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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

# Efficient Keyword Search for E-Health Record in Cloud Server

Neha kouser, Kumar H R.

PG Student, Dept. of C.S.E., SIET, Visvesvaraya Technological University, Belagavi, India[1]

Assistant Professor, Dept. of C.S.E., SIET, Visvesvaraya Technological University, Belagavi, India[2]

**ABSTRACT**-An electronic health record system is a new application that will bring very good convenience in healthcare. The security and privacy of sensitive personal information are the major interest of users, which could make difficult for further development and commonly adoption of the system. The searchable encryption scheme is a technology to incorporate privacy and security protection and favorable operability functions together, which can play an significant role in electronic health record system. In this paper we present a new cryptographic primitive named as efficient keyword search keyword search with designated tester and timing enabled proxy re encryption function (Re-dtPECK), which is a kind of time dependent searchable scheme. This provides the patients to give the access right permission to other users to operate search function on the personal record in limited time period. The process of searching and decrypting the encrypted document of the data owner by other user can controlled by the data owner. The other user could be automatically take access and search permission after a specific period of efficient time. It can avoid keyword guessing attack and support conjunctive keyword search. The existence of certain keyword can be tested only by the chosen tester. We design a security model and a system model for the proposed Re-dtPECK scheme to show that it is an efficient scheme proved secure in the standard model.To provide more security we use the concept of OTP.The comparison and wide simulations demonstrate that it has a low computation and storage overhead.

**KEYWORDS:** Searchable encryption, time control, conjunctive keywords, designated tester, e-health, resist offline keyword guessing attack.

## I. INTRODUCTION

Nowadays the e-health record system has been very famous.The e-health record system will make medical records to be computerized with the ability to prevent medical errors. The electronic health record system help a patient to create his own health data in one hospital and manage or share the information with other in other hospitals. Many patient-centric EHR system have been implemented such as google health and Microsoft healthvault. The prospect to deploy the EHR system everywhere comes up with the privacy of the patient. The data collected at the healthcare data center contains private data and may be vulnerable to potential leakage and this data may be disclosed to individuals or companies who make profit from that data. Although the service provider can make the patient to believe that the information is secure ,the EHR could be exposed if the server is intruded or an inside staff misbehaves. The obstacle that stands in the way of wide adoption of the EHR system is the concern about privacy and security. The public key Encryption scheme with keyword search(PEKS) allows the user to search on encrypted data without decrypting it. Which is suitable to raise the security of EHR system.

In some cases, if a patient may want share his information with someone, who can be his doctor, without revealing his own private key. To fulfill this requirement the proxy Re-encryption(PRE) method can be introduced..The encrypted index of the patient can be converted into Re-encrypted form by the cloud server on which the delegatee can search. Still another problem arises when the access right is dissemented. When the patient recovers or transferred to another hospital, that time he does not want this private information to be searched or used by his previous physician anymore. To solve this problem a possible approach is to Re-encrypt all this data with a new key. One time password(OTP) is an automatically generated numeric or alphanumeric string or characters that authenticates the user for a single transaction or session.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

## II. RELATED WORK

**Conjunctive Keyword Search**

Various constructions of public key encryption with conjunctive keyword search (PECK) over encrypted data have been proposed[2][3]. It allows the users to query multiple keywords at the same time. However, some of them such as the solution in[3]and [4] have high communication or computation cost. On the other hand, some schemes require an index list of the queried keywords when a trapdoor is generated, which will leak information and impair the query privacy.

**Searchable Encryption With Designated Tester**

In practice, the size of a keyword space is always no more than its polynomial level. An attacker is possibly to launch dictionary attacks or off-line keyword guessing attacks (KG attacks) to exploit the hidden keywords. The EHR keywords are usually selected from a small space, especially the medical terminology.

If an adversary finds that the trapdoors or encrypted indexes have lower entropies, the KG attacks could be launched if the adversary endeavors to guess the possible candidate keywords. In order to resist the threats, the concept of PEKS with designated tester (dPEKS) is proposed. Only a designated tester, which is usually the server, is capable to carry on the test algorithm. The enhanced security models[1][7]and[8] have also been put forward. However, they could not support multiple keywords query or delegate search function.

## III. PROPOSED SYSTEM

In this paper, We try to solve the problem with a new mechanism proposed to automatically cancel the delegation right after a period of time given by the data owner. It implies all the users including data owner are constrained by the time period.

The beauty of the proposed system is that there is no time limitation for the data owner because in the re-encryption phase the time information is embedded.

A time token is generated for every users, A server is used for the process of generation of time token. After receiving a effective time period T from the data owner, the time server generates a time seal St by using his own private key and public key of delegatee.By the Re-encryption algorithm executed by the proxy server, the time period T will be embedded in Re-encryption ciphertext.

To provide better security for the proposed system we use OTP,OTP is more secure then a static password, especially a user-created password which is typically weak.

**Advantages of proposed system:**

We design a novel SE scheme supporting secure conjunctive keyword search and authorized delegation function. Compared with existing schemes, this work can achieve timing enabled proxy re-encryption with effective delegation revocation.

Owner-enforced delegation timing preset is enabled. Distinct access time period can be predefined for different delegatee.

The proposed scheme is formally proved secure against chosen-keyword chosen-time attack. Furthermore, offline keyword guessing attacks can be resisted too.

The security of the scheme works based on the standard model rather than random oracle model. This is the first primitive that supports above functions and is built in the standard model.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

## IV. SYSTEM ARCHITECTURE

The figure 1 presents the HER cloud environment of the proposed Re-dtPECK scheme. There are Three entities, A Data owner, Data user and Data center.The data owner wants to store his private EHR files on a third-party database. He extracts keywords from the EHR files and encrypts those plaintext keywords into the secure searchable indices. The EHR files are encrypted to ciphertext. Then, those information are outsourced to the data center.A data center consists of an EHR storage provider and a search server. The storage provider is responsible for storing data and search server performs search/add/delete operations according to users' requests. A user generates a trapdoor to search the EHR files using his private key and sends it to the search servers. After receiving the request, the search servers interact with the EHR storage provider to find the matched files and returns those retrieved information to the user in an encrypted form.

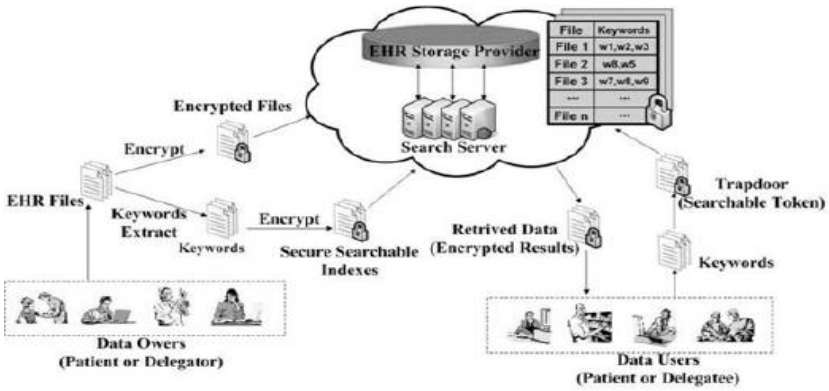



Fig. 1. System Model.

In Fig. 2, the timing enabled proxy re-encryption searchable encryption model is shown. In this model, we highlight the implementation of the time controlled function. The data owner acting as a delegator sends a list of delegation effective time periods for his delegatees to the time server and the proxy server. The entry of the list contains the identity of each delegatee and the effective time period, such as "Jim, 01/01/2014 – 11/01/2015".It indicates that the delegatee Jim is authorized to issue queries and perform decryption operations on the encrypted data of the data owner from Jan. 1th, 2014 to Nov. 1th, 2015. After receiving the list, the time server generates a time seal for each delegatee, which is transmitted to individuals. The time seal is a trapdoor of an effective time period and concealed by the private key of the time server. In the re-encryption operation, the proxy server will encapsulate the effective time into the re-encrypted ciphertext. In order to reduce computing cost, the proxy server will not re-encrypted ciphertext until they are accessed, which is so called lazy re-encryption mechanism. In the query phase, the data owner can conduct ordinary search operations with his own private key. However, the delegatee has to generate a keywords trapdoor with the help of the time seal. The cloud data server will not return the matched files unless the effective time encapsulated in the time seal accords with the time in the re-encrypted ciphertext.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

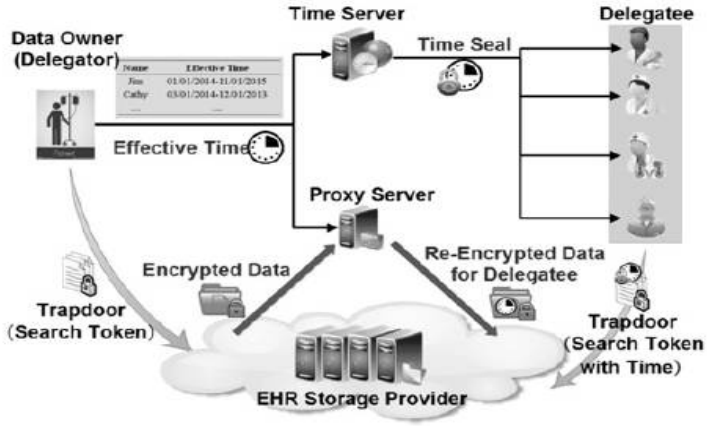
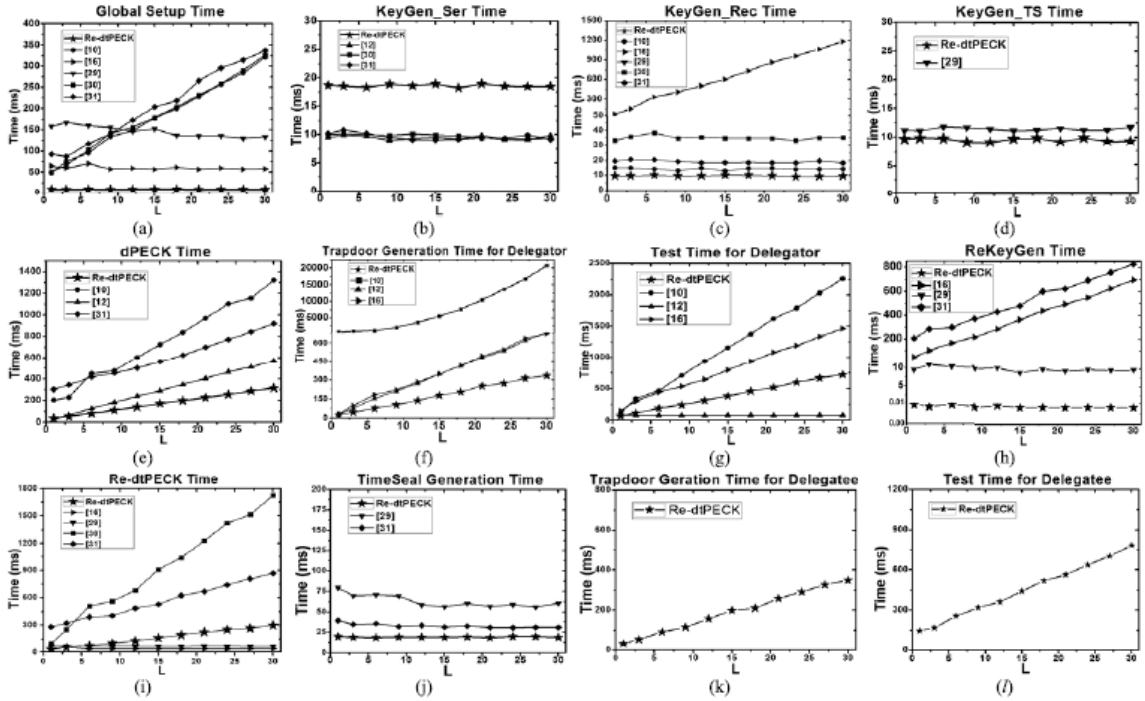



Fig. 2. Timing Enabled Proxy Re-encryption Searchable Encryption Model.

## V.SIMULATION RESULTS

We have evaluated the proposed Re-dtPECK scheme by implementing key components on an experimental workbench, including the system global setup, the key generation, the re-encryption key generation, the trapdoor generation and the test algorithms. The pairing-based cryptography (PBC) Library is used. We have elected the type-A elliptic curve parameter, which provides 1024-bit discrete log security strength equivalent to the group order of 160-bit. The experiments have been executed on a PC running Windows7 with an Intel core CPU at 2.5GHz and a 4.0 GB of the memory. We have evaluated the communication, the computation and the storage overhead of the proposed scheme. To the best of our knowledge, there is no existing work with the searchable encryption and delegation function to provide such experimental results.



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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

## VI.CONCLUSION

In this paper, we have proposed a Re-dtPECK scheme to accomplish the timing enabled privacy-preserving keyword search mechanism for the Electronic health record cloud storage, which could support the automatic delegation revocation. The security analysis and results indicate that our scheme holds much higher security than the existing system. This is the first SE scheme with the timing enabled proxy re-encryption function and the designated tester for the privacy–preserving HER cloud record storage. The proposed system ensure that it is resistance to the KG attacks. Based on the standard model it has been prove secure.OTP provides better security for our system. our proposed scheme can achieve high computation and storage efficiency besides its higher security. Our simulation results shown that the computation and communication overhead of proposed system is feasible.

## REFFERENCES

[1] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *Inf. Sci.*, vol. 238, pp. 221–241, Jul. 2013.
[2] M.-S. Hwang, S.-T. Hsu, and C.-C. Lee, "A new public key encryption with conjunctive field keyword search scheme," *Inf. Technol. Control*, vol. 43, no. 3, pp. 277–288, 2014.
[3] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Theory Cryptogr. Conf.*, vol. 4392. Amsterdam, The Netherlands, Feb. 2007, pp. 535–554.
[4] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 262–267, 2011.
[5] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," *Inf. Sci.*, vol. 180, no. 13, pp. 2576–2587, 2010.
[6] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Proxy re-encryption with keyword search: New definitions and algorithms,"in *Proc. Int. Conf. Security Technol.*, vol. 122. Jeju Island, Korea, Dec. 2010, pp. 149–160.
[7] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search,"*Theoretical Comput. Sci.*, vol. 462, pp. 39–58, Nov. 2012.
[8] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Security models for delegated keyword searching within encrypted contents,"*J. Internet Services Appl.*, vol. 3, no. 2, pp. 233–241, 2012.
[9] K. Emura, A. Miyaji, and K. Omote, "A timed-release proxy re-encryption scheme," *IEICE Trans. Fundam. Electron., Commun.Comput. Sci.*, vol. 94, no. 8, pp. 1682–1695, 2011.
[10] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Inf. Sci.*, vol. 258,pp. 355–370, Feb. 2014.
[11] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang, "A conditional proxy broadcast re-encryption scheme supporting timed-release,"