CONJUNCTIVE WATCHWORD SEARCH WITH ASSIGNED TESTER AND TIMING ENABLED PROXY RE-ENCRYPTION FUNCTION FOR E-HEALTH CLOUDS

B.Lakshmi Bhavani[1], K.Sreehari[2]

[1]*Student, Computer Science and Engineering Department, Prakasam Engineering College, Andhra Pradesh, India,* ***lakshmibhaskruni@gmail.com***

[2]*Asociate Professor, Computer Science and Engineering Department, Prakasam Engineering College, Andhra Pradesh, India,* ***kancharla.sreehari@gmail.com***

Abstract

An application has been developed for the incredible accommodation in the health care. Here the protection and safety of the personal information of the users are the major issue. So here we have introduced a multiple keyword search in order to access the data that is present in the cloud by the delegatees. 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. The patient or the delegator will give the rights to access the data to the users by providing a particular time period in order to access the data. The time has been enabled for the users and data can be accessed. It can likewise bolster the conjunctive catchphrases inquiry and oppose the watchword speculating assaults the keywords that are provided by the data owner 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. This will provide hundred percent security to store the patients' health record in the cloud than the oracle model. 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.

Index Terms: *Searchable encryption, time control, Cloud, Health care, Keyword, Proxy, Delegates*

---------- *** ----------

1. INTRODUCTION

Data encoding is the translation of information into a casing that is confused deprived of an understanding segment. A secret key is a riddle word or expression that gives a specific customer to access the data. There should be some precautions taken in order to protect our work, if there are no basic steps taken to prevent then the information will be at a high risk. There are chances where we can compromise the operations on different computers, or even the working of the organization in all.

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 frameworksblow up the App downloads,

evaluations and surveys in a short time.

A. PROBLEM STATEMENT

the attackers can guess the keyword and guessing of keywords are launched, if the attackers identify the possible applicant keywords then the information is leaked and impair the query privacy. Efficient revocable access control of our data is not possible in existing mechanism. In this case adversary are the attackers who are attacking what keywords we have given with the same keyword only they are going to perform the search operations. So the Keyword which the data owner generates will be stored in the cloud. So to prevent this problem we have provided a particular time for each of the users or the delegates who wants to access the patient's record in the cloud. Once if the keyword is known to the attackers then it's very difficult to prevent the patient's record that has been stored in the cloud. So in order to prevent this only this project has been implemented.

B. OBJECTIVES

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 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.
4) This will provide hundred percent security to store the patients' health record in the cloud than the oracle model.

C. EXPECTED OUTCOMES

File and keywords are successfully encrypted and stored and automatic revocation for the files based on time server from users. The patient will store all his health record in the cloud for the further access when required by the delegates and access is not provided by all only some of the delegates can access the data based on the time period that has been provided. So once the data is uploaded in to the cloud then a keyword has been generated by the dataowner and it has to be encrypted because the hackers may hack the keywords. Once the keyword is known then its very easy for the attackers to do the search operation in the cloud. So it has been encrypted and then later stored in the cloud. Then suppose if the user wants to use the encrypted information which is stored in the server, then the proxy server will decrypt the data only when the keyword and the time provided by the user are correct and then the trapdoor open and the user can access the decrypted data in the cloud.

D. PROBLEM FORMULATION

In Fig. 1, the environment of the proposed Re-dtPECK scheme for the EHR cloud system is presented. There are 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 center.

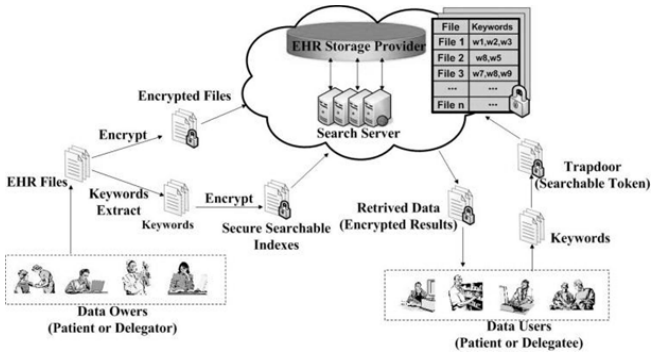

Fig. 1. System Model.

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.

In Fig. 2, the timing enabled proxy re-encryption searchable encryption model is shown.

