RESEARCH ARTICLE OPEN ACCESS

A Study on Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds

[1]A. Senthil Kumar, [2]S.Abirami
[1]Asst.professor, Dept.of.Computer Science, Tamil University, Thanjavur-613010.
[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

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 favourable 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 re-encryption 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 delegate to search and decrypt the delegator's encrypted documents can be controlled. Moreover, the delegate 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, E-health.**

I. INTRODUCTION

THE increasing ability to collect, manage, and share information is raising ever-increasing privacy concerns. This poses a challenging trade-off between the value both to society, and to individuals from the knowledge available from ubiquitous, shared information, and the risk to individuals posed by disclosure and misuse of private data. One solution to this problem is anonymity: ensuring that disclosed data cannot be linked to the individual whom the data are about. The European Community Directive looks at a basic, and yet common and practical, problem: the risk is simply from identifying that an individual is or is not in an anonym zed data set. This could occur when there is a desire to publish a data set to support research on a specific condition, but identifying individuals meeting that condition is damaging. Examples could range from counterterrorism, publishing a database containing information about suspected terrorist groups to support research in automated support for discovering terrorism; to medical research, such as a database of patients with a particular type of cancer. In both cases, identifying that an individual is present in the database is damaging, both to the individual, and in the terrorism example by

disclosing to real terrorist groups that their "cover organization" is suspect.

EXISTING SYSTEM

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 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.

Disadvantages of Existing System:

- The serious privacy and security concerns are the overriding obstacle that stands in the way of wide adoption of the systems
- In the traditional time-release system, 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.

PROPOSED SYSTEM

Endeavour 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. 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.

Advantages of Proposed System:

- 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.

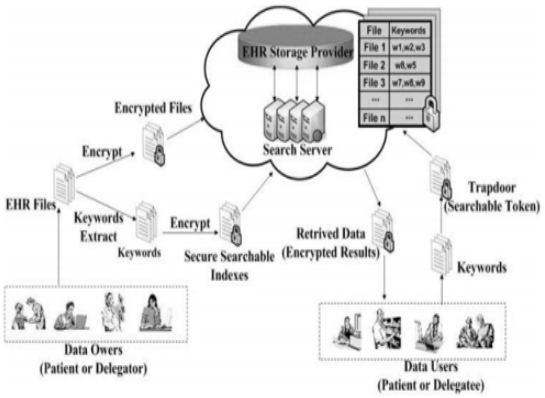


Fig. 1. System Model.

SYSTEM ARCHITECTURE

MODULES

We have 3 main modules in this project,

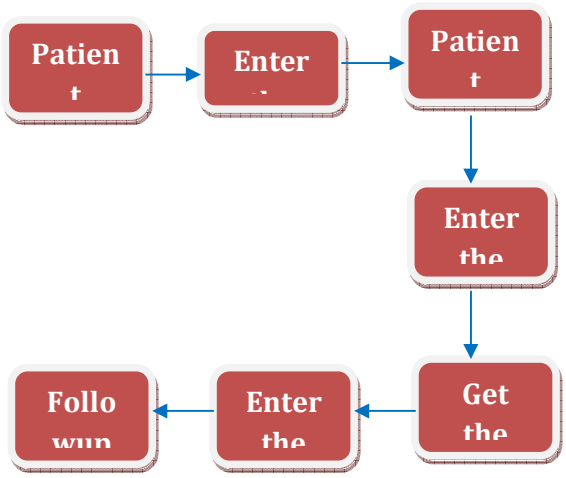
- Data Owner Module
- Data Center Module
- User Module

Module Description:

Data Owner:

The data owner wants to store his private HER 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, that data are outsourced to the data center.

Data Clients: Patient Module



Data Canter:

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.

User:

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.

IV. CONSULTATION

E-cloud framework show three entities data owner who had a authority to file or record of data ,users who want to access the data, and data centre where the actual server store the file and using trapdoor who generate the tokens when the user demand for particular file from the data storage centre. In our proposed work Re-dtPECK technique used to realize the moment allowed privacy-preserving Keyword indices in search procedure for the EHD reasoning storage space, which could support the automated delegation cancellation. Here Security and protective analysis shows our scheme provides reasonable overhead computation in cloud storage applications compared to traditional systems. This is the first retrievable security plan with the moment allowed proxies re-encryption function and the specific specialist for the privacy–preserving EHD reasoning record storage space. The solution could ensure the comfort of the EHD and the potential to deal with assume keyword attacks.

V.REFERENCE

[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, 2011.