ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Prototype for Keyword Search Mechanism Using Identity-Based Encryption

Saroj Khyalia, Ramya B K

M. Tech Student, CNE Branch, Dept. of ISE, SJBIT, VTU, Bengaluru, India

Assistant Professor, Dept. of ISE, SJBIT, VTU, Bengaluru, India

ABSTRACT: In existing system, many encryption techniques were used. One among that was public-key searchable encryption scheme. This scheme took search time linear because of which it was very difficult to obtain the data from the large-scale database. The search complexity of this scheme was dependent on the total number of the ciphertexts. To overcome this problem, new scheme is proposed. In this scheme the keyword could be searched faster when compared to the existing schemes. This scheme is constructed in such a way that ciphertext would be searched based on the rank. Identity-based encryption (IBE) and identity-based key encapsulation mechanisms (IBKEM) which are semantically secure and anonymous are used. The search complexity is based on the number of ciphertexts having the queried keyword.

KEYWORDS: Encryption, Public-Key Encryption, Trapdoor.

I. INTRODUCTION

Encryption is usually used for the security purpose. It is mainly used to achieve data security. Encryption is a process of converting the readable text into the unreadable text. For the data to be secure it is very necessary that encryption is to be performed. There are two types of encryption techniques in cryptograpy namely symmetric encryption and asymmetric encryption. In symmetric encryption, the key used for encryption and decryption is same. In asymmetric encryption the keys used for encryption and decryption are different, here he data will be more secure.

Public-key encryption is a type of asymmetric encryption where two different keys are used for encryption and decryption. For encryption purpose usually the public-key is used and for the decryption purpose private-key is used. In public-key encryption, a person can use the receiver's public-key to encrypt the data and upload in the data server or any public server. This kind of encrypted data can only be decrypted using the receiver's private-key.

A trap doorin an information processing system is an entrance point which circumvents the normal safety measures. It is a hidden program or an electronic component by which the protection system becomes ineffective.

Public-key encryption with keyword search (PEKS) is same as the public-key encryption. This was introduced by Boneh et al. which had an advantage that anyone who knew the public-key of the receiver can upload the data. This scheme had a disadvantage that it took the search time linear due to which the retrieval from the large database would be difficult.

To overcome this problem, a new scheme is proposed [8]which we are using, where the high efficient search performed can be obtained without sacrificing the semantic security. Semantic security can be safeguarded in two ways namely 1) if no catchphrase look trapdoor is known, all ciphertexts are vague, and no data is spilled about the structure, and 2) given a watchword seek trapdoor, just the comparing relations can be uncovered, and the coordinating ciphertexts release no data about whatever is left of ciphertexts.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

II. RELATED WORK

In the prior year find on encoded information has been generally examined. Since a cryptographic perspective, the possible work is partitioned into two classifications. To begin with is Symmetric searchable encryption and second is Public-key searchable encryption.

Symmetric searchable encryption is also called as the symmetric-key encryption with keyword search (SEKS) where the same key is used for encryption and decryption. This was first introduced by Song et al. [1] in the year 2000. In this paper the deterministic encryption algorithms were used. Deterministic encryption schemes are the one which produced the same ciphertext always for any plaintext and the key even when executed on different encryption algorithms. The drawback of this paper was it used linear search approach to search the keywords.

Curtmola et al. [2] in the year 2006 paper was also based on the SEKS scheme but it was proved to be semantically secure i.e., no extra information about the matching ciphertext was revealed. The drawback of this paper was that the length of the keyword search trapdoor was linear to the size of the database.

Chase et al. [3] in the year 2010 proposed a scheme to encrypt the structured data. A secure method to search this structured data was also proposed. The drawback of this paper was that it did not concentrate much on the unstructured data.

Brakerski et al. [4] in the year 2011 deterministic PKE scheme was proposed with better security. The drawback of this paper was that this scheme was not semantically secure i.e., it would reveal the information about the matching ciphertexts.

Kamara et al. [5] in the year 2012 proposed the dynamic searchable symmetric encryption to support the dynamic update of the encrypted data. The drawback of this paper was that the time taken to update the encrypted data was more.

