Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

Conjunctive Multi Keyword Search Security Model with Proxy Re-Encryption Function in E-Health Clouds

[1]Megha CS, [2]Samhitha M, [3]Subramani M, [4]Vinod Shivram,[5]Annie Sujith

Abstract

An electronic health record system is a unique application that brings great comfort in the health care. Users are more concerned with their private data and its security which is difficult for further development process and promotion of the systems. Here we make use of one of the secured technology called as searchable encryption scheme which incorporates security protection and play important role in E-Health record systems. In this paper we introduce primary cryptography named as Conjunctive Multi Keyword Search Security Model with Proxy Re-Encryption Function In E-Health Clouds. This Scheme allows the patients to fragmentally access the search functions in limited time. It helps patients to accesses the search functions partially over their records with time limit. The time period for the users to search and decrypt the documents is controlled. The users access will be automatically impoverished by the authority after the specific period of time. This scheme supports multi keyword search avoid the keyword guessing attacks. The proposed model is an efficient scheme proved for secure in standard model. The proposed system has low computation and storage overhead that is proved by comparison and extensive simulation.

Keywords- Searchable encryption, time control, conjunctive keywords, e-health, resist offline keyword guessing attack.

Introduction

The Electronic health records (EHR) will bring great change in maintaining the medical records in computerized manner by preventing medical errors. This will enable patients staying in one hospital to share or manage their information with other hospital by creating their own health information. There also exists other EHR systems such as Microsoft Health Vault[3] and Google Health[4].

In this paper, we propose a multi keyword search security model with proxy Re-encryption. In public key encryption scheme with keyword search(PEKS)[3] allows user to search on encrypted information without decrypting it, which is suitable to enhance the security of EHR system. Sometimes a patient wants to give his search right to his doctor without revealing this own private key. This can be made possible by proxy re-encryption method. the data owner issues a unique key to all his users which is known as private key that is generated during the registration. All the users may use this key to access the data or information they need. The files can be Searched by a keyword. In the proposed data owner creates the keyword hence proposed scheme is formally proved secure against chosen-keyword chosen-time attack.

Existing system

Public key encryption scheme with keyword search (PEKS) allows a user to search on encrypted information without decrypting. Sometimes a patient may want to act as a delegator to delegate his search right to a delegate, who can be his doctor, without revealing his own private key. The encrypted index of the patient are converted into a re-encrypted form which can be searched by the delegate. There arises a problem when the access right is distributed. If the patient is transferred to another hospital or recovered and discharged from the hospital, patient does not want the private data to be searched and used by his previous physicians. This problem is

solved by re-encrypt all his data with a new key. This process cost more.

Disadvantages

(i) The serious privacy and security concerns are the overriding obstacle that stands in the way of wide adoption of the systems.

(ii) In the traditional time-release system, the time seal is encapsulated in the cipher text at the very beginning of the encryption algorithm. It implies that all users including data owner are constrained by the time period.

Proposed system

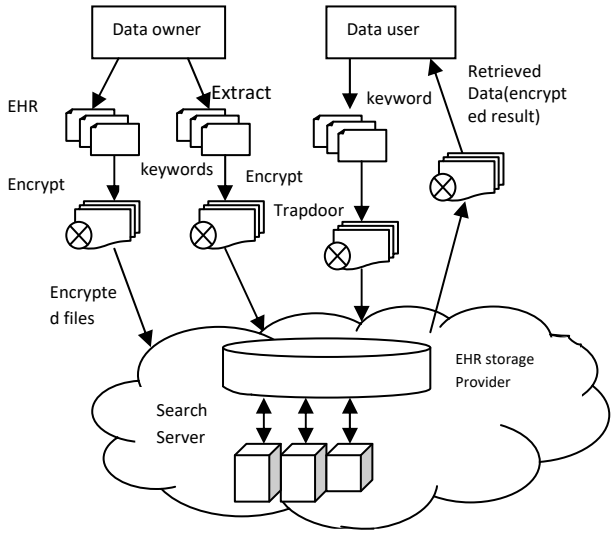

Figure 1. System model

The Conjunctive Multi Keyword Search Security Model with Proxy Re-Encryption Function in E-Health Clouds is proposed which has the following merits.

1) Compared with existing schemes, this system can achieve timing enabled proxy re-encryption with delegation revocation.

