An Effective Timing Enabled Proxy Re-encryption Scheme and Conjunctive Keyword Search with Designated Tester for E-healthcare Clouds

T.S.padekar[1], Prof.S.Rokade[2]
[1, 2] Department of Computer Engineering,
[1, 2] PREC, Loni, Maharashtra.

Abstract- *Th Electronic health (e-health) record system is a new application that will get extraordinary comfort in healthcare.The protection and security of the sensitive personal record is the major concern of the users, which could advance further development improvement and broadly reception of the systems.The searchable encryption (SE) plan is an innovation to join security protection and ideal operability works together, which can assume an essential part in the e-health record framework. In this proposed system, we present a novel cryptographic primitive named as conjunctive keyword search look with designated tester and timing empowered proxy re-encryption function (RedtPECK), which is a sort of time-dependent identifiable encryption scheme. It could empower patients to delegate incomplete get to rights to others to look work over their records in a restricted time span. The duration of the time span for the delegatee to find and decrypt the delegators encrypted records can be monitored. Also, the delegatee could be automatically revoked of the access and find authority after a defined period of time. It can also help the conjunctive keywords search as well as avoid the keyword guessing (KG) attacks. Due to this, only the designated tester is capable to test the possible certain keywords.e present study focuses on the analysis of material handling system with the help of discrete event simulation. The simple factory layout of packing system is considered and modeled with the queuing system based on time and the size delay function.it is found that the total system once modeled can helps in the improve modify or study the process in detail and helps to understand the system very effetely*

Keywords- Searchable encryption, Time control, Conjunctive Keywords, Designated Tester, E-health, Keyword Guessing attack.

I. INTRODUCTION

The electronic heath records (EHR) framework will create medical records that are computerized with the capability to detect avoid medical errors [1]. It will allow a patient to create his own health record in one hospital and control or share his medical information in other hospitals. Most practical patient-centric EHR framework has been developed like Microsoft Health Vault [2] and Google Health [3]. Given the ambitious prospect to development and deploy the HER system ubiquitously, privacy concerns of the patients come up. Healthcare data collected in a data as well as information center may contain private information and insecure to potential leakage and reveal to the individuals or troop who may make benefit from them. Even though the service provider can overcome the patients to trust that the privacy information will be safekeeping, the EHR could be liable if the server is break in or an internally staff misbehaves. The serious private and security occupy are the overlap distortion that play of wide adoption of the framework.Public key encryption strategy with keyword search (PEKS)[4-7] where user allows to search on encrypted information without decrypting it, which is perfect to increase the security of EHR framework. In some condition, a patient may be act as a delegator to delegate his search right to a delegatee, who may be a doctor, without displaying his own private key.The proxy re-encryption (PRE) technique can be introduced to fulfill the necessary. The server could change the a reencrypted form from the encrypted index of the patient which can be finded by the delegatee. However, next problem arrives when the access protocol is broadcasted. When the patient regain and leaves the hospital as well as is transferred to some different hospital, he does not want the the some special private data to be find and used by his previous physicians anymore.A possible way to solve this mystery is to re-encrypt all data of that particlur person with a new key, which will bring a much maximum cost. It will be more stressout to revoke the delegation protocol in a larger size form The proposed system attempt to work out the problem with a novel mechanism proposed to spontaneous revoke the delegation protocol after a period of time appointed by the data owner previously. In the existing time-release system [29,31], the time assurance to encapsulated in the ciphertext at the very starting of the encryption algorithm. It shows that all users with data owner are fixed by the time span. The quality of the proposed framework is that there is no time span bounds for the data owner because the time information is fixed in the reencryption phase. The data owner is able to preset various efficient access timespans for different customers when he designate his delegation protocol. An efficient timespan set by the data owner can be precised with a starting and ending time (for instance, 07/01/2017-11/01/ 2017). A time span server is used in framework, which is legislature to form a time token for the users. After receiving an efficient time period T from the data owner, the time server forms a time seal T S by using his own operation private key and the public key for delegatee.In that way, the time period T is digest in the time seal T S .By the rencryption algorithm implement by the proxy server. the time period T will be added in the re-encrypted ciphertext. which is the timing enabled proxy re-encryption function. When the delegatee problems a query request, he should form a trapdoor for the queried keywords using his own private key and time seal T S . Only if the time period digest in the trapdoor matches with the effective time period added in the proxy re-encrypted ciphertext, the cloud service provider will be respond to the search query. otherwise, the search request will decline. In that way, the access protocol of the delegatee will close automatically. The data owner necessarily not to dosome other process for the delegation cancellation To the best of our knowledge, this is the first work that enables automatic delegation revoking based on timing in a searchable encryption system. A conjunctive keyword search scheme with designated tester and timing enabled proxy re-encryption function (RedtPECK) is proposed, which has the following merits.

