Conjuctive Keyword Search With Timing Enabled Proxy Re-encryption Function for E-health Clouds

[1]Rithika A H, [2]Latha C A

[1]M Tech Scholar, [2]Professor and Head
Department of ISE
AMC College of Engineering, Bangalore, India

Abstract— Electronic health record system is a novel application which will impact a greater facilities in health care. The security and protection of the patient's private information is a major concern that will impact the further development and wider adoption of systems. To enable the privacy, protection and user friendly operation functions both which plays a major role in the e-health record system. In this paper we are initiating a novel cryptographic primitive called conjunctive keyword search with proxy re-encryption function. This encryption scheme is a timing the searchable encryption scheme is incorporated. This encryption scheme is timing based which will allow the users to delegate access rights partially to the third parties to perform search on the users report in a designated period of time which is set by the patient or user. The time period for the delegate can be limited and recode the documents that is encrypted by the user. The delegate will be taken of the accessing right after the time period that is designated by the user. It will also enable the keyword conjunctive search and prevent it from searching through guessing of keywords. For the proposed proxy re-encryption scheme a security and a system model is formulated to prove that the scheme is efficient. We have conducted a demonstration in which the comparison and simulations is found to have low computation and storage overhead.

Keywords – searchable encryption, conjunctive keyword search, e-health record system, prevent guessing keyword search

I. INTRODUCTION

The electronic health record system which will bring a greater facility in healthcare is made computerized that is the medical report of the patients are stored in cloud. It will allow the patients to form their own health reports on their own and maintain it in one particular hospital and also to transfer the report details to other health care hospitals. The security and the privacy of the patient's personal health record information are the major concern which could obstruct the further progress and development.

The searchable technique is incorporated which allows the health report of the patient that is stored in the data center will contain all personal information which may be leaked to the other companies who may take a gain from them and may mislead. The service provider can influence the users to trust that their report and their personal information will not be leaked to others and it is been kept safely, but the health record system may have shared if it is intruded or the people within the organization may have shared. Public key encryption scheme along with the keyword search enables the patients to make a search with the information which is already encrypted by the data owner without having to decode it, which will increase the security of the Electronic health record systems. In some cases the patient wants to act as a user to delegate his search authority to a delegate who can be his doctor or any third party without leaking his private key. The proxy re-encryption method is implemented to satisfy the specifications.

The server will change the encrypted information of the patient into a re-encrypted form which makes a way for the delegate to search. The problem arises when the access authority is been shared, when the patient after he gets cured and is discharged or if the patient is shifted to another health care nursing home, the patient may not want his personal information to be searched and make use by already consulted doctors anymore.

A possible method to overcome this problem is to re-encrypt all the data with the new key, which will increase the cost to highest. It will become more inconvenient and trouble to get back the delegation right in an expandable size. In this project the problem is solved by a novel mechanism which is proposed to revoke itself automatically the access right after a duration of time which is allotted by the data owner previously.

II. RELATED WORK

A. Conjunctive keyword search

Different constructions of public key encryption with conjunctive keyword search over the data that is encrypted have been proposed. It enables the users to query multiple keywords parallel. Some of the solutions have high communication and higher computational cost. On the other side fewer schemes in which the solutions requires a list index of the keywords queried when a trapdoor is generated, which will leak the data and information of the users.

B. Searchable Encryption with Designated Tester

The keyword size is always more than its polynomial level. An intruder is able to launch dictionary attacks or offline search of keywords guessing attacks to corrupt the hidden document keywords. The keywords are normally selected or taken from the reports in medical terminology. If the trapdoor is found by the adversary then is a possibility of guessing the candidates keywords. In order to avoid the attacks and threats the public encryption scheme concept with the designated tester is proposed. The test algorithm is carried out by the designated tester only. The more advanced security models have also been

put forward nut could not support the multiple keywords query search function.

C. Proxy Re-encryption with Public Keyword Search

The proxy Re-encryption converts a cipher text encrypted by a delegator's public key into those that can be decrypted using delegator's private key with re-encryption key. The users can search the cipher text with the keyword trapdoor when the keywords hidden are not known to the proxy server. The limitation on this scheme that only one single keywords is used to search the encrypted document. The time controlled proxy re-encryption is referred, it desires to encrypt the message for the multiple users with same release time. However the scheme enables the data owner to establish the release time at the initial stage of the encryption algorithm. Only single release time is preset for all the recipients to satisfy the requirements for uniqueness. Another issue is need of high computation cost in both the encryption and re-encryption phases.

