The Security and Efficiency in Attribute-Based Data Sharing

Mr. Gadhe Nilesh B.[1] Mr. Bhaskar Swapnil A.[2]
[1,2]Department of Computer Engineering
[1,2]Shri Chhatrapti Shivaji College of Engineering, Rahuri, India

Abstract— In the recent data sharing paradigm there have been need for data security in distributed systems such as online social networks, One of the most dangerous issues in data sharing systems is the access policies. Cipher text policy attribute-based encryption (CP-ABE) is solution for this issue use cryptography. The senders to define their own access policies using attributes and enforce the policies on data to be distributed. However, a key escrow problem is a major drawback in existing system. In our contribution we solve key escrow problem. The key generation center generating their private keys and decrypt any messages addressed to specific users. This is not suitable for data sharing system where the data owner make their private data only accessible to authorized users. Therefore by applying CP-ABE in the data sharing system introduce another challenge with regard to the user revocation hence the access policies are defined over the attribute universe. In this paper, we propose a advance Cipher text Policy-ABE scheme for a data sharing system by using the characteristic of the system architecture. The proposed scheme gives the following advantages: 1) the key escrow problem can be solved by escrow-free key issuing protocol, the secure two-party computation between the key generation center and the data-storing center is performed, and 2) Due to proxy encryption, the selective attribute group key distribution is the main function of the ABE.

Key words: Attribute Based Encryption, Data Sharing, Revocation, Removing Escrow, Access Control

I. INTRODUCTION

In previous development of the network and computing technology (data sharing) enables many people to easily share their data with others using computing technology means external storages over the internet. People can share their data and message with friends by uploading their private data, text message and photos into the online social networks; or upload highly secure military information and personal health records (PHRs) into online data servers use for sharing with their primary doctors or for cost saving. As people take advantage of these new services and technologies, their rights about data security and access right control also improved. The use of the data is not properly by the or unauthorized access by outside users or storage server could be potential threats to their data. The secure data only accessible to the authorized people. Attribute-based encryption (ABE) is a promising cryptographic approach that gives a fine-grained data access control [3], [4], [5], [6].

It defines access policies based on various attributes of the user, environment or the data object. The each user with a various set of attributes is allowed to decrypt the data as per the security policy. The encrypt or define their own attribute set over a universe of attributes that a descriptor needs to possess in order to decrypt the cipher text, and enforce it on the contents [5]. This effectively removes the need to rely for preventing unauthorized data access, which is the traditional access control [1]. By applying cipher text policy attribute-based encryption in the data sharing system has several challenges. In cipher text policy attribute-based encryption, KGC generates private keys of users by applying the KGC's private keys to users' associated set of attributes. The major advantage of this system is to reduce the need for processing and storing secrete key certificates under traditional public key infrastructure (PKI). SO, the advantage of the CP-ABE comes with a major drawback which is known as a key escrow problem.

The key revocation is the another challenge. Therefore some users change their associate attributes at some time, or some private keys are compromised, update or key revocation for each attribute is necessary for systems secure. This issue is even more complex especially in ABE. The Key Generation Center can decrypt every CP addressed to specific users by creating their attribute keys.

This can be potential threat to the data confidentiality and privacy in the data sharing systems.

II. LITERATURE SURVEY

There are two policies of ABE that is KP-ABE (key-policy ABE) and cipher-text-policy ABE(CP-ABE). The KP-ABE are used to encrypt data describe by attributes and policies are built into users private keys; In CP-ABE, the attributes describes the users rights, and an encryptor determines a policy on the user. In above two policies, CP-ABE is more essential to the data sharing system because it having the access policy decisions in the hands of the data owners[1].Cipher text-Policy Attribute-Based Encryption (CP-ABE), The user private key is based on set of attributes, so the cipher text is associated with an access policy for attributes. The user can decrypt the message if the attribute set of his private key satisfies the access policy denoted in the cipher text. In many distributed systems if a user having a certain set of credentials or attributes then a authorized user should only be able to access data .So, the only method for for a such policies is to employ a trusted server to store the data [2]. In [3], The important characteristics of the system are public and private key size. First, public keys in our two systems are small size and enable a user to create a cipher text this is used to revokes an unbounded number of users. The private key is the second key cryptographic material that must be stored on the receiving devices is small. The size of private key storage is as small as possible. This can be especially critical in small devices like sensor nodes, where maintaining low device cost is crucial [3].

