Timing Enabled Proxy Re-Encryption Function for E-Health Clouds with Designated Tester Using Conjunctive Keyword Search

Aiman Hasan[1], Dr. Rekha Patil[2]

[1]PG Student, Department of CNE, PDA College of Engineering, Kalaburagi, Karnataka, India.

[2]Professor, Department of CSE, PDA College of Engineering, Kalaburagi, Karnataka, India

ABSTRACT

An "ELECTRONIC HEALTH (E-HEALTH) RECORD SYSTEM" is the new and interesting application that will bring great amenity in healthcare system. Users basically have two major concerns related to their personal information like the privacy and security of the sensitive personal information, which might harm or obstruct further development. The searchable encryption (SE) theory incorporates security protection and favorable operability functions together, which can play an important role in the e-health record system. Our work aims at introducing a kind of a time-dependent SE scheme named Timing Enabled Proxy Re-Encryption Function for E-Health Clouds With Designated Tester Using Conjunctive Keyword Search. Proposed work enables patients to give the authority to others for partially accessing and working on their sensitive personal information for a limited period of time. The length of the time period for the authorized person to search and decrypt the data owner's encrypted documents can be controlled. In addition, the authorized person will be automatically deprived of the access and search authority after the time period expires. Conjunctive keywords search is supported and also and resist the keyword guessing attacks. Only the specified/allotted tester is able to test the existence of certain keywords. Then, system model and a security model for the proposed scheme is designed to show that our work is efficient and it has a no computation and low storage overhead.

Keyword - *Proxy Re-encryption, time control, conjunctive keyword search, designated tester, e-health, resist offline keyword guessing attack.*

1. INTRODUCTION

THE ELECTRONIC heath records (EHR) system will make medical records to be equipped with the capability to surpass medical errors [1]. It provides a special opportunity to a patient to create his own health related information in one hospital. That sensitive personal information can be managed and shared by others in other hospital. Google Health [2] and Microsoft Health Vault [3] are some of the existing practical patient-centric EHR systems.
Given the powerful potential to arrange the EHR system widespread, privacy concerns of the patients come up. Healthcare data present in the data centre includes private information and is also vulnerable to potential leakage. Although the service providers persuades the patients to believe that the private information will be protected, the EHR could be revealed if the server is disturbed or an inside staff behaves improperly.

The concept of "Timing enabled proxy re-encryption function" is to deploy the timing factor to enhance the security models and eliminates the hazards. In comparison with the single keyword search, the conjunctive keyword search function gives the users an amenity to return the accurate results so that users' multiple requirements are fulfilled. This work achieves a timing enabled proxy re-encryption with operative delegation cancellation and is successfully

proved secure against chosen-keyword chosen-time attack. In the classical time-release system lots of your time obstruction is personified in the cipher text at the initiation of the security foundation. It means that all users such as data owner are confined by the time period. The refinement of the proposed system is that there is no deadline for the data owner because the information related to the time period is guarded in the re-encryption phase.
Organization of paper: 1.Introduction, 2.Related work, 3.Proposed Work, 4. Implementation and Results, 5.Conclusion.

2. RELATED WORK

In Timed-Release Proxy Re-Encryption (TR-PRE) concept if the proxy transformation is utilized to a TRE ciphertext, the release time is still active [4]. In [5] a user's access right lapse automatically after a predestined period of time. Searching a record inclusive of multiple encoded keyword without implicating any original information and a new PECK idea based on pairings, where there is no involvement of pairing operations in the encryption and trapdoor phases and a secure channel between server and users is eliminated [6]. In [7] they considered two searchable public key encryption designs with a designated tester and also suggested that they are insecure in contrast to keyword guessing attacks. Second consideration is a bidirectional searchable proxy re-encryption with designated tester. Most designs have just analysed on insider security, on equality of CSI and focuses on the prevention of insider attackers like server manager which is able to obtain keyword information through CSI in the database. Assuring the Security for outsider attackers who are not able to view encrypted records but strive to fetch information on keywords by conquering and customizing protocol messages [8]. The work in [9] presents the first Chosen-Ciphertext Secure anonymous conditional proxy re-encryption with keyword search (C-PRES) idea with the assistance like chosen-ciphertext security; keyword-invisibility; unidirectionality; non-interactivity; and collusion-impedance. In [10] they designed and deployed a practical dynamic symmetric searchable encryption schemes that effortlessly and secretly inquire server-held encrypted databases with large number of record-keyword pairs and also easily support additions and deletions of the data over revocation lists. The work in [11] draws attention for the introduction of CPRES, where the proxy can first approve if a ciphertext holds a described keyword, after which re-encryption of the ciphertext is done with the answering re-encryption key. Defining the enduring paradigm of PEKS that is free from secure channel and is also immune against chosen keyword attack, chosen ciphertext attack, and keyword guessing attack [12].
There are four main contributions of this paper: (1) Supremacy authorization where the data owner can assign his accessible rights to other users without bringing out into open his secret key; (2) Time contained cancellation where in the authorized appointment will expire when the set in advance active period of time contradicts with the ongoing time. The authorized users are stopped from attaining the medical records overtime; (3) Discrete authorization time for distant users which means that the data owner is not confined by the time and is able to set discrete authorization time for variant users; and (4) Security which focuses on the inclination of the confidentiality of the EHR focus on keeping the private documents of the users confidential from both the unauthorized guest and also from the EHR cloud service provider. Also the conducted work offers resistance against offline KG attacks.

