in the system and must be updated to allow more users. Second, the cryptographic key material that must be stored securely on the receiving devices is small. Keeping the size of private key storage as low as possible is important as cryptographic keys will often be stored in tamper-resistant memory, which is more costly. This can be especially critical in small devices such as sensor nodes, where maintaining low device cost is particularly crucial.

3. Proposed System

In this paper, we propose a novel CP-ABE scheme for a secure data sharing system. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. The 2PC protocol deters them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. The data confidentiality and privacy can be cryptographically enforced against any curious KGC or data storing center in the proposed scheme.

3.1 Advantages

- The key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data storing center.
- Fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.

4. Modules Explanation

4.1 Data Owner

4.1.1 Login

In Login Form module presents users a form with username and Password fields. If the user enters a valid username/password combination they will be granted to access data. If the user enter invalid username and password that user will be considered as unauthorized user and denied access to that user.

4.1.2 Key Generation Center (KGC)

It is a key authority that generates public and secret parameters for CPABE. 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 / decrypted.

4.1.3 Data owner (set Access Policy, Encrypt File)

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. Data Owner 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.

4.1.4 Send Data Storing Center

Data storing center store the data owner Encrypt the file and Store Data storing center.

4.2 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 corresponding contents services. 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. Data storing center store the data. Data Storage Centers provides offsite record and tape storage, retrieval, delivery and destruction services.

4.2.1 User

- **Authentication (Registration /Login)**
  New user access data storing means must, new User can enter our details and register here. In Login Form module presents users a form with username and Password fields. If the user enters a valid username/password combination they will be granted to access data. If the user enter invalid username and password that user will be considered as unauthorized user and denied access to that user.
- **User Access:**
  In this module the user checks attributes and access policy.

4.3 View Available Files

Data Storing Center Store the number of files that files are displayed authorized user based on user access policy.

4.4 User Get File

It 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, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the cipher text and obtain the data User to select particular file and get Key from Key Generation Center.

4.5 Decrypt File

Decryption is the reverse process to Encryption. Frequently, the same Cipher is used for both Encryption and Decryption. While Encryption creates a Cipher text from a Plaintext, Decryption creates a Plaintext from a Cipher text. User uses that particular file key decrypt and save that file

5. Technique or Algorithm

To applying CP-ABE in the data sharing system, In CP-ABE, the key generation center (KGC) generates private keys of users by applying the KGC's master secret keys to users' associated set of attributes.

A cipher text policy attribute-based encryption (CP-ABE) system consists of four fundamental algorithms: Setup, Encrypt, KeyGen and Decrypt.

Setup: Setup takes as input a security parameter and returns a public key PK and a master key (Private Key) MK. The public key is used for encryption. The master key, held by the central authority.

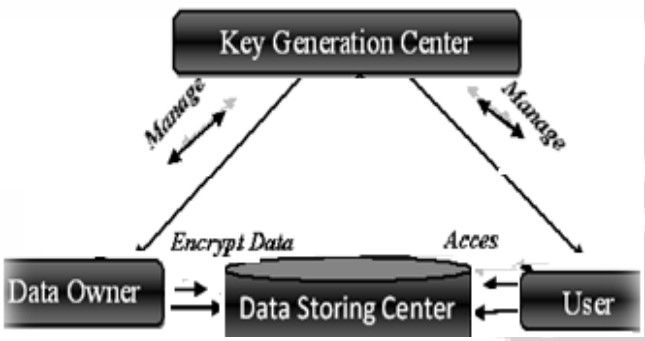
KeyGen: KeyGen takes as input the public key PK and a master key (Private Key) MK.

Encrypt. Encrypt takes as input the public key PK, a message M and an access structure W. It returns a cipher text CT such that a private key generated from attribute set S can be used decrypt CT.

Decrypt: Decrypt takes as input a cipher text CT. It returns the message M if S satisfies W, where S is the attribute set used to get MK.