Arriaga et al. [6] in the year 2014 proposed the PEKS scheme to maintain the keyword search trapdoors security or privacy. The drawback of this paper was that the trapdoors could not be fully hidden from the server and would leak the frequency of the keywords.

III. SYSTEM DESIGN

There are 4 modules in this project as shown in fig. 1. It consists of data owner, data server, end-user and the verifier.

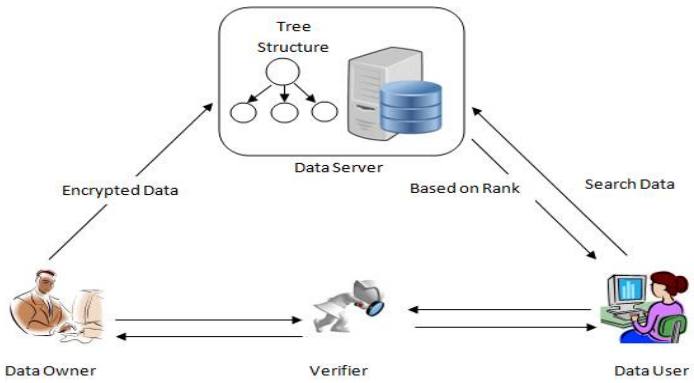

Fig. 1. System Architecture

The data owner uploads the file to the data server and the end-user searches the file in the data server using the keyword. Before data owner uploads a file to the data server he should be verified by the verifier whether he is a valid user or not. If not the data owner has to first register himself and should login using his username and the password. Only after the data owner is verified by the verifier he can upload the encrypted data to the data owner.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

If the end-user wants to search any data in the data server he should first be verified by the verifier if he is valid or not. If not then he has to first register and then login using username and password. After the end-user is verified he can search the data in the data server using the keyword.

Data server will receive the request from the end-user, after receiving it would search if the data is present or not in its database. If the data is present then the server would send the requested data back to the end-user based on the rank.

Verifier is used to authenticate both the data owner and the end-user if they are authorized users or not.

IV. IMPLEMENTATION

1. Identity-Based Encryption (IBE)

This is the algorithm used in this paper for encryption of the data. The fig. 2 shown below shows the IBE[7] procedure.

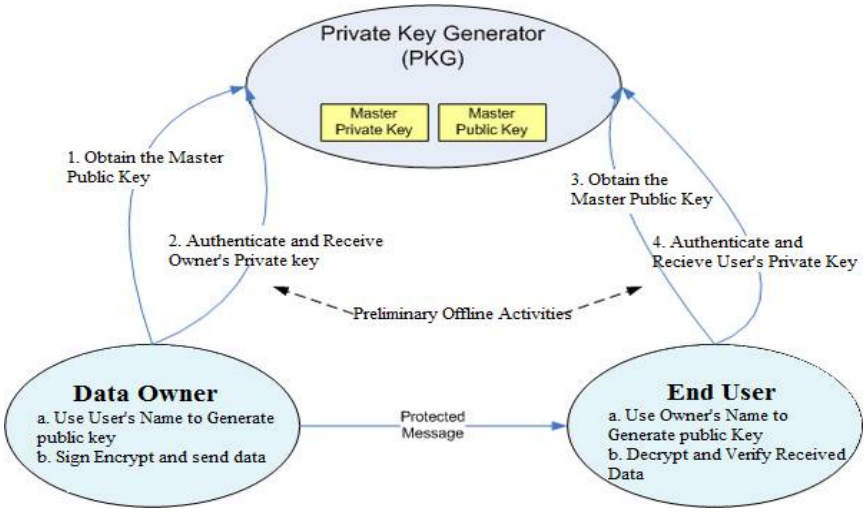

Fig. 2. IBE Procedure

Data owner before uploading the data he will obtain the masters public key from the public key generator and after receiving the public key he will authenticate himself using his own private key. In the same way even the end user before searching for a keyword he will obtain masters public key and will authenticate him using his own private key. Then the data owner encrypts the data and sends it to the user and the user will receive the data. End user will verify and decrypt the data received from the data owner.