2) The proposed system is proven against offline chosen guessing attacks, chosen keyword, chosen time attack.

3) Rather than the random oracle model this scheme works based on standard model.

The figure.1 shows the proposed system model. There are three types of entities. Data Owner, Data user and Data Center(Authority). Authority is one who owns the data center he provides the private storage space to the data owner to store his EHR files. Data owner extracts the keywords from the EHR files and converts them into secure searchable indices. The EHR files are encrypted to cipher text.

A data center provides EHR storage and a server to search. Role of storage provider is to store data and search/add/delete operations are performed by search server as per user request. User uses the trapdoor generated to search the EHR files using his private key and sends it servers to search. The servers on receiving the request interact with the EHR storage provider to find the matched files and returns the result to user in encrypted form.

Workflow of the scheme

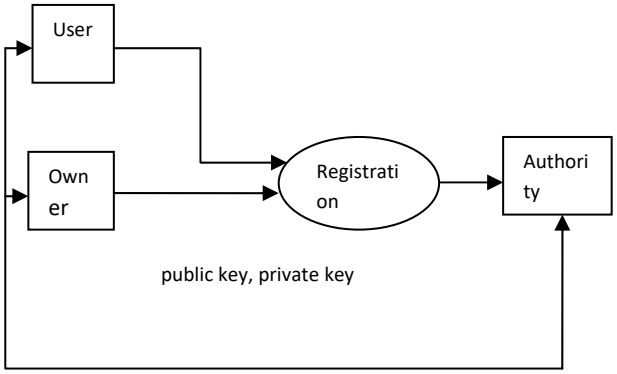

Figure 2: Level 0

The figure 2 is the start of the scheme. Initially the user and the owner must get registered with the authority. Authority provides a unique number called private key to all the users registered. And the public key remains same for all the users.

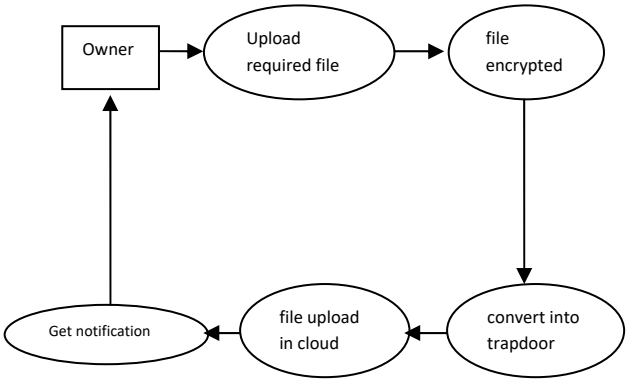

Figure 3. Level 1

The figure 3 shows the workflow of the owner end (Uploading the file to cloud). In this step, the owner has to first upload the required EHR file, during this process the file is encrypted first and converted to the trapdoor. The encrypted file is uploaded on to the cloud and the owner who uploaded the file gets the notification.

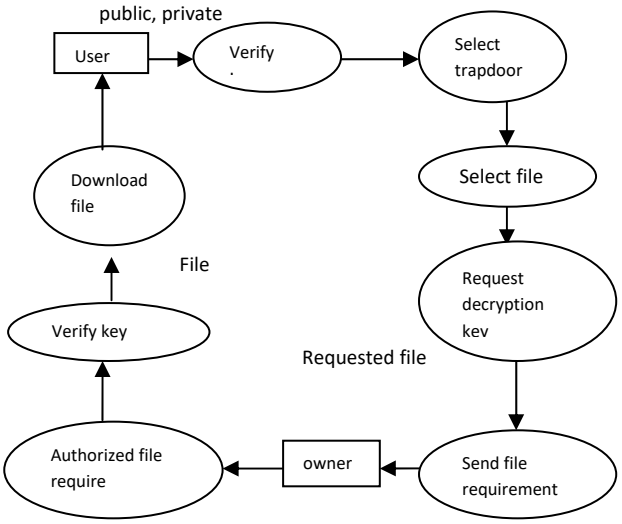

Figure 4 Level 2

figure 4 shows the workflow of the user end (Requisition and downloading of the file). The user has to first login into the portal and then has to undergo verification. This process is done by verifying the private key of the user. After verification the user has to select his appropriate file in the TMT table. The user has to copy the trapdoor and search for the file in Cloud search.

