Conjunctive Keyword Search With Designated Tester And Timing Enabled Proxy Re-Encryption Function For E-Health Clouds

Prasad Kumbhar[1], Rohit Bhujbal[2], Sopan Bargaje[3], Aditya Divekar[4], Pankaj Phadtare[5]
[1, 2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Trinity College Of Engineering And Research ,Pune, Maharashtra, India

Abstract- *An electronic health (e-health) record system is a novel 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 hinder 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 novel cryptographic primitive named as conjunctive keyword search with designated tester and timing enabled proxy reencryption function (Re-dtPECK), which is a kind of a time- dependent SE scheme. It could enable patients to delegate 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 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- Searchable encryption, time control, conjunctive keywords, designated tester, e- health, resist offline keyword guessing attack.

I. INTRODUCTION

THE ELECTRONIC heath records (EHR) system will make medical records to be computerized with the ability to prevent medical errors [1]. It will facilitate a patient to create his own health information in one hospital and manage or share the information with others in other hospitals. Many practical patient-centric EHR systems have been implemented such as Microsoft Health Vault [2] and Google Health [3].Given the ambitious prospect to deploy the EHR system ubiq- uitously, privacy concerns of the patients come up. Healthcare data collected in a data center may contain private information and vulnerable to potential leakage and disclosure to the individuals or companies who may make profits from them.Even though the service provider can convince the patients to believe that the privacy information will be safekeeping, the EHR could be exposed if the server is intruded or an inside staff misbehaves. The serious privacy and security concerns are the overriding obstacle that stands in the way of wide adoption of the systems. Public key encryption scheme with keyword search 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 delegatee, who can be his doctor, without revealing his own private key. The proxy re-encryption (PRE) method can be introduced to fulfill the requirement. The server could convert the encrypted index of the patient into a re-encrypted form which can be searched by the delegatee. 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. 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. In the traditional time-release system , [30], 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. 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 instance . 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 key-words 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. 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 re- encryption function (Re-dtPECK) is proposed, which has the following merits.

1) We design a novel searchable encryption scheme sup-porting 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.

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

3) The proposed scheme is formally proved secure against chosen-keyword chosen-time attack. Furthermore, off- line 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.

4) 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.

II. LITERATURE SURVEY

1) Designing a system for patients controlling providers

AUTHORS: J. C. Leventhal, J. A. Cummins, P. H. Schwartz, D. K. Martin, and W. M. Tierney

BACKGROUND:

Electronic health records (EHRs) are proliferating, and financial incentives encourage 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.

METHODS:

We established an online system for capturing patients' preferences for who could view their EHRs (listing all participating clinic providers individually and categorically-physicians, nurses, other staff) and what data to redact (none, all, or by specific categories of sensitive data or patient age). We then modified existing data-viewing software serving a state-wide health information exchange and a large urban health system and its primary care clinics to allow patients' preferences to guide data displays to providers.

2) Public key encryption with keyword search

AUTHORS: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano

We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as *Public Key Encryption with keyword Search*. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

3) Public key encryption schemes supporting equality test with authorisation of different granularity

AUTHORS: Q. Tang

In this paper, we extend the work about public key encryption schemes supporting fine- grained authorisation (FG-PKEET), done by Tang (2011b). First of all, we correct some flaws in Tang (2011b) and discuss how to extend the proposed cryptosystem to support approximate equality test. Secondly, we present a comparison between FG-PKEET and other similar primitives including AoN- PKEET by Tang (2011a) and PKEET by Yang et al. (2010), and demonstrate their differences in complexity and achieved security. Thirdly, to mitigate the inherent offline message recovery attacks, we extend FG-PKEET to a two-proxy setting, where two proxies need to collaborate in order to perform an equality test. Finally, we propose a cryptosystem and prove its security in the two-proxy setting.

4) Efficient verifiable public key encryption with keyword search based on KP-ABE
AUTHORS: P. Liu, J. Wang, H. Ma, and H.Nie

As a very attractive cryptographic primitive, the public key encryption with keyword search (PEKS) enables users to search on encrypted data, and hence is applicable to the setting of cloud computing. Although the existing PEKS schems can allow a user to search encrypted data confidentially, most of them failed to verify the searched result and the system did not specify the users who can make a request for encrypted data files stored on the cloud server. Recently, a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS) was proposed by Zheng. It allows a data user, whose credentials satisfy the data owner's access control policy, to search the encrypted data file and verify the searched result. However, the scheme exists an unrealistic assumption of secure channel as in the Boneh's scheme. In this paper, we propose a new scheme which "removes secure channel" and construct a novel method for verifying the searched result from the cloud server based on key policy attribute-based keyword search (KP-ABKS) of VABKS. It can be effectively to verify the correctness and integrity of the data file which the data user desired for. By our simulation for the verification, it proves that our scheme is more practical than VABKS.