6. System Architecture

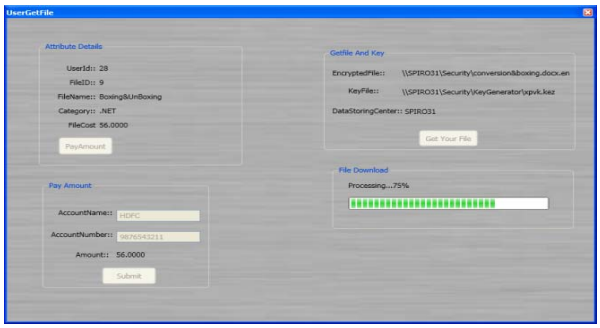
The nodes involved are admin and clients which stands as UI for the system. The deployment is performed as per the requirements of Hardware and software specified in the requirements phase.



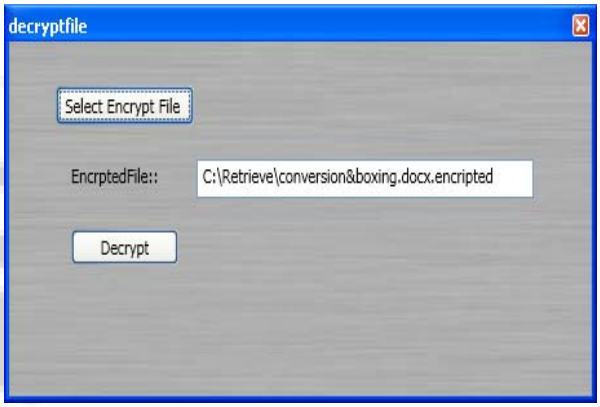
Key generation center is a key authority that generates public and secret parameters for CPABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. Data storing center is an entity that provides 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 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. 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 he will be able to decrypt the cipher text and obtain the data

7. Snap Shot

File Download



Decrypt File



8. Applications

Application

- Secure two-party computation between the key generation center and the data storing center

Advantage

- The advantage CP-ABE comes solve key escrow problem.
- Secure two-party computation between the key generation center and the data storing center
- Data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials.
- Selective attribute key distribution on top of the ABE.
- secure and fine-grained data access control in the data sharing system

9. Future Enhancement

In the future, it would be interesting to consider attribute-based encryption systems we can apply advanced cryptosystem for data sharing. In future we encrypt multimedia content Solve fully distributed approach is the performance degradation Neglected key expired time we can use multi Data Storing Center Proxy servers to update user secret key without disclosing user attribute Information.

10. Conclusion

To achieves more secure and fine-grained data access control in the data sharing system. We demonstrated that the proposed scheme is efficient and scalable to securely manage user data in the data sharing system. Data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials.

References

[1] Lewko, A. Sahai, B. Waters," Revocation Systems with Very Small Private Keys," Proc. IEEE Symposium on Security and Privacy 2010, pp. 273–285, 2010.
[2] Boldyreva, V. Goyal, V. Kumar," Identity-Based Encryption with Efficient Revocation," Proc. ACM Conference on Computer and Communications Security 2008, pp. 417–426, 2008.
[3] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "Mediated Cipher text- Policy Attribute-Based Encryption and Its Application," Proc. WISA 2009, LNCS 5932, pp. 309–323, 2009.
[4] L. Cheung, C. Newport, "Provably Secure Cipher text Policy ABE," ACM Conference on Computer and Communications Security, pp. 456–465, 2007.
[5] S. Yu, C. Wang, K. Ren, W. Lou," Attribute Based Data Sharing with Attribute Revocation," Proc. ASIACCS '10, 2010.

Author Profile

Mrs. M. Pratheepa is presently Pursuing Final Year M.TECH CSE, in PRIST University, Puducherry Campus, Puducherry, India.

Ms.Bharathi. R, received The M.Tech in Computer Science And Engineering. Presently she is Working Assistant Professor in Computer Science and Engineering at PRIST University, Puducherry Campus, and Puducherry, India.