3. PROPOSED WORK

This work includes a searchable encryption scheme that supports conjunctive keyword search with an authorized representative function which is owner-imposed work and achieves timing enabled proxy re-encryption with efficient representative cancellation. In this work the data owner is not bound to the time limitation as the information related to time is enclosed in the re-encryption phase. Data owner can preset different access time period for different users followed by a time seal which can increase/decrease the effective time. Furthermore, resistance against offline keyword guessing attacks is supported. Time control feature which offers access to medical records even if the data owner is offline. Dynamic data change that is addition and deletion of encrypted data is the most useful feature.

3.1 System Model

This work mainly focuses on the implementation of the time factor. The data owner broadcast an invoice of authorized active time periods for his data consumers, time server and the proxy server. The listing encloses the

uniqueness of each data consumer and the active time period, such as "Jack, 01/01/2016 – 01/30/2017". It intimates that the data consumer Jack is authorized to grant inquiry and enforce decryption operations on the encrypted data of the data owner from Jan. 1st, 2016 to Jan. 1st, 2017.After acquiring the list, the time server accomplishes a time seal for each data consumer, which is broadcasted respectively. The time seal is a backdoor of an active time period and is covered up by the private key of the time server.

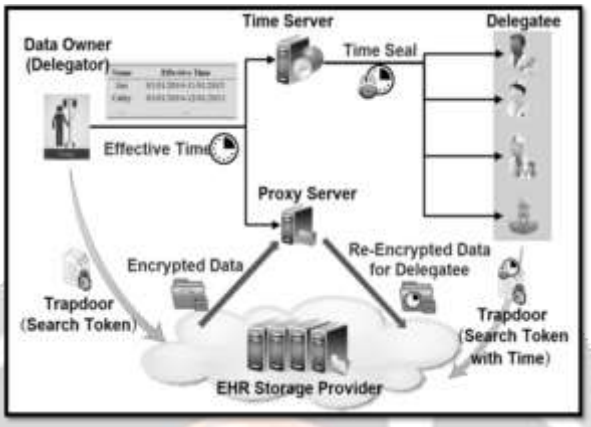

Fig -1: Storage Architecture with Timing Enabled Proxy Re-encryption Model

Later to lower computing rate, the proxy server won't re-encrypt the ciphertext till they are acquired and this mechanism is called lazy re-encryption technique [13]. The cloud data server won't recover the similar records except the active time enclosed in the time seal admits with the time in the re-encrypted ciphertext, which is different as compared with the classical proxy re-encryption SE schemes. The figure above shows the system environment of the proposed concept. EHR Cloud storage incorporates five entities as follows:

3.2. Data Owner

Data owner carries the data and transmit the encrypted data to cloud service provider to store the data in cloud servers. Data owner describes and administer the access theory over users, apply this theory to encrypt the data and then sync them to cloud servers to use in common with the other users.

3.3. Admin

The admin handles all the functions with the assistance of cloud Service Providers (CSPs). CSPs uphold cloud Infrastructures which consist of first an EHR storage provider which stores the data and the second is a search server which performs operations like addition/deletion and searching as per the user's request. Data owners pack enough amount of sensitive data to be stored in EHR storage provider which will be transmitted to all the users. Cloud servers occupy enough storage capacity and computational assets.

3.4. Data Consumer

Data consumers are the bodies who access the encrypted data stored in cloud servers. Only the authorized users who comply with the access theory of data owner can decrypt the encrypted data to retrieve the plaintext data.

3.5. Time Server

A time server is responsible to produce time seal for the users. The time seal is a backdoor of an effective time period and is responsible for distribution, revocation and update attribute keys of users.

3.6. Proxy Server

The role of proxy server is just to re-encrypt the owner uploaded file into the ciphertext and outsource it to the user.Data owner and data consumer communicate via proxy re-encryption server used for retrieving the sensitive data file from EHR storage provider.

This owner-imposed work achieves timing enabled proxy re-encryption with efficient representative cancellation. Many of the versatile functions of this work includes

Time control feature which offers access to medical records even if the data owner is offline.
Dynamic data change: Addition and deletion of encrypted data is the most useful feature.
Proxy: In EHR systems proxy re-encryption is practical.
Confidentiality: The private records of users should be kept in secrecy from both unauthorized system guest and the EHR storage provider. The health records are guarded by the way of a robust encryption primitive.
Standard model: Our work is proved immune based on standard model and have larger security alignment.
No sharing of key: The secret keys and the decryption keys are generated separately for multi-client setting.
The keys will be generated randomly and will always be unique.
Abide offline KG attacks: Our work fights against offline guessing of keyword attacks and offers higher efficiency.

