JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

# Preserving and Retrieving Health Records using Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption in Cloud

**Sushma S A.[1*], Shubha C[2], Asha K[3]**

[1,2]Dept. of ISE, Siddaganga Institute of Technology, Tumkuru, India
[3]Dept. of CSE, Don Bosco Institute of Technology, Bengaluru, India

**Available online at: www.ijcseonline.org**

Accepted: 10/Sept/2018, Published: 30/Sept/2018

***Abstract-*** Electronic health records(EHR's) allows the patient to create his own health information in a hospital and share the information with other doctors in other hospitals.EHR provides security to the personal information of users. For providing privacy and security to EHR's we use SE(Searchable Encryption) which is a cryptographic technique that allows the user to search for a specific information in encrypted content. In this paper we have used conjunctive keyword search with designated tester and timer enabled proxy re-encryption function which is a time dependent SE scheme. Public key encryption with keyword search (PECK) allows the user to search on encrypted data without decrypting it. Sometimes the patient may want to provide access rights to others , it may be his doctor without revealing his private key. This can be accomplished using proxy re-encryption(PRE). Patients can provide partial access rights to others in a limited time period to perform search operations. The amount of time the third party can search and decrypt the encrypted documents can be controlled. The access rights can be revoked back when the time period expires. This prevents re-encryption of the entire document and generation of keys. A time server is used in the system to generate time tokens for users.

***Keywords***- Cloud, Health care, Keyword, Proxy, Delegates

## I. INTRODUCTION

THE ELECTRONIC heath records (EHR) framework will make medicinal records to be automated with the capacity to avert restorative blunders. Electronic Health records (EHRs) are multiplying, and monetary motivating forces energize their operation. Relating Reasonable Information Exercise values to EHRs needs changing patients' privileges to switch their own data with providers' data desires to take privileged, top notch mind [1]. It will encourage a patient to mark his private health record information in unique healing center that oversee or impart the information to others in dissimilar doctor's facilities. Numerous reasonable patient-driven EHR frameworks have been executed, for example, Microsoft Health Vault and Google Health [2]. Medicinal services information gathered in a server farm may contain private data and powerless against potential leakage and disclosure to the people or organizations who may make benefits from them. Despite the fact that the specialist co-op can convince the patients in the direction of trust that the protection information will be supervised, if the server is encroached or inside staff gets out of hand then the electronic health record could remain uncovered The genuine protection and security concerns are the intervening burden that obstructs wide selection of the frameworks.

## II. RELATED WORK

### A. Conjunctive Keyword Search

It allows the users to query multiplekeywords at the same time [3], [4]. Some schemes like[4] require an index list of thequeried keywords when a trapdoor is generated.

### B. Searchable Encryption With Designated Tester

The EHR keywordsare usually selected from a small space, especially the medical terminology.In order to resist the threats, the concept of PEKS withdesignated tester (dPEKS) is proposed in [5],[6]. Only adesignated tester, which is usually the server, is capable tocarry on the test algorithm.

### C. Proxy Re-Encryption With Public Keyword Search

Proxy re-encryption (PRE) enables a proxy with are-encryption key to convert a ciphertext encrypted by adelegator's public key into those that can be decrypted by delegatee's private key. Proxy re-encryption with public keywordsearch (Re-PEKS) [3] has introduced the notion of key-word search into PRE. The users with a keyword trapdoor cansearch the ciphertext while the hidden keywords are unknownto the proxy.

## III. EXISTING SYSTEM

Public key encryption scheme with keyword search (PEKS) allows a user to search on encrypted information without decrypting it, which is suitable to enhance the security of EHR systems. In some situations, a patient may want to act as a delegator to delegate his search right to a delegate, who can be his doctor, without revealing his own private key. The proxy re-encryption (PRE) method can be introduced to full fill the requirement. The server could convert the encrypted index of the patient into a re-encrypted form which can be searched by the delegate. However, another problem arises when the access right is disseminated. When the patient recovers and leaves the hospital or is transferred to another hospital, he does not want the private data to be searched and used by his previous physicians anymore. A possible approach to solve this problem is to re-encrypt all his data with a new key, which will bring a much higher cost. It will be more troublesome to revoke the delegation right in a scalable size.

**Disadvantages of Existing System:**

1. The serious privacy and security concerns are the overriding obstacle that stands in the way of wide adoption of the systems
2. Key words guessing can take place.
3. Re-encryption of the entire document is time consuming.
4. In the traditional time-release system, the time seal is encapsulated in the ciphertext at the very beginning of the encryption algorithm. It implies that all users including data owner are constrained by the time period.

## IV. PROPOSED SYSTEM

In this paper, we endeavour 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. 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. Owner-enforced delegation timing preset is enabled. Distinct access time period can be predefined for different delegate. The proposed scheme is formally proved secure against chosen-keyword chosen-time attack.

**Advantages of Proposed System:**

1. 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.