IBE i.e. Identity-based encryption is an exciting another method to public-key encryption, as IBE removes the need for a Public Key Infrastructure (PKI). The users using an IBE do not need to look up the public keys and the relative certificates of the receivers, the identities (e.g. IP addresses or email) are sufficient to encrypt. The most popular solution requires the data owners to also use time periods when encrypting, and all the users to update their private keys regularly by contacting the trusted authority [4].

All rights reserved by *www.ijsrd.com*

A. Existing System

In existing system consist of many algorithms easily decrypt the data and single key is used for this. Most of the existing ABE schemes are based on the architecture in which a single trusted authority, or KGC generate the whole private keys of users with its private information. The key escrow problem is main disadvantage of existing system. The key generation center generates private keys for user for decrypt any messages addressed to specific users. This is not sufficient for data sharing scheme, where the sender make their private data only accessible to authorized users.

B. Proposed Solution

In this paper, we introduce a new Chipper text Policy-ABE for a secure data sharing system. User secret keys generated by the key issuing protocol create by performing a secure two-party computation two PC protocol in the KGC and the data storing center. The 2PC protocol deters them from obtaining any secret information between them, such that none of them could generate the whole set of user keys alone. In our scheme, the privacy can be cryptographically enforced against any curious KGC or data storing center. The 2PC protocol solved key escrow problem, which is constructed using. By taking advantage of the selective attribute group key distribution, the fine-grained user revocation of each attribute could be done by proxy encryption.

C. Attribute Based Data Sharing System

1) Data Owner

The data owner creates the data, and uploads it into the external data storing center for sharing. The data owner defines their (attribute based) access policy, and the data owner own their data by encrypting the data under the policy before share it. Data Owner Encrypt the file using their attributes. Encryption is process of conversion of data in the form of cipher text .The unauthorized people that cannot be easily access this data.

2) Data Storing Centre

Data storing center stores the user data. Data storing center provides a data to the data sharing service. It controls the accesses of outside users to the storing data and providing corresponding services. The data storing center having key authority that generates secrete user key with the KGC, and issues and revokes attribute group keys to authorized users according to their attribute, which gives a fine-grained user access control.. Data Storage Centers provides services like offsite record and storage, retrieval, delivery.

3) User

The user is a person who use this system. The user access the data. If a user having a set of attributes satisfying the access policy of the encrypted data and these policies defined by the data owner, and is not same as any of the attribute groups, then he decrypt the cipher text and obtain the data. The user can send the key request for decryption of data to the data owner. The received message can be decrypt using the key send by data owner.

4) Key Generation Centre

Key generation center generates public and private keys for CP-ABE. It is used for issuing, updating and revoking attribute keys for users. Based on their attributes it gives differential access rights to each users. Key generation center generate keys for cryptography. This key is used to encryption and decryption of the data.

III. ARCHITECTURE

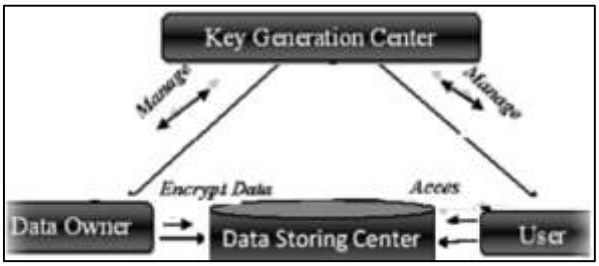

Fig. 1: Architecture of a data sharing system.

IV. METHODOLOGY

The key generation center and the data storing center generates users secrete key by using secure two-party computation (2PC) protocol. In the existing ABE schemes are based on the architecture where a single trusted authority, the Key generation center to generate the whole private keys of users by using its master secret information. So, the key escrow problem is the KGC can decrypt the cipher text addressed to users by generating their private keys at any time.

A. Cipher text – Policy ABE

We define the CP-ABE with user revocation capability scheme. This scheme consists of the following six algorithms:

1) Setup:

This algorithm is a randomized algorithm that takes no input other than implicit security parameter. It gives outputs the master key MK and public key PK.

