iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1218

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for Electronic Health Cloud

Mrs. Rashi Saxena[1], N. Yogitha[2], G. Swetha Reddy[3], D. Rasika[4]
[1]*Associate Professor/Department of CSE/ CMR Technical Campus,Hyderabad,Telangana-501401*
[2, 3, 4]*Research Scholars/ Department of CSE/CMR Technical Campus,Hyderabad,Telangana-501401*

Abstract: ***An electronic health (e-health) record system is a new and innovative application that will bring great convenience in healthcare. The privacy and security of the sensitive personal information are the major concerns of the users, which could hold back further development and widely adoption of the systems. The searchable encryption (SE) scheme is a technology to incorporate security protection and favorable operability functions together, which can play an important role in the e-health record system. In this paper, we introduce a new cryptographic primitive named as conjunctive keyword search with designated tester and timing enabled proxy re-encryption function (Re-dtPECK), which is a kind of a time-dependent SE scheme. It could enable patients to envoy partial access rights to others to operate search functions over their records in a limited time period. The length of the time period for the delegatee to search and decrypt the delegator's encrypted documents can be controlled. Moreover, the delegatee(Owner) could be automatically deprived of the access and search authority after a specified period of effective time. It can also support the conjunctive keywords search and resist the keyword guessing attacks. By the solution, only the designated tester is able to test the existence of certain keywords. We formulate a system model and a security model for the proposed Re-dtPECK scheme to show that it is an efficient scheme proved secure in the standard model. The comparison and extensive simulations demonstrate that it has a low computation and storage overhead.***

Keywords: Server, Cryptography, Keyword search, Searchable encryption, Conjunctive keywords, e-health record system, designated tester, Cloud computing.

I. INTRODUCTION

Projects main aim is to provide Electronic health records (EHRs) which are proliferating, and financial incentives encouraging their use. Applying Fair Information Practice principles to EHRs necessitates balancing patients' rights to control their personal information with providers' data needs to deliver safe, high-quality care.

We describe the technical and organizational challenges faced in capturing patients' preferences for patient-controlled EHR access and applying those preferences to an existing EHR. This timing enabled proxy Re-Encryption searchable Encryption scheme highlight the implementation of the time span controlled operation. Delegator and Delegate communicate via proxy re-encryption server used for E-health document retrieval from EHD storage server. The proxy re-encryption scheme is used to provide reliable service to data user, hence time seal encapsulation technique, provide a time span and concealed by the secure key of the time span server to access the document or record from the EHD storage server. The EHD cloud document server will not return the similarity Document up to which the most appropriate time period encapsulated in plenty of your time and effort seal accords with plenty of your amount of time in the re-encrypted cipher text, which is different from traditional proxy re-encryption SE schemes.

II. EXISTING SYSTEM

Proxy re-encryption (PRE) enables a proxy with a re-encryption key to convert a cipher text encrypted by a delegator's public key into those that can be decrypted by delegatee's private key. Proxy re-encryption with public keyword search (Re-PEKS) has introduced the notion of keyword search into PRE.

The users with a keyword trapdoor can search the cipher text while the hidden keywords are unknown to the proxy. Later, Wang *et al.* has suggested an improved scheme to support the conjunctive keyword search function. All these Re-PEKS schemes are proved secure in random oracle model. Nevertheless, that a proof in random oracle model may probably bring about insecure schemes.

A. Limitations of Existing System

1) Existing systems have high communication or computation cost.

2) On the other hand, existing schemes require an index list of the queried keywords when a trapdoor is generated, which will leak information and impair the query privacy.

3) 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.

III. PROPOSED SYSTEM

In this paper, we endeavor to solve the problem with a novel mechanism proposed to automatically revoke the delegation right after a period of time designated by the data owner previously. It implies that all 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 the time information is embedded in the re-encryption phase. The data owner is capable to preset diverse effective access time periods for different users when he appoints his delegation right. An effective time period set by the data owner can be expressed with a beginning and closing time (for instance, 01/01/2014-12/01/ 2014). A time server is used in the system, which is responsible to generate a time token for the users. After receiving an effective time period T from the data owner, the time server generates a time seal ST by using his own private key and the public key of the delegatee. In that way, the time period T is encapsulated in the time seal ST . By the re-encryption algorithm executed by the proxy server, the time period T will be embedded in the re-encrypted ciphertext. It is the timing enabled proxy re-encryption function. When the delegatee issues a query request, he should generate a trapdoor for the queried keywords using his private key and time seal ST. Only if the time period encapsulated in the trapdoor matches with the effective time period embedded in the proxy re-encrypted ciphertext, the cloud service provider will respond to the search query. Otherwise, the search request will be rejected. In that way, the access right of the delegatee will expire automatically. The data owner needs not to do any other operation for the delegation revocation.