4. IMPLEMENTATION AND RESULT

The implementation of this work is executed in the utmost renowned tool of java that is Eclipse Luna by connecting it to MySQL Workbench 5.2 CE. Eclipse Luna is an incorporated advancement environment (IDE) for creating applications using standardized java programming language.
Bootstrap and JSP technologies are used for developing WebPages and provide contribution in the UI design. Hibernate is an ORM structure used for database access where as the spring framework provides security in the design. The CSP used in this work is DriveHQ which is an IT cloud service provider and have some unique features like DriveHQ file manager, DriveHQ online backup and cloud file sharing. Generator API's are used for the generation of a random six-digit secret key for both the user and the consumer and will be mailed to the registered emailID.
The experimental results compute that this work achieves high efficiency by providing automatic cancellation of the access rights after a time period allotted by the data owner previously. Also defining in advance disparate access time period for diverse users. We are also able to demonstrate that proxy Server enhances the security by re-encrypting the files. The acquaintance of the EHR storage is ensured by the outcome. Furthermore, offline keyword guessing attacks can be resisted too. Besides its higher security, this work can accomplish high processing and storage ability.

5. CONCLUSION AND FUTURE WORK

The concept of the timing enabled privacy-preserving keyword search mechanism for the EHR cloud storage supports the automated authorization cancellation. The conducted experiment and security analysis shows that this work holds much higher security than the existing solutions with a conservative outlay for cloud applications. The results ensure the acquaintance of the EHR and give impedance to the KG attacks. The competency inquiry shows that this work achieves high processing and storage ability together with its higher security, as compared with other classical searchable encryption schemes. Our future work can support other related E.H.R. applications by adding videos and even we can go for live streaming and even we can add the feature of chatting/video calling.

6. REFERENCES

[1] W. M. Tierney, J. C. Leventhal, J. A. Cummins, P. H. Schwartz and D. K. Martin,"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] Google Inc. *Google Health*. [Online]. Available: https://www.google.com/health, accessed Jan. 1, 2013.
[3]Microsoft. *Microsoft HealthVault*. [Online]. Available: http://www.healthvault.com, accessed May 1, 2015.
[4] K.Omote, K.Emura and A.Miyaji, "A timed-release proxy re-encryption scheme," *IEICE Trans. Fundam. Electron., Commun.Comput. Sci.*, vol. 94, no. 8– pp. 1682–1695, 2011.
[5]Q. Liu, J. Wu and G. Wang, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Inf. Sci.*, vol. 258, pp. 355–370, Feb. 2014.

[6] H. Zhang, F. Gao, M. Ding, and Z. Jin, "An efficient public key encryption 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.
[7] P. Liu and C. Hu, "An enhanced searchable public key encryption scheme with a designated tester and its extensions," *J. Comput.*, vol. 7,no. 3, pp. 716–723, 2012.
[8] D. H. Lee and J. W. Byun "On a security model of conjunctive keyword search over encrypted relational database," *J. Syst. Softw.*, vol. 84, no. 8, pp. 1364–1372, 2011.

[9] W. Susilo, L. Fang, J. Wang and C. Ge, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search,"*Theoretical Comput. Sci.*, vol. 462, pp. 39–58, Nov. 2012.

[10] D.Cash *et al.*,"Dynamic searchable encryption in very-large databases:Data structures and implementation," in *Proc. Netw. Distrib. Syst. Security Symp. (NDSS)*, Feb. 2014, pp. 1–32

[11] Ziqing Wang, Yi Ding, Weidong Zhong and Xu An Wang, "Proxy re-encryption with keyword search from Anonymous Conditional Proxy Re-encryption,"2011 Seventh International Conference on Computational Intelligence and Security

[12] J. Wang, C. Ge, L. Fang and W. Susilo, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," *Inf. Sci.*, vol. 238, pp. 221–241, Jul. 2013.

[13 Y. Zhang, J. Li and Y. Shi, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," *Int. J. Commun. Syst.*, doi: 10.1002/dac.2942, 2015. [14] J. H. Park, W. Susilo, H. S. Rhee 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.
[15] W. Susilo, J. Baek and R. Safavi-Naini, "Public key encryption with keyword search revisited," in *Proc. Int. Conf. ICCSA*, vol. 5072.Perugia, Italy, Jun./Jul. 2008, pp. 1249–1259.
[16] H. S. Rhee, J. H. Park, and D. H. Lee, "Generic construction of designated tester public-key encryption with keyword search," *Inf. Sci.*,vol. 205, pp. 93–109, Nov. 2012.
[17] C.-C. Lee, M.-S. Hwang and S.-T. Hsu, "A new public key encryption with conjunctive field keyword search scheme," *Inf. Technol. Control*,vol. 43, no. 3, pp. 277–288, 2014.

[18] B. Waters and D. Boneh, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Theory Cryptogr. Conf.*, vol. 4392.Amsterdam, The Netherlands, Feb. 2007, pp. 535–554.

[19] S.-H. Heng, W.-C. Yau, B.-M. Goi, and R. C.-W. Phan "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.

[20] 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.