2) Attribute KeyGen:

The attribute key generation algorithm has input master key, a attribute set and a set of user indices. It gives output is a set of private attribute keys for each user in U that identifies by the attributes set.

3) KEKGen:

This algorithm has input a set of user indices and outputs KEKs for each user in U, which will be used for encrypting attribute wise group keys.

4) Encrypt:

The encryption algorithm is a algorithm having input is public parameter (PK), a message, and an access structure A over the universe of attributes. It gives a cipher text such that only a user who satisfies set of attributes and that satisfies the access structure used to decrypt the message.

5) ReEncrypt:

The re-encryption is a randomized algorithm that has input the cipher text including an access structure and a attribute groups. If the attribute groups appear in A, and re-encrypts for the attributes; else, returns specifically, it outputs a re-encrypted cipher text such that only a user who satisfies the set of attributes and that satisfies the access structure and has a authorized member for each of them at the same time able to decrypt the message.

6) Decrypt:

The decryption algorithm takes the input cipher text which contains an access structure A, a private key SK, and a set of attribute group keys according to set of attributes.

All rights reserved by www.ijsrd.com

V. APPLICATION

- Sharing personal health record
- Personal data sharing
- Military application

VI. EVOLUTION AND RESULT

Fig. 6.1: Home page

Fig. 6.2: Registration page

Fig. 6.3: Login page

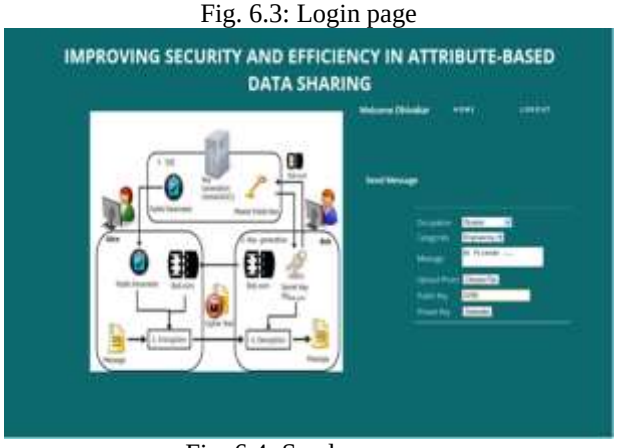

Fig. 6.4: Send message

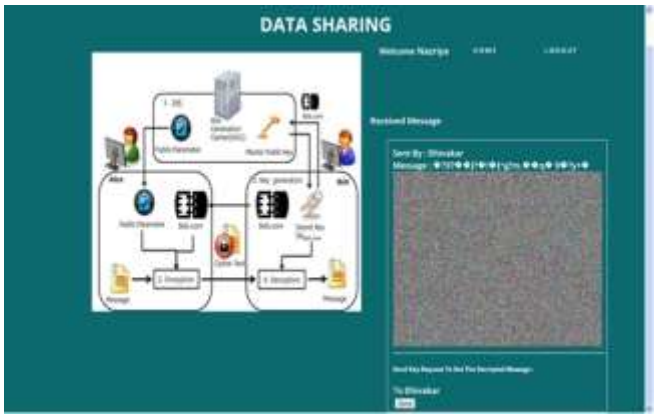

Fig. 6.5: View message

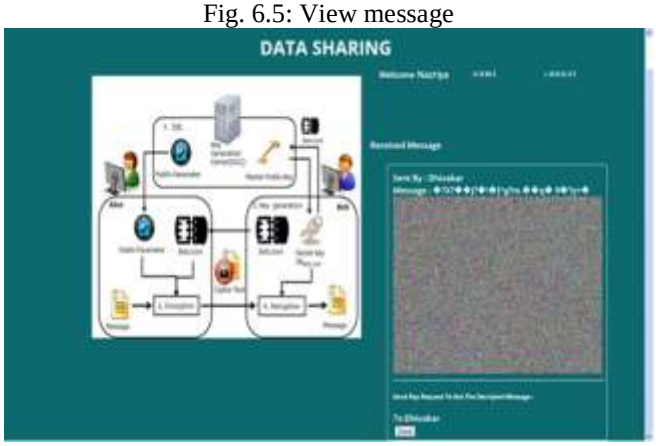

Fig. 6.6: Send Key Request

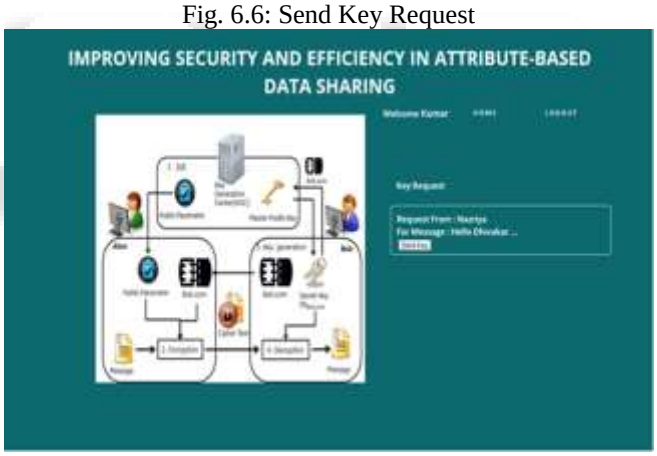

Fig. 6.7: Send Key

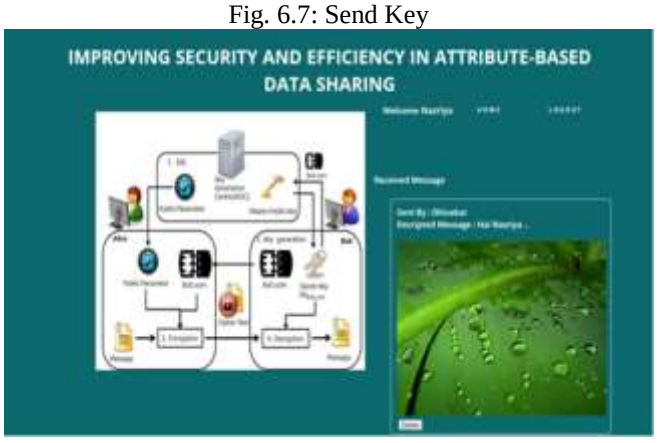

Fig. 6.8: View original message

VII. CONCLUSION

In this paper, we proposed attribute based data sharing scheme for fine-grained data access control. The given

All rights reserved by *www.ijsrd.com*

scheme features a key issuing mechanism that removes key escrow problem during the key generation. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing. This scheme can do an immediate user revocation for each attribute set while taking full advantage of the scalable access control provided by the cipher text policy attribute-based encryption.

VIII. FUTURE ENHANCEMENT

In the future, the attribute-based encryption systems by applying advanced technique for data sharing. In future, we encrypt multimedia content, to improve the performance, Neglected key expired time, we can use Proxy servers and multi Data Storing Centre to update user private key without sharing user attribute information.

REFERENCES

[1] Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing," IEEE. vol:25 ,no:10.october 2013.
[2] M. Pratheepa, R. Bharathi, "Improving Security and Efficiency in Attribute Based Data Sharing," IJSR, Volume 3, Issue 1, January 2014.
[3] B. SakthiSaravanan, R.Dheenadayalu, A.Vijayaraj, "Improving Efficiency and Security Based Data Sharing in Large Scale Network," IJESIT, Volume 2, Issue 1, January 2013.
[4] John Bethencourt, Amit Sahai, BrentWaters, "Ciphertext-Policy Attribute-Based Encryption", IEEE, pp: 321-334,2007.
[5] R. Ostrovsky, A. Sahai, and B. Waters,"Attribute-Based Encryption with Non-Monotonic Access Structures", IEEE, pp:195-203, 2007.
[6] A. Lewko, A. Sahai, and B.Waters, "Revocation Systems with Very Small Private Keys", IEEE, pp:273-285, 2010.
[7] A. Boldyreva, V. Goyal, and V. Kumar,"Identity-Based Encryption with Efficientm Revocation", ACM cof: , pp:417-426, 2001.
[8] S. Rafaeli and D. Hutchison,"A Survey of Key Management for Secure Group Communication", ACM Computing Surveys, vol:35, no: 3, pp:309-329, 2003.
[9] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen," A Content- Driven Access Control System", Identityand Trustonthe Internet, pp:26-35, 2008.

All rights reserved by *www.ijsrd.com*