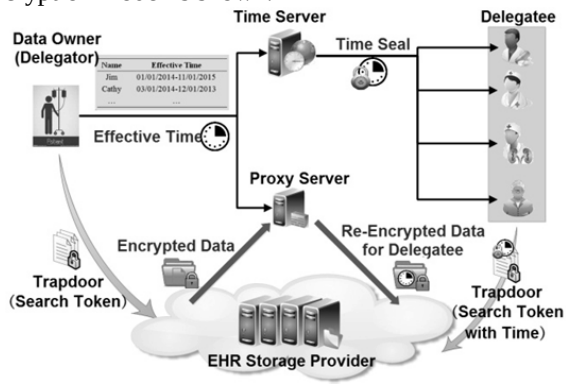

Fig. 2. Timing Enabled Proxy Re-encryption Searchable Encryption Model

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 encapsu- late 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. 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.

Design Goals

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

- *1)* ***Authority delegation***. The proposed SE scheme should allow data-owner-enforced authority delegation, i.e. the data owner could delegate his search right to other users without revealing his private key.
- *2)* ***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.
- *3)* ***Diverse delegation times for different users***. Another challenge of the system is to achieve owner-defined disparate access time periods for different delegatees. The data owner himself will not be constrained by the time.
- *4)* ***Security goals***. The privacy concerns of this secure search system are summarized as follows. 1) *keyword semantic security*: as a Re-dtPECK scheme is proposed, we will prove it indistinguishable against chosen keywords chosen time attack (IND-CKCTA). 2) *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. 3) *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.

Security

In this section, the proposed solution is proved IND-CKCTA and IND-KGA (indistinguishable against keyword guessing attack).

- ***Confidentiality***: The notion of confidentiality of the EHR in this paper means that the private documents of users must be kept secret from both unauthorized system visi-tors and the EHR cloud service provider. By this scheme, the health information is protected by means of a strong encryption primitive. The indexes of the conjunctive key- words are encrypted by the dPECK or Re-dtPECK algo- rithms before uploaded to the cloud server. The service provider could not recover the plaintext of the encrypted data. The keyword extraction from EHR is controlled by the patient and encrypted locally with patient R_i 's own secret key. The ciphertext can be derived with R_i 's private key sk_{Ri} . However, the server could not get any information about the patients' private keys for generating trapdoors and decrypting the protected documents.

RELATED WORK

A. Conjunctive Keyword Search

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

B. 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 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.

Only a designated tester, which is usually the server, is capable to carry on the test algorithm. The enhanced security models have also been put forward. However, they could not support multiple keywords query or delegate search function.

C. Proxy Re-Encryption With Public Keyword Search

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 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 in 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 in are proved secure in random oracle model. Nevertheless, it is shown 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 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.

D. Workflow of Re-dtPECK

There are six elements to take an interest in the cloud including a trusted third party (TTP). For example, the Veterans Health Administration (VHA) is accepted to function as a TTP, who is trusted by facilities, clinics, patients and specialists. A delegator should be John, who is an endless heart disappointment quiet.

The EHR documents of John are put away on a data server in the cloud in a secured shape. John went to Hospital A for the cardiovascular treatment since Feb. first, 2017. He desires to assign the cardiologist Dr. Donny from Hospital A to be his delegatee for advantageous EHR information get to it. Since John arrangements to exchange to Hospital B after June first and he trusts that Dr. Donny is not ready to request his EHR after that time. At that point, Dr. Donny is agreed a period forced specialist to get to the ensured security data (PHI) of the patient John. The time server (TS) will create a period seal for Dr. Donny to guarantee that he can access to Johns PHI within the time of Feb. first May, 30st, 2017. The proxy server (PS) is capable to encode John's PHI to a re-scrambled frame so that Dr. Donny can look on those records with his own particular private key.

The Re-dtPECK framework can be partitioned into three stages.

In stage 1, the TTP instates the framework by executing GlobalSetup calculation and produces the global parameters, which are spread to delegator John, delegatee Dr. Donny, the EHR cloud server, the PS and the TS. The TTP additionally produces sets of private and public key for John, Dr. Donny, the cloud server and the TS by running KeyGenRec, KeyGenSer ,KeyGenT S calculations.