2. Keyword guessing attacks are prevented.

## V. SYSTEM ARCHITECTURE

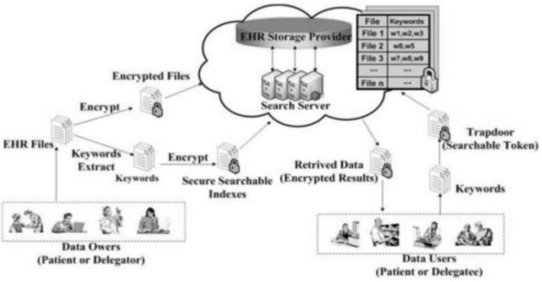

*Fig 1 System Model*

## VI. MODULES

We have 3 main modules in this project,

1. Data Owner Module
2. Data Center Module
3. User Module

**Module Description:**

**Data Owner:**

The data owner wants to store his private HER 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, that data are outsourced to the data center.

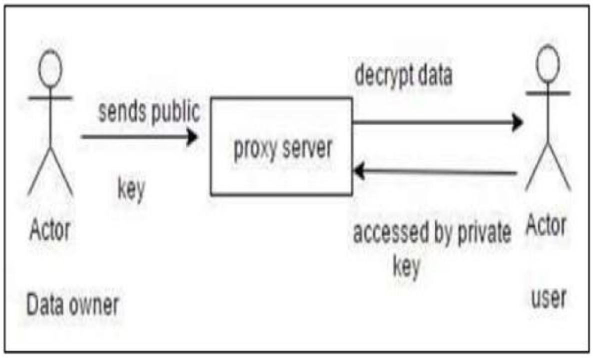

*Fig 2 Sequence Diagram for Data Owner*

**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.

**Data User:**

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.

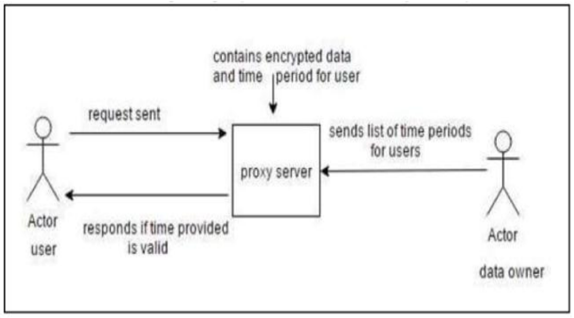

*Fig 3 Sequence Diagram for Data User*

## VII. ARCHITECTURE DESIGN

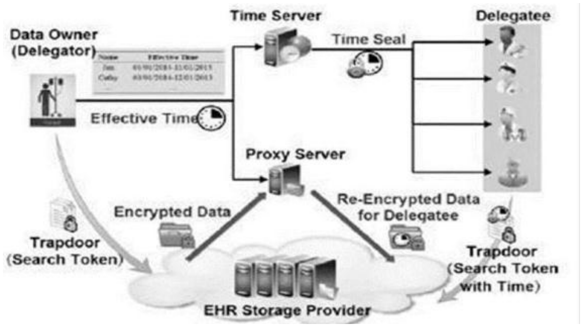

*Fig 4 Architecture Diagram*

In the Figure it explains about the time which has been provided to each of the users in order to access the data that is present in the cloud. The data owner will send the list of times that has been provided to the users to the time server and also it will send to the proxy server. Once after the time server will receive the list, it will allot the time for each of the delegatees or the users. So if the user wants to access the data then he will make use of the key and try to access. The trapdoor will open only if the private key is correct and also the time which has been allotted is correct or not. After verifying only the proxy server will decode the text and the user can view or access the data. In the re-encryption operation, the intermediary or proxy server will typify the powerful time into the re-scrambled ciphertext. With a specific end goal to decrease registering cost, the Proxy server won't re-scramble the ciphertext until they are gotten to, which is alleged apathetic re-encryption component..In the query stage, the data owner can do direct normal search operations with his own particular private key. The delegatee needs to create a keywords trapdoor with the help of the time period. The cloud data server will not give back the matched documents until the viable period represented in the time that agrees with the time period in the re- encrypted ciphertext, it is not the equal as conventional proxy re-encryption searchable encryption tactics. Risk Model: The data owner server in Electronic health record is viewed as semi-trusted, that is straightforward to test information for the benefit of users yet intrusive to detect out the private information of the delegator. Then malicious external attacker could eavesdrop in and dissect the data moved out in the open network, for instance, the encoded records and accesses. He expects to induce security to information as per these data. Furthermore, the refused users may challenge to get through the information past the assigned time using the private keys. As a large portion of size and pursuit effort are ended by the data server, where it accepts that the data server won't conspire with the malicious external aggressor or denied users.

## VIII. ALGORITHM

AES algorithm is used to encrypt the key and the electronic health care records.
AES algorithm AES algorithm uses the concept of both substitution and permutation.

It uses the block size of 128 bit. And the key sizes of 128,192,256 bits. For 128 bit key size we have 10 rounds of repetition, for 192 bit key size we have 12 rounds of repetition and for 256 bit key size we have 14 rounds of repetition.

Each round consists of 4 steps based on key size AES For encryption four steps are follows,
(i) Substitute bytes
(ii) Shift rows
(iii) Mix columns
(iv)Add round key.