A. Advantages Of The Proposed System

1) To the best of our knowledge, this is the first work that enables automatic delegation revoking based on timing in a searchable encryption system. A conjunctive keyword search scheme with designated tester and timing enabled proxy reencryption function (Re-dtPECK) is proposed, which has the following merits.

2) We design a novel searchable encryption 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.

3) The proposed scheme is formally proved secure against chosen-keyword chosen-time attack. Furthermore, offline keyword guessing attacks can be resisted too. The test algorithm could not function without data server's private key. Eavesdroppers could not succeed in guessing keywords by the test algorithm.

IV. SYSTEM ARCHITECTURE

This project architecture describes about how a data will be stored in database. This describes how a user requests and an admin will generate a response. The detailed architecture is explained below.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

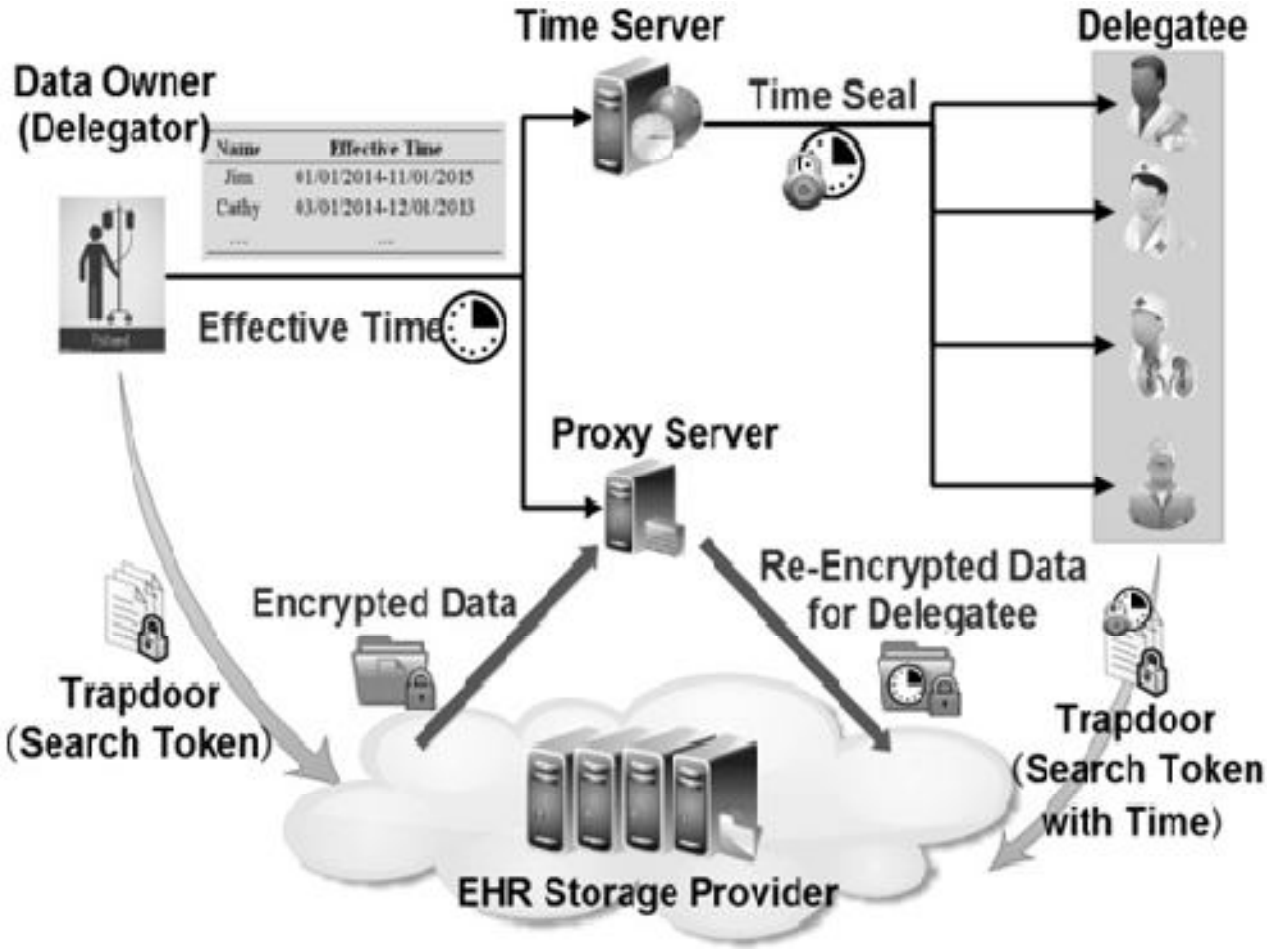


Fig. 3.1.1 Project Architecture

A. Modules Description

1) Modules

a) Delegator owner Module
b) Delegate Module
c) Conjunctive keywords
d) Proxy re-encryption
e) Time Seal Server

B. Module: Delegator Owner Module

The authority delegation is realized mainly by proxy re-encryption mechanism. The proxy server makes use of the re-encryption key to transform the cipher text encrypted by delegator's public key into another form, which can be searched by the delegatee using his own private key.

C. Module: Delegate Module

The delegatee will be divested of the search authority when the effective time expires. In order to achieve the time controlled access right revocation, the predefined time information is embedded in the re-encrypted ciphertext with a time seal. With the help of the time seal, the delegatee is able to generate a valid delegation trapdoor by Trapdoor R-algorithm. If the time information hidden in the re-encrypted cipher text is inconsistent with that in the delegation trapdoor, the equation in Test R-algorithm will not hold. Moreover, Workflow of Re-dtPECK. the search query of the delegatee will be rejected by the data server if the current time beyond the preset time.

