International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 602 - 603

A Review on Enhancing Organization Security using Attribute-Based Encryption for Data Sharing

Ms. Priya D. Tangde
M.E.First Year, CSE
Anuradha Engineering College, Chikhli
Maharashtra, India
priya.tangde@rediffmail.com

Prof. Avinash S. Kapse
Ph.D.(Pursuing),
M.E.(CSE),B.E.(CSE), Department of Computer Science & Engg.
Anuradha Engineering College, Chikhli
Maharashtra, India
askapse@gmail.com

Dr. V. M. Thakare
Professor & Head
Department of CS
Sant Gadge Baba Amravati University, Amravati
Maharashtra, India
vilthakare@yahoo.co.in

Abstract:-With the recent growth of networking, peoples can share their data with others through online, by using social networks or cloud computing but at the same time there has been increasing demand for data security. People would like to make their private data only accessible to the authorized people. In data sharing systems, access policies and the support of policies updates are most challenging issues. Attribute-based encryption (ABE) and Cipher text policy attribute based encryption (CP-ABE) are becoming promising cryptographic solutions to this issue and achives a fine-grained data access control. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. The major drawback of these systems is the key escrow problem. The proposed scheme solves the key escrow problem which depends on attribute based encryption technique for the shared data. Paillier Cryptosystem is utilized for encryption of keys for assignment and revocation process while Twofish algorithm is used to encrypt and decrypt stored data of users. Whenever data owner upload personal documents on cloud server, first the keywords will get fetched from the documents and index will be created. Lucene indexing algorithm is used for indexing of keywords. A Blind Storage scheme allows a client to store a set of files on a remote server.

Keywords— *Data Sharing, Attribute Based Encryption, Lucene, Paillier Cryptosystem.*

*****

I. INTRODUCTION

Due to large number of internet users, it is also required to protect our data from being misused. An unauthorized person should not be made access to the private data of an individual. For this reason we are required to take care of data by implementing data protection techniques like cryptography.
Our work in this area is based on Attribute based Encryption. It is one of the techniques that are more suitable for storing data with encryption. While sharing of data, system provide Data confidentiality, Fine grained access control, Removing Key escrow problem, Removing Revocation problem, Scalability [1].

Cloud contains large amount of data stored in it, hence retrieving the correct information plays a very important role. Indexing can greatly improve the speed of information retrieval. The indexing of document collection is performed by Lucene [2] .Privacy and security are the important issues in cloud computing. In the exiting system KGC is not separated from master admin, hence master admin knows both keys that generated from KGC so in the absence of user master admin may access the private data. This problem is overcome in the proposed system as KGC is separated from the master admin.

II. LITERATURE SURVEY

In [1], Junbeom Hur proposed 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. But the limitation of this system was reliability and load balancing under real time environment.

In [3], author proposed a novel CP-ABE scheme is used to solve the key escrow problem by escrow free key issuing protocol generated by using two party computations. Fine-grained user revocation per each attribute could be done by proxy encryption. They have done servey based on existing Attribute based encryption schemes and their implementation which gives an idea that there are still limitations in existing system also these approaches gives idea about more scope in encryption techniques.

In [4], the authors presented comparative study of different attribute based encryption schemes like KP-ABE,CP-ABE, ABE with non monotonic access structure, HABE,MABE based on various parameters suggest that these schemes are classified according to their access policy and after analyzing these schemes we found that the main access policies are KP-ABE and CP-ABE and further policies are derived using either of these policies as a base and found that cipher text policy based ABE schemes are more efficient and scalable to securely manage user data in the data sharing system.

In[8], author introduced a new Cryptograhic construct called Blind Storage and implemented it using a novel, light weight protocol ScatterStore. Also showed how a dynamic SSE scheme can be constructed using Blind Storage.

III. XISTING SYSTEM

In this system 2PC protocol is used and the encryption is done with the help of the two keys generated. The plaintext entered by the data owner is encrypted partially by the public key which resides with the master admin and the other partial half is done with the help of the private key which resides with the

data owner. The 2PC protocol works on SSL handshake which is a technique used to manage the encryption keys during the plaintext encryption done by both the keys. Similarly, the decryption of data is done by the private key from the admin and the public key from the user[1]. Key escrow is not fully resolved in this system which dealt with key revocation.

IV. PROPOSED SYSTEM

We proposed a scheme which consists of following components Paillier Cryptosystem, User, key Generation Center, Lucene indexer and Blind Storage.

Paillier Cryptosystem:
The Paillier Cryptosystem is a modular, public key encryption scheme, created by Pascal Paillier [5]. In this paper, Paillier Cryptosystem is utilized for encryption of keys for assignment and revocation process while Twofish algorithm is used to encrypt and decrypt stored data of users.

User: In this system the user has two access control list which is Read and Write , Read Only. In first access control list user has privilege to modify, encrypt and decrypt the data, while in second access control list the user can only view the data.

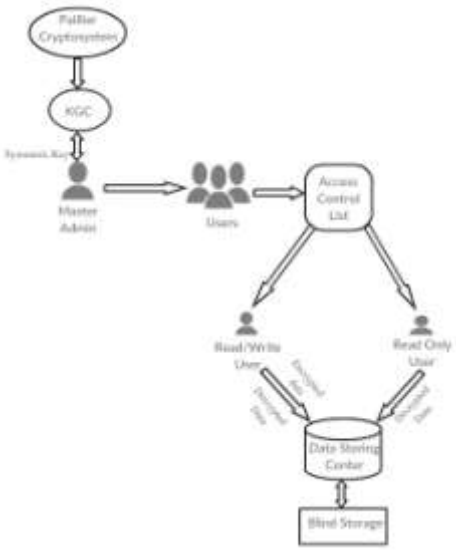

Fig. 1. Proposed System Architecture

KGC (Key Generation Center): The key generation center randomly generates the private key and assign to the user. When the key expires the user contact with the master admin to generate a new key from KGC. This key also has validity set during assignment.

Lucene Indexer:
Whenever data owner upload personal documents on cloud server, first the keywords will get fetched from the documents and index will be created. For creating index of keywords fetched from document, Lucene indexing algorithm has been used. Lucene is full-text search engine architecture, provides**:** a complete query and indexing engine.
Lucene has several advantages like an index is file format and application platform independent. It provides search over documents. Index is managed over dynamic collection of documents Lucene provides continuous updates to the index as the documents are inserted and removed from the storage repository by user. These documents will consist of any number of various fields and that vary according to documents. Lucene API is not dependent on any file formats. First textual information from pdf, HTML, Microsoft word, and many others (except images) get extracted and then index get create [2]. Whenever data owner upload personal documents on cloud server, it may have the security issues over the data confidentiality and authentication access control.

Blind Storage:
The blind storage allows a client to store a set of files on a remote server that the server does not familiar with the files that are stored in it [6].

The encryption technique used here is Twofish. Twofish is a symmetric key algorithm. It generates only one key which is a private key. When the key expires the user contacts with the master admin to generate a new key from KGC. The master admin generates the key and assigns the key to the user. If the user privileges are read and write the previously entered data is re-encrypted and is stored with the user.

V. CONCLUSION

In this paper the proposed scheme issues a key that removes key escrow problem. Paillier Cryptosystem is utilized for encryption of keys for assignment and revocation process. The system uses blind storage which helps the user to store the file in a secure way and indexing is given for each file for easy retrieval.
The resulting system effectively achieve confidentiality of documents and index and more secure than exiting system.

REFERENCES

[1] Junbeom Hur “Improving Security and Efficiency in Attribute-Based Data Sharing”, VOL. 25, NO. 10, OCT2013
[2] Addagada, Sridevi "Indexing and Searching Document Collections using Lucene" (2007) University of New Orleans Theses and Dissertations. Paper 1070
[3] Apurva Gomase1, Prof. Vikrant Chole2 ”A Review on Secure System Implementation using Attribute Based Encryption” IJCSMC, Vol. 3, Issue. 11, November 2014, pg.465 – 468
[4] Mangesh Gosavi1 , Tabassum Maktum2 “Survey of Various Attribute Based Encryption Schemes Used in Data Sharing System” IJARCSSE, 2015
[5] The Paillier Cryptosystem By Michael O’Keeffe The College of New Jersey Mathematics Department April 18, 2008
[6] D. Kavitha, S. Hemavathy “A Survey on Cloud Computing Security Issues And Multi-Keyword Ranked Data Search Efficiency in Blind Storage” Vol. 3, Issue 9, September 2015
[7] Keerthi B, V Rajesh kannan “Implementation of Attribute Hiding Strategy and Key Revocation in Cloud Environment” IJISET Vol. 1 Issue 2, April 2014.
[8] Muhammad Naved, Manoj Prabhakarn, carl A.Gunter ”Dynamin Searchable Encryption Via Blind Storage” Univercity of Illinois at Urbana-Champaign
[9] Changsha Ma ; Chang Wen Chen “Secure media sharing in the cloud :Two-dimensional-scalable access control and comprehensive key management”, Multimedia and Expo (ICME), 2014 IEEE International Conference, DOI: 10.1109 /ICME. 2014. 6890308 , Publication Year: 2014 , Page(s): 1 -6