Step 1:
Substitution of bytes The 16-byte inputs are substituted in order to form a resultant matrix of four rows and four columns

Step 2:
Shift rows Shifting the rows consists of 4 steps,

(i) Not shifting the first row,
(ii) Circular shift of second row
(iii) Circular shift of third row with two bytes to the left
(iv) Circular shift of fourth row with three bytes to the left.

Step 3:
Mix columns Invertible linear transformation is used to combine four bytes in a column. A set of completely new 16-byte input is formed. e). Step 4: Add round key In this step the 16-byte input is transformed into 128 bit and then they are XORed with a round key of 128-byte. And the output produced is a cipher text and similarly the rounds are repeated based on the key size.

## IX. SYSTEM GOALS

1) This project is designed in such a way that authorized person can access the data. So for this we are designing searchable encryption scheme means in the encrypted content we are performing the search operations with multiple keywords.
2) The other objective is to provide different time for different delegates from the dataowner.
3) The keywords that are provided by the dataowner will be encrypted and will perform the search operation. This is done because the hackers cannot guess the keyword. In this case we are preventing the keyword guess attacks.

## X. LITERATURE SURVEY

The following works are carried out previously in the area of data storage in the cloud.

**1. AUTHORS:** Leventhal, Schwartz, Cummins Martin, and Tierney. All the records that are related to health have increased rapidly and business payments will inspire their use. When some of the principles of Fair information practices are applied to electronic health record then the patients privileges have to keep track of all the private information with the suppliers information that need to be delivered safely and good quality of care should be taken. We have defined the practical and structural contest that have been faced during the patient’s likings for the patients’ health record access and it applies for the present electronic health record. We would provide a system where it could contain the list of all the clinics which are provided and also the list of individuals like doctors, nurse etc,that are participating. We then can change the present information seeing the software which will serve as the exchange for the health information. And in the towns of the clinics the patients’ health record can be provided [3]. Keyword Exploration with Public Key Encoding.

**2. AUTHORS:** Boneh, Ostrovsky, Crescenzo and Persiano
In this the data that has been encoded can be searched by using the public key. Consider an example where one of the user John who will send an email to Alica where the data has been encoded using Alica public key. Here the email access wants to know that the email will have keyword “knowledge” in it so that it can find the route easily.Here Alica will not give any kind of access to the data in order to decode all the messages in it.So here we are going to define and build a appliance in which the Alica will provide a key in order to know whether the keyword “knowledge” is present or not. So this appliance is Public key encoded with the keyword search. Other example, let us consider a server which will store all the messages for Alica .Here Alica can send a key to the server where it can recognize message that will have that keyword. So, the main idea is to encode the data using the public key concept.[4] Open key Encryption Plans Supporting Correspondence Test with Authorization of Various Granulity.

**3. AUTHORS:** Tang The public key encoding is extended by auxiliary fine-grained authorization (FG- PKEET).In the first case we need to spot some of the faults and also the future cryptosystem has to be extended for the equality test.In the second case there are some of the evaluation between FG-PKEET and other alike primitives such as AoNPKEET and PKEET and prove their changes in difficulty and also gain security.In the third case to moderate the intrinsic disconnected the message to rescue from the attackers. We perform twice proxy setting in which both the proxy should perform equality test. Here we have proposed cryptosystem with the two proxy setting.[5]

## CONCLUSION

1] In this paper we have successfully proposed a scheme for timer enabled, privacy preserving keyword search mechanism for EHR cloud storage.
2] In the proposed system there is no time limitation for the data owner.
3] Until now, this is the first searchable encryption scheme with timing enabled proxy re-encryption function and a designated tester.

## REFERENCES

[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] J. W. Byun and D. H. Lee, “On a security model of conjunctive keywordsearch over encrypted relational database,” J. Syst. Softw., vol. 84, no. 8,pp. 1364–1372, 2011.
[4] M. Ding, F. Gao, Z. Jin, and H. Zhang, “An efficient public keyencryption with conjunctive keyword search scheme based on pairings,”in Proc. 3rd IEEE Int. Conf. Netw. Infrastruct. Digit. Content (IC-NIDC),Beijing, China, Sep. 2012, pp. 526–530.
[5]J. Baek, R. Safavi-Naini, and W. Susilo, “Public key encryption withkeyword search revisited,” in Proc. Int. Conf. ICCSA, vol. 5072. Perugia, Italy, Jun./Jul. 2008, pp. 1249–1259.
[6]C. Hu and P. Liu, “An enhanced searchable public key encryptionscheme with a designated tester and its extensions,” J. Comput., vol. 7, no. 3, pp. 716–723, 2012.

**Authors Profile**

Mrs.Sushma S.A pursued her B.Tech in ISE in Siddaganga Institute of Technology. She pursued her M.Tech in CSe in BVB College of Engineering,Hubli..She is currently working as Asst.Professor in Department of ISE in Siddaganga Institute of Technology, Tumakuru. She has 3 years of teaching experience and 1 year of industrial experience. She has published 3 research papers in national and international conference. Her domain of interest is Speech Processing, Big Data, Artificial Intelligience and Deep Learning.