III. PROPOSED SYSTEM

In this proposed system we solve the problem with a novel method that is proposed to revoke or get back the access rights automatically after the time period that is designated by the user. We design a searchable encryption scheme which will support conjunctive keyword search and approved delegation function. Comparing with the existing systems the time seal was encapsulated in the cipher text at the beginning of the encryption algorithm, this scheme can achieve timing enabled proxy re-encryption with the revocation of delegation right effectively.

Different time period is provided and designated to different delegate. The time server which is used in the system is responsible to generate the time tokens for each users. After receiving an effective time period from the data owner the time server will generate a time seal. By the re-encryption algorithm executed by the server proxy the time period will be embedded in the re-encrypted cipher text. Then the generated trapdoor will be opened to the query request using private key and time seal and cloud will respond if the file is matched. The proposed system is proved safe and secure against selected keyword and selected timing attacks.

System Architecture

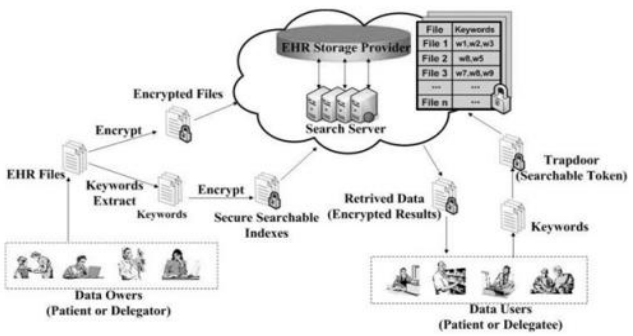

Fig. 1. System Model.

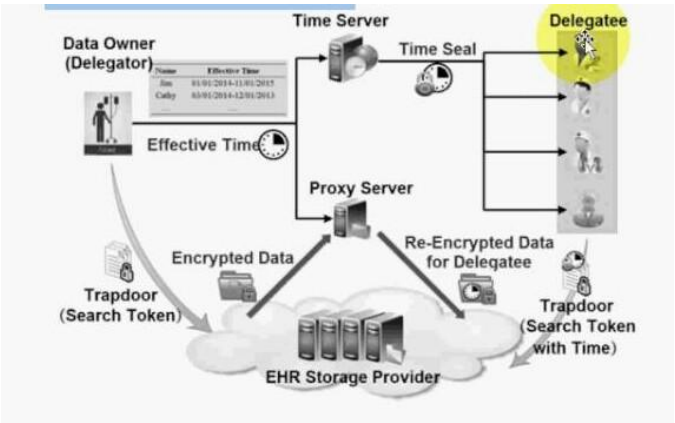

Fig.8. Timing Enabled Proxy Re-encryption

IV. IMPLEMENTATION

The proposed system consists of three main modules 1.Data owner module 2. Data center module and 3. User module.

1) Data owner module

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 cipher text. Then that data are outsourced to the data center.

2) Data center

The data center consists of an EHR storage provider and a search server. The storage provider is responsible for storing the data and search server performs search or add or delete operations according to the request of user.

3) User

A user will generate a trapdoor to search the EHR files using his private key and forwards it to the search servers. After receiving the request the search servers will interact with the EHR storage provider to find the matched files and returns those retrieved information to the user in an encrypted form.

Advantages of Proposed Systems

1) In the proposed system time limitation is not applicable for the data owners the time details is embedded in the re-encryption stage.
2) It provides a trust cloud framework for the accountability and in cloud computing. It will also propose a multi-faceted trust management architecture for cloud computing to help the users of the cloud service to identify trustworthy cloud service providers.

V. CONCLUSIONS

In this paper we have proposed a novel proxy re-encryption 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 and 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. Our simulation results have also shown that the communication and computation overhead of the proposed solution is feasible for any real world application scenarios.

References

[1] J. Leventhal, J. Cummins, P. Schwartz, D. Martin, W. Tierney. "Designing a system for patients controlling providers' access to their electronic health records: organizational and technical challenges," Journal of General Internal Medicine, vol. 30, no. 1, pp. 17-24, 2015.

[2] Microsoft healthvault. http://www.healthvault.com.

[3] GoogleInc.
Googlehealth. https://www.google.com/health.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, Interlaken, Switzerland, May 2-6, 2004, vol. 3027, pp. 506–522, Springer.

[5] Q. Tang, "Public key encryption schemes supporting equality test with authorisation of different granularity," International Journal of Applied Cryptography, vol. 2, no. 4, pp. 304-321, 2012.

[6] P. Liu, J. Wang, H. Ma, H. Nie, "Efficient Verifiable Public Key Encryption with Keyword Search Based on KP-ABE," In Proc. 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), IEEE, pp. 584-589, 2014.

[7] L. Fang, W. Susilo, C. Ge, J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Information Sciences, vol. 238, pp. 221-241, 2013.