D. Module: Conjunctive Keyword

Compared with the single keyword search, the conjunctive keyword search function provides the users more convenience to return the accurate results that fulfills users' multiple requirements. The users do not have to query an individual keyword and rely on an intersection calculation to obtain what they needs. To the best of our knowledge, there is no existing proxy re-encryption searchable encryption scheme could provide the conjunctive keywords search capability without requiring a random oracle. Our scheme has solved this open problem. The scheme could provide both the conjunctive keywords search and the delegation function. Unfortunately, it is proved in the random oracle (R.O.) model, which greatly impairs the security level.

E. Module: Proxy Re-Encryption

The proxy re-encryption technology is practical in EHR systems. It will greatly facilitate patient delegating the search and access rights. Schemes in could not provide the proxy re-encryption searchable encryption function to the users.

F. Module: Time Seal Server

An important design goal is to enable time controlled access right revocation. The delegation appointment will terminate when the preset effective time period disagrees with the current time. It should prevent the authorized user from accessing the records overtime.

V. HARDWARE AND SOFTWRE REUIREMENTS

A. Hardware Requirements

A Hardware interface specifies the logical characteristics of each interface between the software product and the hardware components of the system. The following are some hardware requirements.

1) System : Pentium IV 2.4 GHz
2) Hard Disk : 40 GB.
3) Floppy Drive : 1.44 Mb.
4) Monitor : 15 VGA Colour.
5) Mouse : Logitech
6) Ram : 512 Mb.

B. Software Requirements

Software Requirements specifies the logical characteristics of each interface and software components of the system. The following are some software requirements,

a) Operating system : Windows XP/7.
b) Coding Language : JAVA/J2EE
c) Data Base : MYSQL
d) Web Server : Tomcat 7.3
e) IDE : Net Beans/Eclipse

