International Innovative Research Journal of Engineering and Technology

ISSN NO: 2456-1983

International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

E-Health Function For Cloud Using Tester And Timing Proxy

A.Deepika[1],S.Hemalatha[2],S. Premsathya[3],S.Vinodhini[4]
[1,2,3,4]U.G Scholar,Mrk Institute Of Technology

Guide, Mr.T.PERIYASAMMY. M.E.,

Assistant Professor Dept. Of Computer Science MRK INSTITUTE OF TECHNOLOGY – Kattumannar Koil

[1]deepikatamilselvi@gmail.com,[2]hemaoct20@gmail.com,[3]premsathyabecse@gmail.com,[4]vinobecse754@gmail.com

Abstract:

Project proposes a new initiate to enhance the existing Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds with a new feature of extension to solve the data security problem while access the sensitive data by the user. The attackers know the date when the user accesses the data. So attackers easily trying to access the data. We now introduce the new way of data accessing process. If when the user wants data from cloud storage the user gives the request to the Time Seal Server (TS). And then it verifies the user authentication. Then it allows the user to access the data in a particular time session. File accessing process is over then the session is over .file transfer time is very short time so attackers can't the users file and also user gives request any time so it's very complicated for the attackers to access the user data illegally.

Index Terms— Searchable encryption, time control, conjunctive keywords, designated tester, e-health, resist offline keyword guessing attack.

I. INTRODUCTION

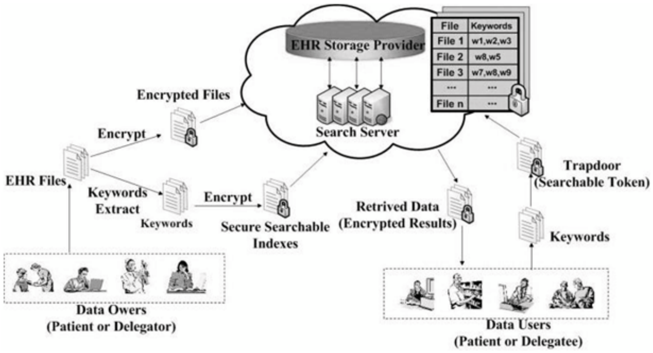
The electronic heath records (EHR) system will make medical records to be computerized with the ability to prevent medical errors. It will facilitate a patient to create his own health information in one hospital and manage or share the information with others in other hospitals. Many practical patient-centric EHR systems have been implemented such as Microsoft Health Vault and Google Health . 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 delegator to delegate his search right to a delegatee, who can be his doctor, without revealing his own private key. cost. It will be more troublesome to 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.

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 (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 .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.

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 amechanism proposed to automatically revoke the delegation right after a period of time designated by the data owner previously. In the traditional time-release system [28], [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 .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.

Various constructions of public key encryption with conjunctive keyword search (PECK) over encrypted data have been proposed [8]–[10]. It allows the users to query multiple keywords at the same time [11], [12]. However, some of them such as the solution in [9] and [10] have high communication or computation cost. On the other hand, some schemes such as the solutions in [8] and [12] require an index list of the queried keywords when a trapdoor is generated, which will leak information and impair the query privacy.



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.

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.

- 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.

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

The test algorithm could not function without data server’s Eavesdroppers could not succeed in guessing keywords by the test algorithm.

The security of the scheme works based on standard model rather than random oracle model. This delegator’s public key into those that can be decrypted by del- egatee’s private key. Proxy re-encryption with public keyword search (Re-PEKS) has introduced the notion of key- word search into PRE. The users with a keyword trapdoor can search the ciphertext while the hidden keywords are unknown to the proxy. The limitation on the schemes is that only one keyword will be allowed to search in the encrypted documents. 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, it is shown in that a proof in random oracle model may probably bring about insecure schemes.

The time controlled PRE has been addressed . It desires to encrypt a message for multiple recipients with the same release time. However, the schemes in foist the data owner to determine the release time at the beginning of encryption algorithm. Only one release time is set for all recipients rather than disparate time for different users, which could not fulfill the need for uniqueness. Another shortcoming is that it needs a large computation cost in both encryption and re-encryption phases .

Usually selected from a small space, especially the med- ical 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. Byun *et al.* and Yau *et al.* have broken several classical schemes by the KG attacks.

In order to resist the threats, the concept of PEKS with designated tester (dPEKS) . Only a designated tester, which three types of entities: an information owner, users and a 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

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. , 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,

It indicates that the delegatee Jim is authorized to issue queries and perform decryption operations on the encrypted data of the data owner. 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-encrypt the ciphertext until they are accessed, which is so called lazy re-encryption mechanism [20]. 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, which is different from traditional proxy re-encryption SE schemes.