- Design strange searchable encryption strategy helping secure conjunctive keyword search and authorized delegation purpose. Analogize with existing strategy this work can accomplish timing enabled proxy re-encryption with efficient delegation revocation.
- Owner-enforced delegation timing set in advance is allowed.Different access timespan can be
- predefined for different delegatee.
- The proposed scheme is generally validate as a secure against chosen-keyword chosen-time attack. And also, off-line keyword guessing assault can be opposed too.
- The test algorithm could not function without data servers private key. Eavesdroppers could not succeed in presume keywords by the test algorithm.
- The security of the strategy function work based on the standard archetype rather than arbitrary oracle model. This is the first primitive that helps above functions and is build in the standard archetype.

II. REVIEW OF LITERATURE

1) **Conjunctive Keyword Search:** Different forms of public key encryption with conjunctive keyword search (PECK) on encrypted data have been developed [8-10]. It enables the users to send more than one keywords at the once [11-12]. But, some among them like solution provided in [9-10] have high communication and low computation overhead. On the other hand, some research [8, 12] require an index set of the keywords that are fired by user as a query when a trapdoor is generated, which leads to leak of the information as well as impair the query protection and security.

2) **Searchable Encryption with Designated Tester:** In general,the size of a keyword space is shall not greater than its polynomial level. A hacker can perform dictionary attacks or perform off-line keyword guessing attacks (KG attacks) to hack the encrypted keywords. In the Electronic Health Record related keywords are normally taken from a small space, especially they belong to the medical terminology. If an attacker get that the trapdoors or indexes that are in encrypted format have lower entropies, the keyword guessing attacks could be performed if the attacker try to guess the possible related keywords. Author Byun [19] and Yau [20] have cracked several traditional strategies by using the keyword guessing attacks. In order to avoid the threats, the idea of Public key encryption strategy with keyword search with designated tester (dPEKS) is elaborated in [21-25]. Only a designated tester,which is normally the server, is allow to carry on the test algorithm. The improved security models [26-28] could not allow multiple keywords in the query.

3) **Proxy Re-encryption with Public Keyword Search:** Proxy re-encryption (PRE) allow a proxy with a re-encryption key to translate a ciphertext encrypted by a data owners public key into such that it can be decrypted by users secret key.Proxy re-encryption with public keyword search (Re-PEKS) [13-15] has proposed the concept of keyword search into Proxy re-encryption. The users along with a keyword trapdoor can look for the ciphertext whereas the hidden keywords are not known to the proxy. The disadvantage on the schemes defined in [13-15] is that only single keyword is allowed tofind in the encrypted documents. In later stage, Wang et al.[16] has proposed an efficient strategy to help the conjunctive keyword search scheme. Schemes defined in [13-16] are shown secure in random oracle model. But in some schemes shown in [17-18] are insecure for random oracle model. The time managed Proxy re-encryption has been proposed in [29-31]. The schemes in [29, 31] need to

defined the release time at starting of encryption operation. Only single release time is fixed for all users, which not satisfy the property of uniqueness. Another disadvantage is that it creates a huge computation overhead in encryption as well are-encryption phases [30].

III. SYSTEM ARCHITECTURE

In Fig. 1, the environment of the proposed Re-dtPECK strategy for the EHR cloud framework is exhibited. There are three sorts of entity: an information owner, users and a data center. The information proprietor needs to store his private HER records on a outsider as well third party as database. He separates keywords from the HER documents and encrypts those plaintext keywords into the safe searchable files.The EHR records are encrypted to ciphertext. Then, those data are outsourced to the data center

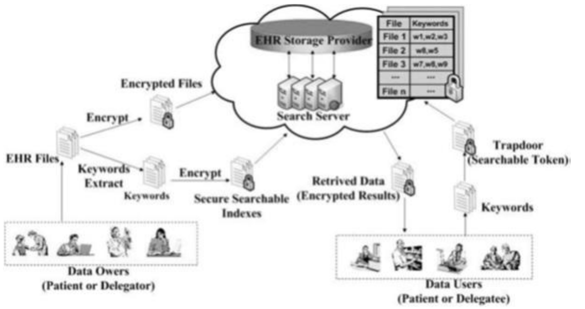

Figure 1. System Architecture

A data center comprises of an EHR storage supplier and a pursuit server. The capacity provider is in charge for storing information and search server performs search/add/erase operations as per to users requests. A user creates a trapdoor to seek the EHR records utilizing his private key and forward it to the search servers. After receiving the request, the search servers collaborate with the EHR storage supllier to locate the coordinated records and returns those retcovered data to the user in an encrypted frame.