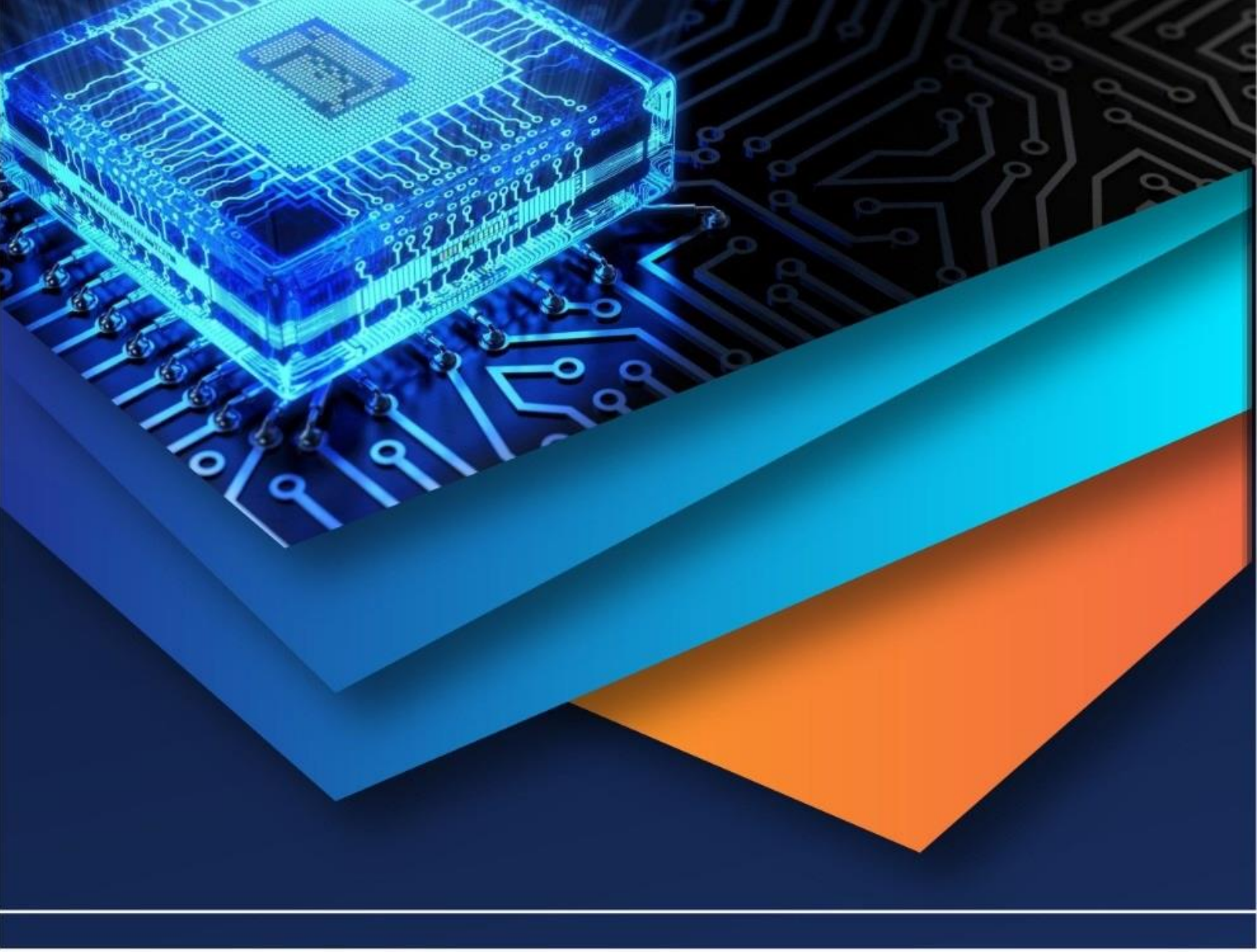
VI. CONCLUSIONS

In this paper, we have proposed a novel Re-dtPECK scheme to realize the timing enabled privacy-preserving keyword search mechanism for the EHR cloud storage, which could support the automatic delegation revocation. The experimental results and security analysis indicate that our scheme holds much higher security than the existing solutions with a reasonable overhead for cloud applications.

To the best of our knowledge, until now this is the first searchable encryption scheme with the timing enabled proxy re-encryption function and the designated tester for the privacy–preserving HER cloud record storage. The solution could ensure the confidentiality of the EHR and the resistance to the KG attacks. It has also been formally proved secure based on the standard model under the hardness assumption of the truncated decisional *l*-ABDHE problem and the DBDH problem. Compared with other classical searchable encryption schemes, the efficiency analysis shows that our proposed scheme can achieve high computation and storage efficiency besides its higher security. Our simulation results have also shown that the communication and computation overhead of the proposed solution is feasible for any real world application scenarios.

BIBLIOGRAPHY

[1] J. C. Leventhal, J. A. Cummins, P. H. Schwartz, D. K. Martin, and W. M. Tierney, "Designing a system for patients controlling providers' access to their electronic health records: Organizational and technical challenges," J. General Internal Med., vol. 30, no. 1, pp. 17–24, 2015.
[2] Microsoft. Microsoft HealthVault. [Online]. Available: http://www.healthvault.com, accessed May 1, 2015.
[3] Google Inc. Google Health. [Online]. Available: https://www.google.com/health, accessed Jan. 1, 2013.
[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, vol. 3027. Interlaken, Switzerland, May 2004, pp. 506–522.
[5] Yang Yang and Maode Ma,Senior Member,IEEE,"Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11,NO.4,APRIL 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY