Ciphertext Policy - Attribute Based Encryption (CP-ABE) System Solution for Securely Sharing Images Owned by One Stakeholder with Unknown Stakeholder

Miss. Pooja Tandale, Mr. Sidheshwar Khuba

Abstract— One of the most challenging issues in sharing systems is the enforcement of access policies and the policies updates support. Ciphertext policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to this issue. Cipher text – Attribute Based Encryption scheme enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the ciphertext. Thus, each viewer with a different set of attributes is allowed to decrypt different pieces of data per the security policy. It is designed to use CP-ABE scheme to improve security and efficiency in attribute based image sharing. The designed image sharing system includes Key Generation Center, Image Owner, Image Viewer, Image Server system entities that helps to share image securely using CP-ABE scheme. Here, specifically focus is on sharing image in '.jpg/.jpeg' format.

Index Terms— Image security, Image sharing system, Attribute base encryption, Access Control, Network security, CP-ABE, Image Encryption.

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) comes in two types 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 [2], [3].

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 [4], [5], [9]. 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. Chase and Chow [6] presented a distributed KP-ABE scheme that solves the key escrow problem in a multiauthority system. Chow [7] 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 Bethencourt et al. [4] and Boldyreva et al. [8] 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.

It would be interesting to consider attribute-based encryption systems by applying advanced cryptosystem for data sharing. Designed system should encrypt images.

2 Existing System

Junbeom Hur proposed a CP-ABE scheme[1] for a secure data

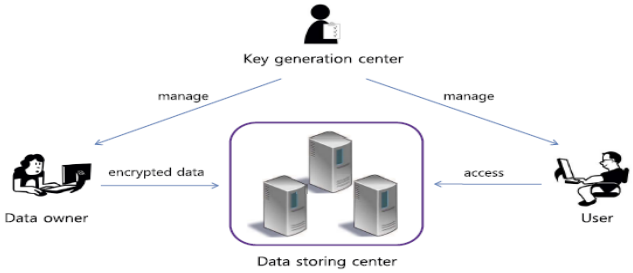

Fig.1 Architecture of data sharing center

- *Miss. Pooja Tandale , currently pursuing masters degree in computer science and engineering at NKOCET in Solapur University,India. E-mail: tandalepooja11@gmail.com*
- *Mr.Sidheshwar Khuba, Professor in department of computer science and engineering at NKOCET in Solapur University, India. E-mail: sa.khuba@gmail.com*

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 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 privacy and data confidentiality can be cryptographically enforced against any KGC or data storing center.

Thus, existing system is efficient to securely manage the data distributed in the data sharing system..

3 Proposed System

Designed Ciphertext Policy - Attribute Based Encryption (CP-ABE) system securely share image owned by one stakeholder with unknown stakeholder. The KGC is responsible for the attribute key management as in the previous CP-ABE schemes without leaking any confidential information to the other parties. Therefore, designed system is the most suitable for the image sharing scenarios where users encrypt the image and upload it to the image server. The designed system share '.jpg/.jpeg' image securely in distributed system using CP-ABE scheme.

4 Methodology

The designed system architecture is depicted in Fig 2, which includes the following system entities:

1. Key generation and Key distribution System. It is a key authority that generates parameters for CP-ABE i.e. public and secret parameters. And differential access rights granted to individual users based on their attributes. Thus, it should be prevented from accessing the plaintext of the encrypted image.

2. Image Server. It is an entity that provides image sharing service. It controls the accesses from outside users to the storing image and providing corresponding contents services.

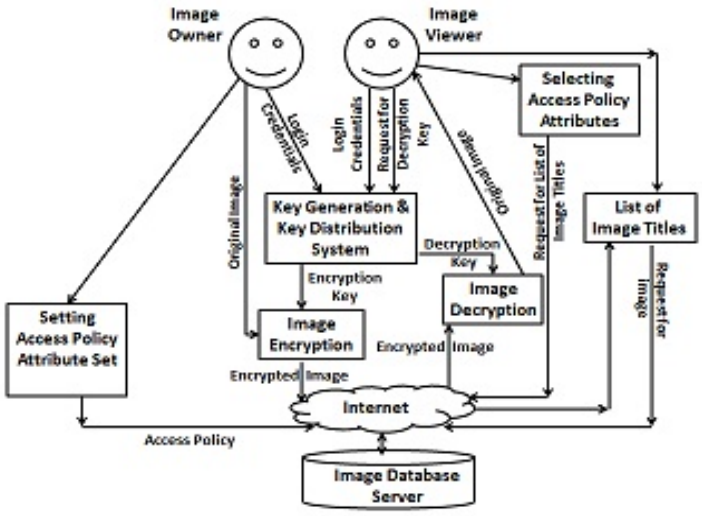

Fig. 2 System Architecture

3. Image owner. It is a client who owns image, and wishes to upload it into the server for ease of sharing. Image owner is responsible for defining (attribute-based) access policy, and enforcing it on its own image by encrypting the image under the policy before distributing it.

4. Image Viewer. It is an entity who wants to access the image. If a user possesses a set of attributes satisfying the access policy of the encrypted image, and is not revoked in any of the valid attribute groups, then he will be able to decrypt and obtain the image.

5 Conclusion

The designed system securely share image owned by one stakeholder with unknown stakeholder using ciphertext policy attribute based encryption technique.So the designed system helps to improve image security and specific access control for improper use of the data by the storage server or unauthorized access by outside users.

Acknowledgment

I place on record and warmly acknowledge the continuous encouragement, in valuable supervision, timely suggestions and inspired guidance offered by Prof. Sidheshwar A. Khuba, Professor, Department of Computer Science and Engineering, Nagesh Karajagi Orchid College of Engineering &Technology, Solapur.

References

[1] J.-M. Zhu and J.-F. Ma, "Improving Security and Efficiency in Attribute Based Data Sharing," IEEE Transactions on knowledge and data engineering , vol. 25, no. 10, october 2013

[2] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application," Proc. Int'l Workshop Information Security Applications (WISA '09), pp. 309-323, 2009.

[3] 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.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[5] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. Int'l Symp. Information, Computer, and Comm. Security (ASIACCS), pp. 343-352, 2009.

[6] 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.

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

[8] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

[9] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded Ciphertext Policy Attribute-Based Encryption," Proc. Int'l Colloquium Automata, Languages and Programming (ICALP), pp. 579-591, 2008.