ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Data sharing with Security and Efficiency using Attribute Based System

K. Dhana Lakshmi[1], Hussain Syed[2], M.Bharat[3]

M.Tech, IT, QIS Institute of Technology, Ongole, India [1]

Assistant Professor, IT, QIS Institute of Technology, Ongole, India [2]

Assistant Professor, IT, Guru Nanak Institutions Technical Campus, Hyderabad, India [3]

Abstract: Data sharing paradigm in distributed systems such as Social Networks and Cloud Computing, there is an increasing demand for distributed data security in the recent adoption and diffusion. The most challenging issue in data sharing is the enforcement of access policies. In this Cipher text Policy Attribute-Based Encryption (CP-ABE) is a promising cryptographic solution for this issue. This allows data owners to define their own access policies over user attribute and enforce the policies on data that is to be distributed. The major drawback with this is Key escrow problem. The key generation canter (KGC) will decrypt any message addressed to a specific user by generating their private keys. This is not a good scenario because the data owners want to be accessed to only specific users. We propose a CP-ABE scheme for data sharing, which allows the key escrow problem would be solved. The security and performance indicates that the proposed scheme is efficient and secure the data distributed.

Keywords: Data sharing, attribute-based encryption, key escrow, access policies.

I. INTRODUCTION

Social networks and computing technology enables people to share their data easily with others using online external storages. People can share their thoughts and lives with friends by uploading their messages or private photos into the online social networks such as Facebook and MySpace. People enjoy the advantages of these new technologies and services by using them, their main concerns are about data security and access controls. Improper use of the data or unauthorized access by outside users would be a potential threat to their data. People would like to make their private data accessible only to the authorized people with credentials they have specified. Attribute-based encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control. It allows to define access policies based on different attributes of the requester, environment, or the data object. Especially, Cipher text Policy attribute-based encryption (CP-ABE) enables the Encrypt or to define the attribute set over a universe of attributes that the Decrypt or needs to possess in order to decrypt the cipher text. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. This method eliminates the need to rely on data server in order to prevent the unauthorized data access. Nevertheless, applying CP-ABE in the data sharing system has many challenges. The key generation canter (KGC) in CP-ABE generates private keys of users by applying KGC's master secret keys to users' associated set of attributes. Thus, the benefit of this approach is to 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 drawback which is called as a key escrow problem. Here the KGC can easily decrypt cipher text addressed to specific user by generating their attribute keys. This is a potential threat to the data confidential and privacy in data sharing systems.

II. EXISTING SYSTEM

The main problem of storing the encrypted data in the cloud lies in revoking the access rights from the user. A user whose permission is revoked will still retain a copy of keys issued earlier, and thus can decrypt data in the cloud. The naïve solution is, the data owner must immediately re-encrypt the data, so that the receiver will make request for the key, once the request was received the data owner can send the key or decline the request. This solution leads to a performance of bottleneck, especially when there is a frequent user revocation. The other alternative solution is to apply the proxy re-encryption (PRE) technique. This approach is called as command –driven re-encryption scheme, where the cloud server executes the encryption while receiving commands from the data owner. The main disadvantages are:

- We can easily decrypt the data with some decryption software without the security key which is assigned by the data owner.
- Only single key is used for the highly sensitive data.
- If key is forgot we cannot send multiple key request to the data, and so we cannot decrypt the data without the key.

III. PROPOSED SYSTEM

Here, we have considered the existing system and removed the drawbacks in the system and introduced a secure transfer of data in the network. This will protect the data lose and data thefts. It also has a secure message module which protects the user's message from several persons in the network. The advantages on using the proposed system are:

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

- Highly secured data transfer with advanced encryption techniques that the other person cannot decrypt it easily.
- We have used the Attribute Based Encryption (ABE) system which provides more security to our data.
- Here the receiver can send multiple key requests to the data owner for the single data receiver received.

A. Architecture

The architecture consists of Key Generation Center, Data Storage Center, Data Owner and User. The Fig. 1 shows the architecture.

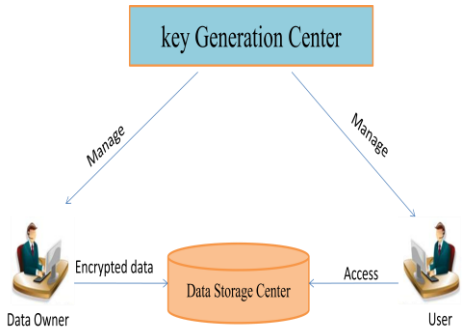

Fig. 1. Architecture

B. Algorithm Used:

Attribute based Encryption (ABE) Algorithm.

IV. MODULES

The list all the modules are explained below.

A. Login Form

In the Login Form the user is view with the Username, Password fields along with that login Button and Registration Button. If the user is new he/she should first register the details. After successful registration, he should enter his Username and Password given while registration. If the entered Username and Password are correct, the user will be considered as Authorized user and if not the user is denied.

B. Key Generation Center (KGC)

The Key Generation Center generates both the public and secret parameters for CP-ABE. It is the in-charge of issuing, updating and revoking attribute keys for the users. This will grant the differential access rights to the individual users based on their attributes. Key generation is a process of cryptography. The key generated is used to encrypt/decrypt the data that is being encrypted / decrypted.

C. Data owner (set Access Policy, Encrypt File)

Data Owner is a client who owns the data, and wishes to upload message and photos to the external storage canter to share to other individuals. Here the data owner is responsible for defining (attribute based) access policies and encrypt the data before distributing it. The data owner gets the key from key generator to encrypt the file. Encryption is the conversion of data in the form, called cipher text which is not understood by other individual (Unauthorized).

D. 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 Centres provides offsite record and tape storage, retrieval, delivery and destruction services.

E. Key Request

If the receiver wants to unlock or decrypt the message he has to send the key request to the data owner or sender. If the key request was received the sender will reflect the key. If he sends the key then only the receiver can decrypt the data. At the receiver side the key and the request id will be displayed after sender sends the key. Using that the receiver can decrypt the data.

F. Send Key

Once the key request was received, the sender can send the key or he can decline it. With this key and request id which was generated at the time of sending key request the receiver can decrypt the message.

G. View Available Files

Data Storing Center Stores the files that are accessed by authorized user based on the User access policies.

H. 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.

I. 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.

V. SNAP SHOTS

A. Login Form

The login form consists of the username and password. These fields filled will be valid for only the registered persons with valid username and Password at the time of registration Fig. 2. Shows the login Form.

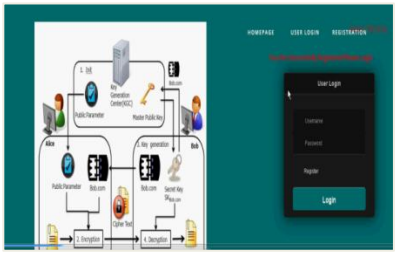

Fig. 2. Login Form

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

B. Sending Message

Once the valid user has logged in, the user can send messages or share personal information to the other valid person with some access policies. The Fig.3. Shows the sending message form.

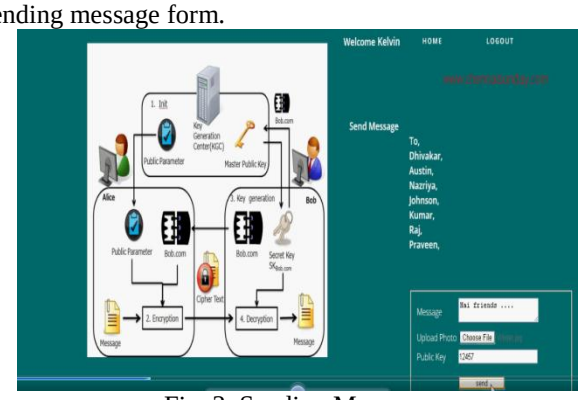

Fig. 3. Sending Message

C. Received Message with Encryption

The other person with valid credential received the message from his friend, will receive a message like this. The message and the photos will be encrypted. The below Fig. 4. Shows the Encrypted message

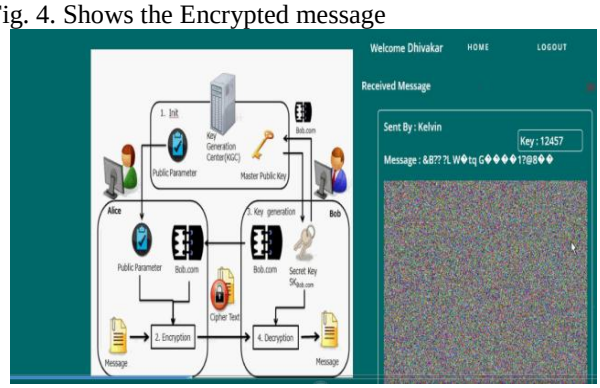

Fig.4. Encrypted Message

D. Key Request

The receiver who received the message with encryption cannot directly view the messages and photos. He/she needs to request for a key from the sender. The below Fig. 5 shows the Key Request

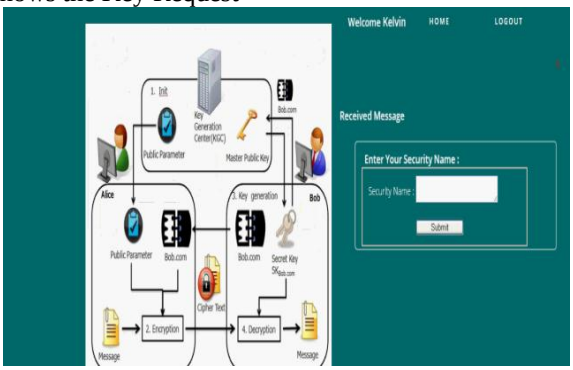

Fig. 5 Key Request

E. Decrypted Message

Once the sender sends the key, the receiver can enter the key and he/ she can view the view the message as below. The below Fig. 6 shows the Decrypted Message.

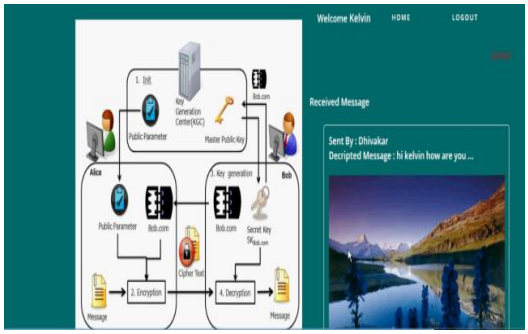

Fig. 6 Decrypted Message

This shows that the messages and photos we share are kept secure and this is efficient also.

VI. ADVANTAGES

- The advantage CP-ABE is to solve the key escrow problem.
- Provides security with two-party computation between the key generation center and the data storing center.
- Data privacy and confidentiality in data sharing systems against any other system managers and adversarial outsiders without the required (corresponding) credentials.
- It is secure and has fine-grained data access control in the data sharing system

VII. CONCLUSION

To achieve more security in data access control in data sharing system, we have demonstrated that proposed system is more efficient and secure. It is easy to manage the data of data owner by providing the access policies to the other user. Here in this, data privacy and confidentiality in data sharing against any other system managers. Here outsiders cannot join and see the data without proper credentials. Hence this scheme is more secure and confidential.

REFERENCES

[1]. Junbeom Hur, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 10, OCTOBER 2013.
[2]. [2]J. Anderson, "Computer Security Planning Study," Technical Report 73-51, Air Force Electronic System Division, 1972.
[3]. L. Ibrahim, 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.
[4]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006
[5]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[6]. R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007.
[7]. P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A Content-Driven Access Control System," Proc. Symp. Identity and Trust on the Internet, pp. 26-35, 2008.
[8]. 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.
[9]. The Pairing-Based Cryptography Library, http://crypto.stanford.edu/pbc/, 2012.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

BIOGRAPHIES

Mrs. K. Dhana Lakshmi is a student pursuing M.Tech in Information Technology at QIS Institute of Technology, Ongole, India. Her interested areas are Network Security and Cloud Computing.

Mr. HUSSAIN SYED is an Assistant Professor in Department of Information technology at QIS Institute of Technology, Ongole, India. His interested areas are Software Engineering, Computer Organization & Architecture, DBMS, Data warehousing Management Information Systems, Decision Support Systems, E-Commerce.

Mr. M. Bharat is an Assistant Professor in Department of Information technology at Guru Nanak Institutions Technical Campus, Hyderabad. His interested areas are Network, Cloud Computing and Computer Forensics.