Then select the file and send a request to the owner, for the decryption key of the file. The user has to send the file requirement as well to the owner. On the other end i.e, the owner receives the request from the user, the admin checks whether the user has requested for appropriate file (Does the file actually belongs to the user or not).

The owner then approves the file and the user gets the decrypted file. The user must verify first using the private key and then download the file. After the download the user finally gets the decrypted information, which he had requested for.

Performance Analysis

There are few important indicators to check whether the scheme is suitable for privacy preserving in E-Health cloud storage. Those indicators are security level, efficiency and utility function.

Here we have compared Re-dtPECK proposed system with other SE schemes in terms of functionality, communication and computation overhead.

- **Time control**

In privacy-preserving systems the EHR data owner will be enabled by the time controlled function to spread his access rights to other user in limited time even when EHR data owner is offline

- **Conjuctive Keywords**

Conjuctive Keyword search function when compared with single key word search gives the users with more than requested results and satisfy them with multiple results.

- **Against off-line KG attack**

Till date there is no specific technique to avoid spy attacks over public communication channel. If this is not prevented, then outside attacker can easily implement off-line KG attack by seeing the data transfers between Data center and patient. Existing Systems have not kept an eye on this and not considered. But proposed system is resistant to KG Attacks.

- **Proxy**

In E-Health Record Systems, Proxy re-encryption mechanism is practical. Hence it is smooth process for patient delegating search and access rights. In Existing System there is no concept of Proxy re-encryption SE Scheme function to users.

- **Standard Model**

The Existing System Schemes are dependent on Random Oracle (R.O) model. But it was not useful for security purpose in real life.

It is proved that when Random Oracle are substituted with concrete hash functions then schemes lead to insecure schemes. Hence it is necessary to design secure primitive which is not dependent on R.O model.

- **No Key Sharing in multi-client setting**

Existing System Schemes are designed in symmetric searchable encryption setting where only single user can upload or query.

If it wants to serve multiple clients, then multi-client setting must be used. This scheme must provide symmetric key which can be shared by authorized users.

- **Dynamic Data Change**

In Existing System, the encrypted data can be added or deleted without using same symmetric key.

Proposed scheme has important functions that are useful and has stronger security functionality compared to existing SE schemes.

Conclusion

In the proposed paper, Re-dtPECK scheme is introduced to know the timing enabled privacy preserving keyword searching mechanism for E-Health Record cloud storage which supports Automatic Delegation Revocation.

The experimental results that are obtained and security analysis prove to be more secured than existing systems with reasonable overhead for cloud applications.

Till date this is the first SE scheme for timing enabled proxy re-encryption for privacy preserving EHR cloud. It also resists KG attacks.

Compared to other classical SE schemes the efficiency of proposed scheme is high and can achieve high security, high computing power and storage efficiency.

Acknowledgements

We acknowledge that the content in this paper is prepared by doing a survey of different thesis and papers on conjunctive keyword search with Proxy Re-Encryption Function in E-Health Clouds.

References

[1]. Yang Yang and Maode Ma, "Conjunctive Keyword Search with Designated Tester and timing Enabled Proxy Re-Encryption Function for E-health Clouds" vol 11, No 4 april 2016

[2] 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 technicalchallenges," J. General Internal Med., vol. 30, no. 1, pp. 17–24, 2015.

[3] Microsoft. Microsoft HealthVault. [Online]. Available: http://www. healthvault.com, accessed May 1, 2015.

[4] Google Inc. Google Health. [Online]. Available: https://www. google.com/health, accessed Jan. 1, 2013.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

Author's details

1.Megha C S UG Student, CSE, T John Institute of Technology, Karnataka, India, meghaswamy04@gmail.com

2. Samhitha M UG Student, CSE, T John Institute of Technology,Karnataka, India, samhithaurs3225@gmail.com

3. Subramani M UG Student, CSE, T John Institute of Technology, Karnataka, India, msubramani912@gmail.com

4.Vinod Shivaram UG Student, CSE, T John Institute of Technology, Karnataka, India, vndshivaram@gmail.com

5. Annie Sujith,Assistant professor,CSE,TJohn Institute ofTechnology,Karnataka,India,annie.jithu@gmail.com