5) Public key encryption with keyword search secure against keyword guessing attacks without random oracle
AUTHORS: L. Fang, W. Susilo, C. Ge, and J. Wang

The notion of public key encryption with keyword search (PEKS) was put forth by Boneh et al. to enable a server to search from a collection of encrypted emails given a "trapdoor" (*i.e.,* an encrypted keyword) provided by the receiver. The nice property in this scheme allows the server to search for a keyword, given the trapdoor. Hence, the verifier can merely use an untrusted server, which makes this notion very practical. Following Boneh et al.'s work, there have been subsequent works that have been proposed to enhance this notion. Two important notions include the so- called *keyword guessing attack* and *secure channel free,* proposed by Byun et al. and Baek et al., respectively. The former realizes the fact that in practice, the space of the keywords used is very limited, while the latter considers the removal of secure channel between the receiver and the server to make PEKS practical. Unfortunately, the existing construction of PEKS secure against keyword guessing attack is only secure under the random oracle model, which does not reflect its security in the real world. Furthermore, there is no complete definition that captures secure channel free PEKS schemes that are secure against chosen keyword attack, chosen ciphertext attack, and against keyword guessing attacks, even though these notions seem to be the most practical application of PEKS primitives. In this paper, we make the following contributions. First, we define the strongest model of PEKS which is secure channel free and secure against chosen keyword attack, chosen ciphertext attack, and keyword guessing attack. In particular, we present two important security notions namely IND-SCF-CKCA and IND-KGA. The former is to capture an inside adversary, while the latter is to capture an outside adversary. Intuitively, it should be clear that IND-SCF- CKCA captures a more stringent attack compared to IND-KGA. Second, we present a secure channel free PEKS scheme secure without random oracle under the well known assumptions, namely DLP, DBDH, SXDH and truncated *q*-ABDHE assumption. Our contributions fill the gap in the literature and hence, making the notion of PEKS very practical. We shall highlight that our scheme is IND-SCF-CKCA secure.

III. METHODOLOGY

EXISTING SYSTEM:

- Proxy re-encryption (PRE) enables a proxy with a re-encryption key to convert a ciphertext 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 ciphertext while the hidden keywords are unknown to the proxy.
- Later, Wang *et al.* has suggested animproved 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.

DISADVANTAGES OF EXISTING SYSTEM:

- Existing systems have high communication or computation cost.
- 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.
- 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.

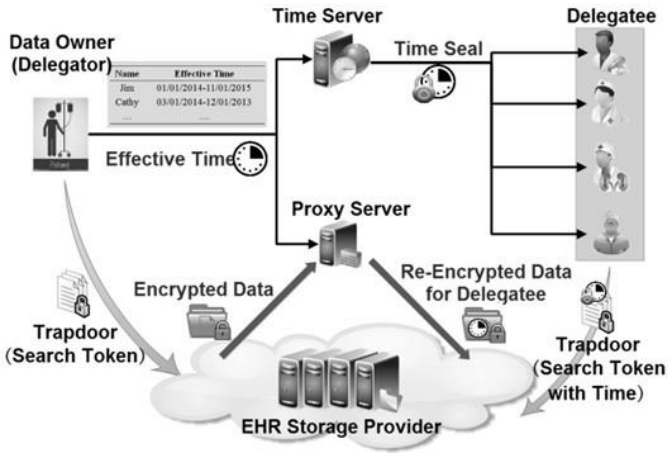
PROPOSED SYSTEM:

- 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 cipher text. 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 cipher text, 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.

ADVANTAGES OF PROPOSED SYSTEM:

- 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.
- 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 delegatee.
- 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.
- 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.

IV. SYSTEM ARCHITECTURE



V. MODULES

- Delegator owner Module
- Delegate Module
- Conjunctive keywords
- Proxy re-encryption
- Time Seal Server

MODULES DESCRIPTION :-

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 ciphertext encrypted by delegator's public key into another form, which can be searched by the delegatee using his own private key.

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 *TrapdoorR* algorithm. If the time information hidden in the re-encrypted ciphertext is inconsistent with that in the delegation trapdoor, the equation in *TestR* 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.

Conjunctive keywords search:

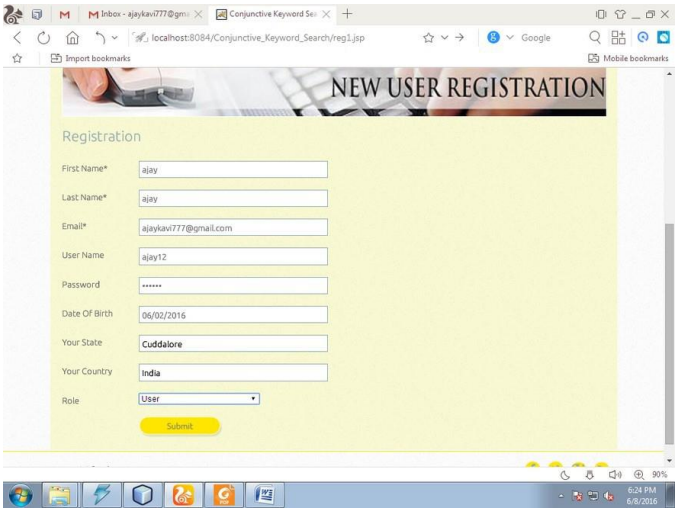
Compared with the single keyword search, the conjunctive keyword search function provides the users more convenience to return the accurate results that fulfills users' multiple requirements. The users do not have to query an individual keyword and rely on an intersection calculation to obtain what they 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.