In stage 2, EHR records are delivered within John's helpful procedure. The encoded EHR records and reports will be produced utilizing the dPECK calculation and put away at the cloud data server. As the medical information gathered, John may expect to seek on his encoded EHR records. He utilizes a keyword set Q to depict the health record document that he needs to discover. At that point, he runs Trapdoor calculation to create a trapdoor for keyword set Q and sends the trapdoor to cloud server. In the wake of accepting the inquiry query, the cloud server runs test calculation with the cloud server's private key and returns every one of the documents that contain Q. On the off chance that the assignment marker θ equivalents to 1, stage 3 will be executed. John sends an task notice to the TTP, PS, TS,delegatee and data server together with a mark marked by John. The successful designation time of PHI get to appointment for delegatee is indicated. It implies that the patient John has appointed the get to rights to Dr. Donny. The beneficiaries will check the mark utilizing public key of John. In this framework, the mark calculation won't be indicated. In any case, there is a prerequisite on the calculation that the mark plan ought to be clearly unforgeable. The notice will be rejected if the mark comes up short the check. In the event that it is checked valid, the TTP runs ReKeyGen calculation to produce a reencryption key and send it to the PS covertly.

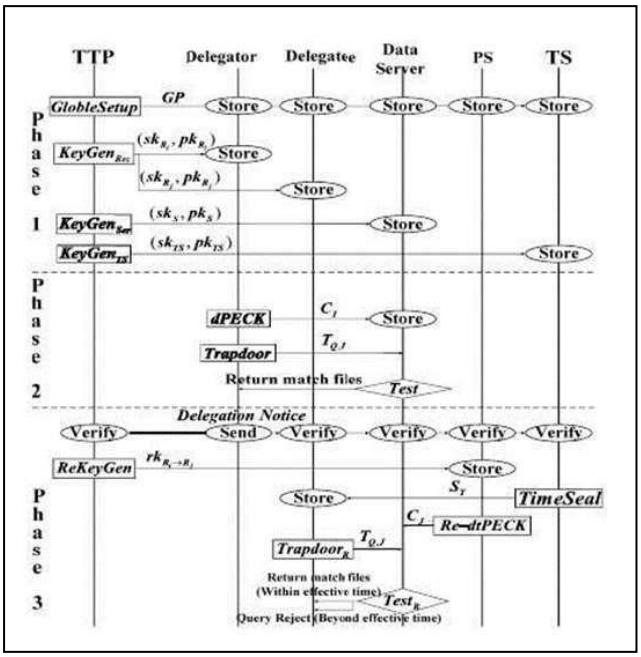

Fig. 3: Workflow of Re-dtPECK

CONCLUSION AND FUTURE WORKS

This project provides a security to the healthcare records of the patients that are stored in the cloud. This application can be very useful during the emergency cases where the previous health record of the patient is required. For each of the authorized users has been enabled with Proxy re-encryption function in E-health cloud in order to prevent the misuse of data by the attackers.

With the help of random multiple keywords the search operation can be performed to access the data and proxy server will help to decrypt the encrypted data if the user has the valid time period provided.

Further this application can be used for many authorized user in future. And some additional versions of the application can be added and used. The storage of the data is secure and widely used in the health care applications.

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. 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.
[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] 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.
[9] 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.
[10] 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.
[11] 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.
[12] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester," Int. J. Comput. Math., vol. 90, no. 12, pp. 2581–2587, 2013.
[13] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," J. Syst. Softw., vol. 83, no. 5, pp. 763–771, 2010.
[14] C. Hu and P. Liu, "A secure searchable public key encryption scheme with a designated tester against keyword guessing attacks and its extension," in Proc. Int. Conf. Adv. Comput. Sci., Environ., Ecoinform., Edu. (CSEE), vol. 512. Wuhan, China, Aug. 2011, pp. 131–136.
[15] C. Hu and P. Liu, "An enhanced searchable public key encryption scheme with a designated tester and its extensions," J. Comput., vol. 7, no. 3, pp. 716–723, 2012.
[16] 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.
[17] 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.
[18] M. Bellare, A. Boldyreva, and A. Palacio, "A uninstantiable randomoracle- model scheme for a hybrid-encryption problem," in Proc. Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT), vol. 3027. Interlaken, Switzerland, May 2004, pp. 171–1.