2. Prototype

The Fig. 3 shows the processes happening in the data server i.e., the login process of the data owner and the end user. The verifier checks the credentials of both the data owner and end user before the data owner uploads the file and the end user search for the keyword. If the credentials of the data owner and end user matches then a pop up message arrive that they have logged in the data server successfully. In the fig shown below, the green arrows show the verifier checking the credentials of the end user before searching the keyword.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

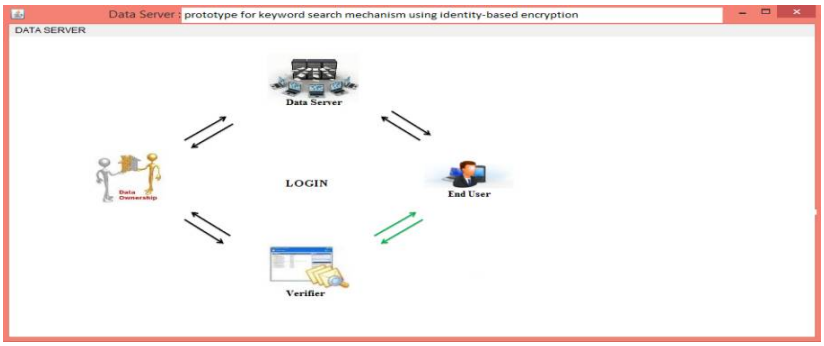

Fig. 3. Prototype for Data Server

The Fig. 4 shows the data owner uploading the file to the data server after successful registration. After the verifier checks the credentials of the data owner and if the credentials are matched then he can login into the data server. Once he is logged in then the screen shown in below occurs. Then the data owner will browse the file and upload the file to the data server.

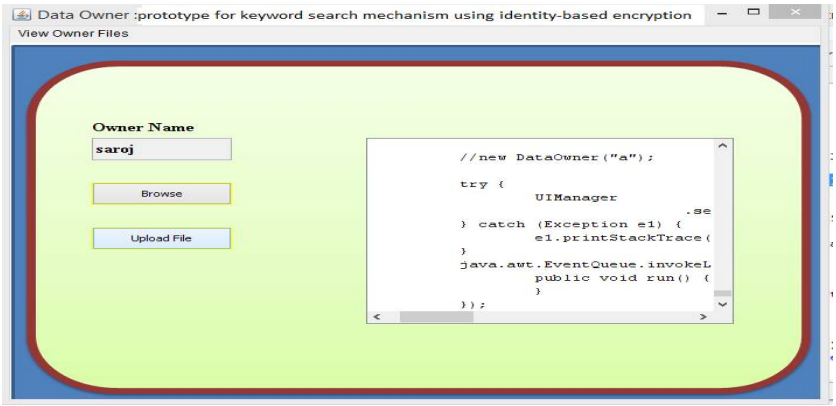

Fig. 4. Prototype for Data Owner to upload the file to the data server

The Fig. 5 shows the end-user searching the keyword in the data server after successful registration. Once the verifier checks the credentials of the end user and the credentials are matched then the end user can login to the data server to search for the keyword. The screen shown below occurs where the end user will first request for the secret key and then he will search for the keyword within a particular file or a file with that keyword.

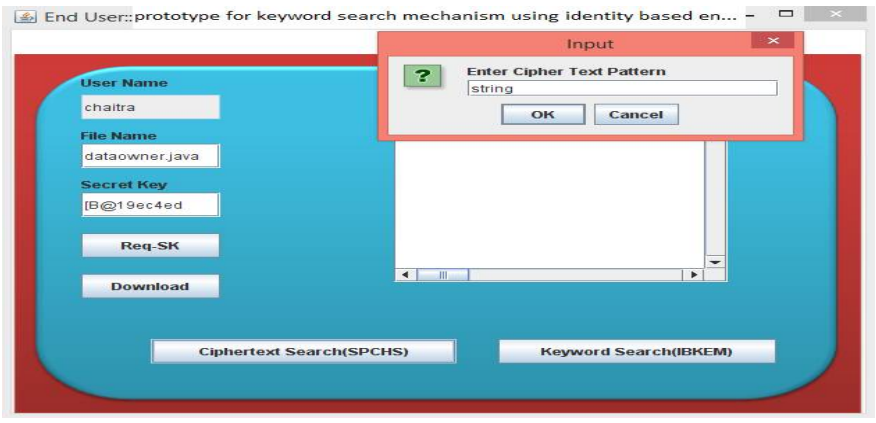

Fig. 5. Prototype for End-User to search the keyword

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

V. RESULTS

The Fig. 6 shows the results obtained after the end-user search the keyword. It shows which keyword the end-user has searched and the time taken to search that keyword. It also shows the time delay taken for searching the keyword.