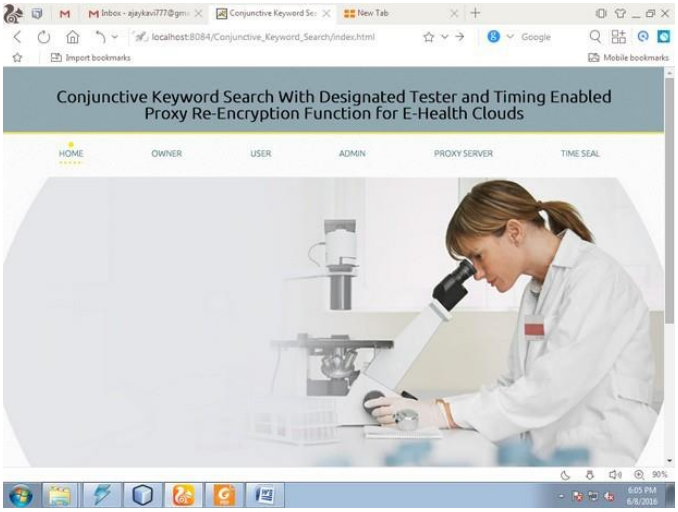
Proxy re-encryption:

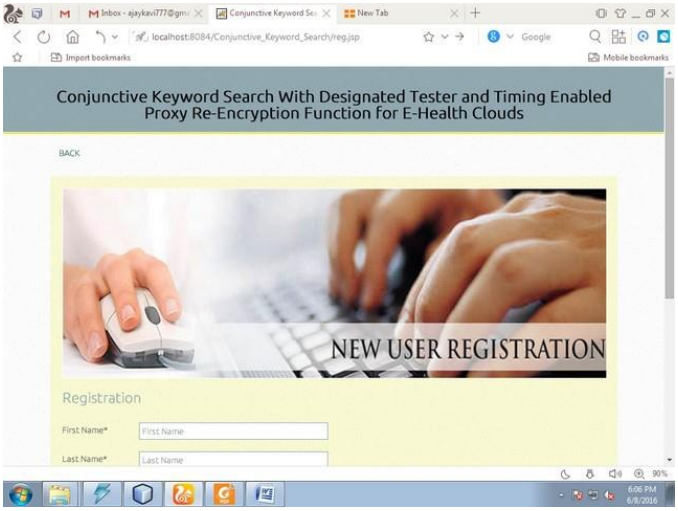
The proxy re-encryption technology is practical in EHR systems. It will greatly facilitate patient delegating the search and access rights. Schemes in could not provide the proxy re-encryption searchable encryption function to the users.

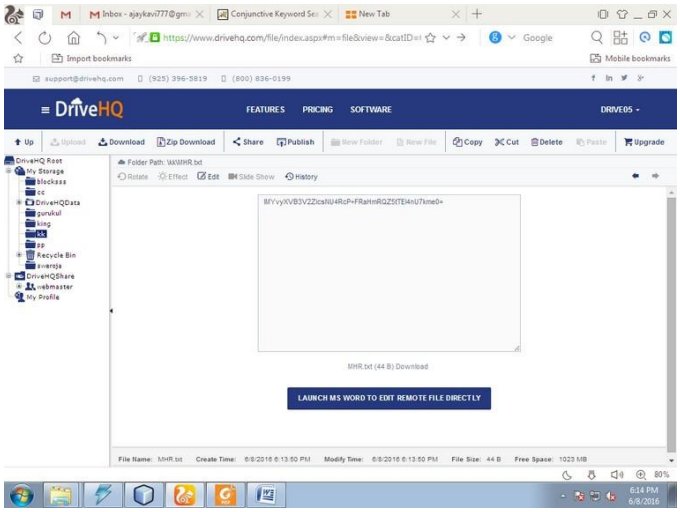
Time controlled revocation:

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.









SOFTWARE REQUIREMENT:

- Operating system: Windows 7.
- Coding Language: JAVA/J2EE
- Tool :Netbeans 7.2.1
- **Database: MYSQL**

VI. CONCLUSION

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.

VII. FUTURE SCOPE

The output which has been shown in figure is currently a web Prototype, but our future work would be building an application where the users can use it as app and change the whole system over the globe.

REFERENCES

[1] 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.**