# Attribute Authority and Timing Enabled Proxy Re-Encryption Function on E-Health Cloud

MANCHALA MADHUSUDHANA REDDY[1], H. ATEEQ AHMED[2]
[1]PG Scholar, Dept of CSE, Dr. K. V. Subba Reddy Institute of Technology, Kurnool, AP, India
[2]Assistant Professor PG Scholar, Dept of CSE, Dr. K. V. Subba Reddy Institute of Technology, Kurnool, AP.

## 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 Attribute Authority. 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.

## I.INTRODUCTION

Electronic heath records (EHR) system will make medical records which are computerized with the capability to prevent medical errors. It will smooth the process of a patient to create his own health information in one hospital and manage or share the information with others in other hospitals. Many practical patient-centric EHR systems have been implemented such as Microsoft Health Vault and Google Health and other service providers. Health records collected in a data center may contain private information of the patient and therefore leads to vulnerable potential leakage and disclosure to the individuals or companies who may make use for their business and own profits. Even though the service provider can influence the patients to believe that the private information will be safeguarded, the EHR can possibly be exposed if the server is intruded or an inside staff misbehaves. The serious privacy and security concerns are the overriding obstacle that stands in the way of wide adoption of the systems. we make an effort to solve the problem with a primitive mechanism proposed to automatically revoke the delegation right after a period of time designated by the data owner previously. 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. The data owner has the right to preset diverse effective access time periods for different users when he appoints his delegation right. An effective time period set by the data owner can be expressed with a beginning and closing time. For example, 1/2/2017 – 12/2/2017.The first work that enables automatic delegation revoking based on timing in a searchable Encryption.we enhanced the security by adding the concept of Attribute Authority.

## II.RELATED WORK

In Timed-Release Proxy Re-Encryption (TR-PRE) concept if the proxy transformation is utilized to a TREciphertext, the release time is still active. In a user's access right lapse automatically after a predestinedperiod of time. Searching a record inclusive of multiple encoded keywords 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. In 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 reencryption 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. The work in presents the first Chosen-Ciphertext Secure anonymous conditional proxy re-encryption with keyword search (CPRES) idea with the assistance like chosen-ciphertext security; keyword-invisibility; unidirectionality; noninteractivity;and collusion-impedance. In they designed and deployed a practical dynamic symmetricsearchable 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 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.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 EHRcloud service provider. Also the conducted work offers resistance against offline KG attacks.

## III.PROBLEM STATEMENT

If the adversary identifies that there are lower entropies in the trapdoor, the attackers can guess the keyword and guessing ofkeywords 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. Whenever the dataowner that is the patient who has given a key to the doctor who is a delegate to access his record that is present in the cloud. Once the doctor finishes accessing the data that is present there are chances that the doctor may later miss use the data, so for that a new key cannot be generated so easily. The patient should decode the old key and the patient again has to reencrypt the new key and then later update it into the cloud. So this can only be done by enabling the time for the users so that they can access it within the time that has been provided by the data owner.

## IV.IMPLEMENTATION

In Fig 1. Explain there are three types of entities: an information owner, users and data center. The data owners also called as patient or delegator uploads the e-health record files or EHR files into the cloud server where all data services are provided. The EHR files are encrypted by a symmetric encryption algorithm and a symmetric key in encapsulated with the delegator’s public key pkA by key encapsulation mechanism.

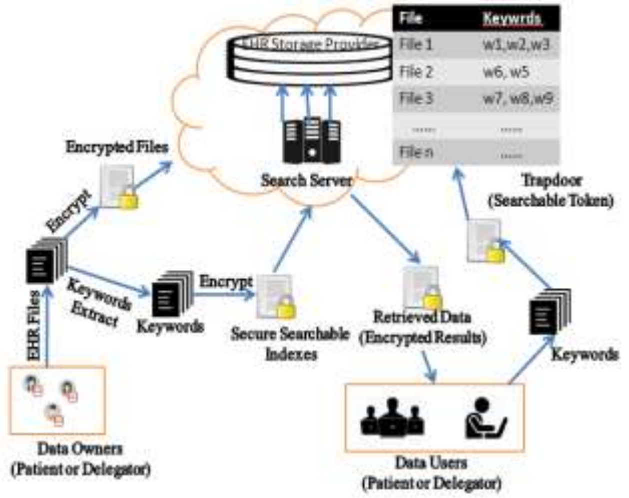

Figure:1

The algorithms in the following focus on the searchable keywords encryption and the timing controlled delegation function. From the records, certain words are taken as keywords for the delegatee to open the file by using the keywords. The keywords are once again encrypted and stored as secure searchable indexes and directly stored in the cloud server for retrieval purpose by the doctor or patient. If the data users want to retrieve the information from the cloud. The delegatee should enter the keywords to search the particular file. 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 . 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.