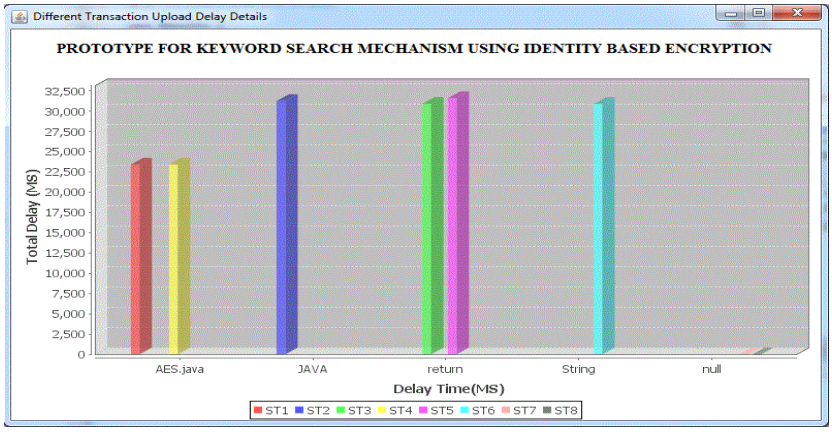

Fig. 6. Graph obtained after the keyword search

VI. CONCLUSION AND FUTURE WORK

In this paper we can see that the new scheme is proposed which takes less time to search the keyword compared to the existing schemes. This scheme is semantically secure i.e., it would not reveal any extra information about the matching ciphertexts. The search complexity in this scheme is dependent on the number of ciphertexts containing the queried keyword. Few encryption algorithms are used in this paper for the encryption of the data. In the future we are going to apply new encryption algorithms and analyse the system performance

REFERENCES

1. D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEES&P,May2000, pp. 44–55.
2. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions andefficient constructions,” in Proc. ACM CCS, 2006, pp. 79–88.
3. M. Chase and S. Kamara, “Structured encryption and controlled disclosure,” in Advances in CryptologyASIACRYPT (Lecture Notes in Computer Science), vol. 6477, M. Abe, Ed. Berlin, Germany: Springer-Verlag,2010,pp. 577–594.
4. Z. Brakerski and G. Segev, “Better security for deterministic public-key encryption: The auxiliary- input setting,” inAdvances inCryptology—CRYPTO (Lecture Notes in Computer Science), vol. 6841, P. Rogaway,Ed. Berlin,Germany: Springer-Verlag, 2011, pp. 543–560.
5. S. Kamara, C. Papamanthou, and T. Roeder, “Dynamic searchable symmetric encryption,” in Proc. ACM Conf. Comput. Commun. Secur., 2012, pp. 965–976.
6. Arriaga, Q. Tang, and P. Ryan, “Trapdoor privacy in asymmetric searchable encryption schemes,” in Progress in Cryptology—AFRICACRYPT (Lecture Notes in Computer Science), vol. 8469, D. Pointcheval and D.Vergnaud,Eds. Berlin, Germany: Springer-Verlag, 2014, pp. 31–50.
7. https://en.wikipedia.org/wiki/ID-based_encryption.
8. Peng Xu, Qianhong Wu, Wei Wang, Willy Susilo, Josep Domingo-Ferrer and Hai Jin, “ Generating SearchablePublicKey Ciphertexts With Hidden Structures for Fast Keyword Search,” IEEE Transactions on Information Forensics andSecurity, Vol. 10, No. 9, September 2015.

BIOGRAPHY

Saroj Khyalia is a student pursuing M.Tech in Computer Network Engineering, Department of Information Science and Engineering, SJB Institute of Technology, VTU, Bengaluru, India.Her area of interest is computer networks, security etc.

Ramya B K working as Assistant Professor Department of Information Science and Engineering, SJB Institute of Technology, VTU, Bengaluru, India. Her areas of interests are computer network (Wireless Sensor Network), Cloud Computing.