B. Threat Model

The EHR data server is deemed as semi-trusted, who is honest to search information for the benefits of users but curious to spy out the private information of the patients. On the other hand, malicious outside attacker could eavesdrop and analyze the information transferred in public channel, such as the encrypted indexes and trapdoors. He intends to infer privacy information according to these data. Furthermore, the revoked delegatees may try to access data beyond the designated time period using their private keys. As most of the storage and search work are completed by the data server, it is assumed that the data server will not collude with the malicious outside attacker or revoked delegatees.

C. Design Goals

Our Re-dtPECK scheme for EHR cloud is designed to achieve the following goals.

• ***Authority delegation***. The proposed SE scheme
allow data-owner-enforced authority delegation, i.e.
data owner could delegate his search right to other users without revealing his private key.

• ***Time controlled revocation***. An important design goal
is to enable time controlled access right revocation.
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.

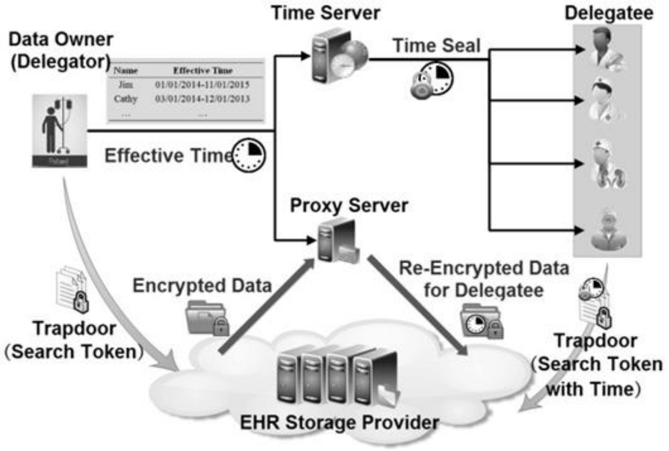
• ***Diverse delegation times for different users***.
challenge of the system is to achieve owner-defineddisparate access time periods for different delegatees. The data owner himself will not be constrained by the time.

• ***Security goals***. The privacy concerns of this secure search system are summarized as follows. *keyword*

semantic security: as a Re-dtPECK scheme is proposed, we will prove it indistinguishable against chosen key- words chosen time attack (IND-CKCTA). *resist KG attacks*: since the EHR keywords are always chosen from a small space, the related searchable encryption schemes maybe vulnerable to offline KG attacks. The proposed scheme should resist such attack.) *standard model*: it is well known that security proved in standard model is stronger than that in random oracle model. This security property guarantees a higher security level. In this subsection, we formally define the conjunctive keyword search with a designated tester and the timing enabled proxy re-encryption function (Re-dtPECK). Then, we describe a concrete Re-dtPECK scheme with a detailed workflow and derive the correctness of the scheme.

Standard model rather than random oracle model. This 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 key- word search into PRE. The users with a keyword trapdoor can search the ciphertext while the hidden keywords are unknown to the proxy. The limitation on the schemes is that only one keyword will be allowed to search in the encrypted documents. 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, it is shown in that a proof in random oracle model may probably bring about insecure schemes.

we endeavor to solve the problem with amechanism proposed to automatically revoke the delegation right after a period of time designated by the data owner previously. In the traditional time-release system [28], [30], the time seal is encapsulated in the ciertext 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 .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.



or computation cost. On the other hand, some schemes such as the solutions in [8] and [12] require an index list of the queried keywords when a trapdoor is generated, which

Various constructions of public key encryption with conjunctive keyword search (PECK) over encrypted data have been proposed [8]–[10]. It allows the users to query multiple keywords at the same time [11], [12]. However, some of them such as the solution in [9] and [10] have high communication

will leak information and impair the query privacy. seal S_T 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 S_T . 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 S_T . 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.

II. 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 EHR 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.

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] 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] Q. Tang, "Public key encryption schemes supporting equality test with authorisation of different granularity," *Int. J. Appl. Cryptogr.*, vol. 2, no. 4, pp. 304–321, 2012.

[6] P. Liu, J. Wang, H. Ma, and H. Nie, "Efficient verifiable public key encryption with keyword search based on KP-ABE," in *Proc. IEEE 9th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Nov. 2014, pp. 584–589.

[7] 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.

[8] 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.

[9] 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.

[10] 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

[11] J. W. Byun and D. H. Lee, "On a security model of conjunctive keyword search over encrypted relational database," *J. Syst. Softw.*, vol. 84, no. 8, pp. 1364–1372

[12] M. Ding, F. Gao, Z. Jin, and H. Zhang.