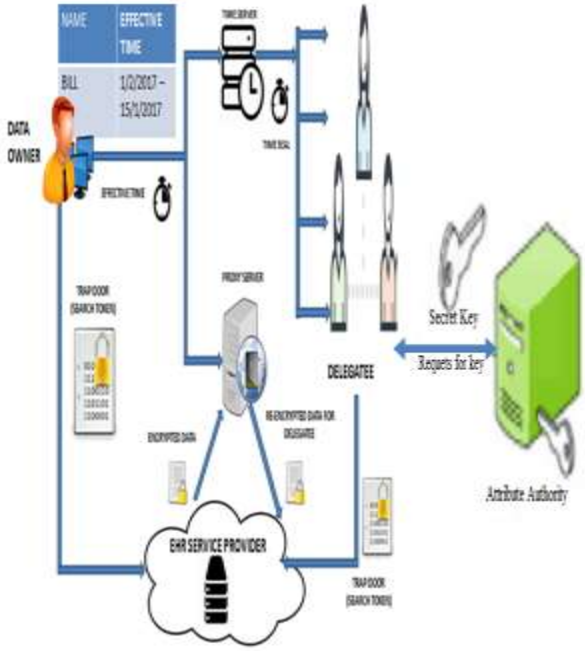

Figure:2

In Fig. 2, Explains the timing enabled proxy re-encryption searchable encryption model with Attribute Authority. In this module, we highlight the operation of the time controlled function. The data owner acts as a delegator sends a list of delegation effective time periods for his delegatees to the time server and the proxy server. The entry list consists of identity of each delegatee and the effective time period, such as "bill, 01/02/2017 – 15/02/2017". It indicates that the delegatee bill is authorized to issue queries and perform decryption operations on the encrypted data of the data owner from feb. 1st, 2017 to feb.15th, 2017. 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 encapsulate 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.When ever the delegatee want to download file. Delegatee request secret key to Attribute Authority. Attribute Authority will provide the Secret key to Delegatee to download file.

## V.MODULE DESCRIPTION

1. Authorization Delegation
2. EHR Storage Provider
3. Time Stamp
4. File Retrieval

### 1.Authorisation Delegation

The patient or delegator should register to provide file synchronization to the cloud server where the doctor can view the encrypted file by using some of the decryption algorithms. The authorization and URS provides a user registration service allowing users to self-register, free of charge. The user needs to set up a profile that includes a user ID, password, and provide a small amount of additional information, including affiliation, country, and a valid e-mail address. This information is never provided to any application without a user's explicit permission. A login, logging in or logging on is the entering of identifier information into a system by a user in order to access that system (e.g., a computer or a website). It is an integral part of computer security procedures. A login generally requires the user to enter two pieces of information, first a user name and then a password. This information is entered into a login window on a GUI(graphical user interface) or on the command line in a console (i.e., an all-text mode screen), depending on the system and situation. A user name, also referred to as an account name, is a string (i.e., sequence of characters) that uniquely identifies a user. User names can be the same as or related to the real names of users, or they can be completely arbitrary.

### 2.EHR Storage Provider

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. 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. The EHR data server is deemed as semi-trusted, who is honest to search information for the benefits of users but curious to spy out the private information of the patients. On the other hand, malicious outside attacker could eavesdrop and analyze the information transferred in public channel, such as the encrypted indexes and trapdoors.

**3.Time Stamp**

The timing enabled proxy re-encryption searchable encryption model is shown. In this model, we highlight the implementation of the time controlled function. The data owner acting as a delegatorsends 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 "bill, 01/02/2017 – 15/02/2017". It indicates that the delegatee Bill is authorized to issue queries and perform decryption operations on the encrypted data of the data owner from Feb. 1st, 2017 to Feb. 15th, 2017. 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 encapsulate the effective time into the re-encrypted ciphertext.

**4. File Retrieval**

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.

## VI.CONCLUSION

The concept of the timing enabled privacy-preserving keyword search with Attribute Authority 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.

## VII.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,"*TheoreticalComput. 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, WeidongZhong and XuAn 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.