In Fig. 2, the timing enabled proxy re-encryption searchable encryption framework is shown. In this framework, we elaborate theimplementation of the time controlled function. The data owner perform role as a delegator who sends a list of delegation effective time span for his users to the time server and the proxy server. The list is used for the identity of each delegatee and the defined time span, such as Alice, 07/01/201711/01/2017. It means that the delegatee Alice is allow to issue queries as well as allow to decrypt the encrypted record of the data owner from Jan. 6th, 2017 to Jan. 11th, 20178. After getting the list, the time server creates a time seal for every delegatee, which is send to users. The time seal is a trapdoor of time span and hide by the secret key of the time server. Next in the re-encryption phase, the proxy server will encrypt the defined effective time into the re-encrypted ciphertext. In the query phase, the delegator can perform find operations with his own secret key. But, the users have to create a keywords trapdoor by using time seal. No any matched files are shown to the user unless time seal communicate with the time which is in the form of re-encrypted ciphertext, which is different from conventional proxy re-encryption schemes.

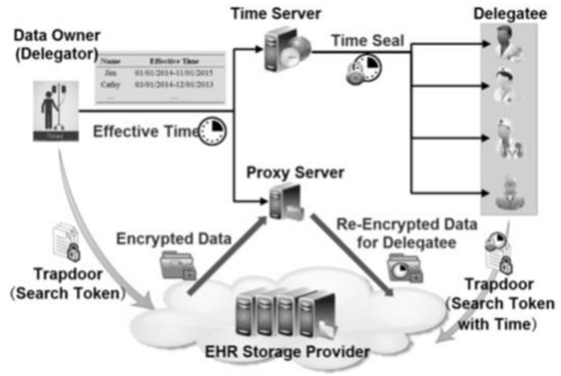

Figure 2. Timing Enabled Proxy Re-encryption Searchable Encryption Framework

IV. MATHEMATICAL MODEL

The Mathematical model is shown in figure-2. In this Document Query I is submitted to state p1 where the Global Setup is done then it is passed to state p2 where the KeyGenRec done then in state p3 where the KeyGenSer is done In next step P4 KeyGenSerTS is done then in P5 ReKeyGen take place at P6 Trapdoor done then P7 Re-dtPECK take place and the output is generated in final state O from which file is downloaded ,if file is not match within time seal again it move to P1

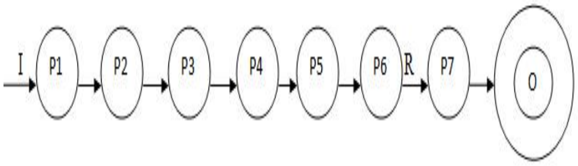

Figure 3. Mathematical Model of System

A. Input Parameter(I)

I = I1
where I is set of Input.
I1= It is keyword which is submitted to state p1.

B. Functional Parameter(Q)

Q= p1,p2,p3,p4,p5,p6,p7
where p is functions/process done in EHD system
p1 =Global Setup algorithm which generate global parameters.
p2 = KeyGenRec generate private and public key
p3 = KeyGenSer generate private and public key
p4 = KeyGenTS generate private and public key
p5 = ReKeyGen generate a re-encryption key and send it to proxy server
p6= Trapdoor which generate private key(token) used for matching the keyword with file keyword stored on EHD storage Server.

C. Output Parameter(O)

O = O1
where O is an Output parameter.
O = Result generated if file downloaded and key match within time seal.

V. IMPLEMENTATION DETAILS

In this section, formally describe the conjunctive keyword search with a designated tester and the timing enabled proxy re-encryption function (Re-dtPECK) with concrete RedtPECK scheme and with a detailed implementation details .The Re-dtPECK scheme consists of following algorithms with an indicator _. When its value is 1, the delegate on function will be activated. Otherwise, the proxy re-encryption will not be enabled. In the system, the EHR documents of the patients are encrypted by a symmetric encryption algorithm and the encrypted by a symmetric encryption algorithm and the symmetric key is encapsulated with the patients public key pkA by the key encapsulation mechanism. The algorithms in the following focus on the searchable keywords encryption and the timing controlled delegation function. The time T chosen from the time space has the form Month/Day/Year-Month/Day/Year to set the starting time and closing time of the delegation. For example, 07/01/ 2017-11/01/2017 means that the delegatee is authorized to operate on delegators secret data from Jan 1st, 2017 to Jan 11th 2017.

- GlobalSetup(k) :Taking a security parameter k as an input, this function generates a global parameter GP.
- KeyGen (Ser) GP : Taking GP as an input, this algorithm generates a private and public key pair (sks ,pks)for the data server.
- KeyGen (Rec) GP : Taking GP as an input, this algorithm generates a private and public key pair (skr ,pkr)for the for the receiver.
- KeyGen (TS) GP : Taking GP as an input, this algorithm generates a private and public key pair (skts ,pkts)for the for Time Server.
- dPECK (GP,pks,pkr,skr,W) :Taking GP,pks,pkr,skr and Keyword set W=(w1....wn) as as the inputs, the function returns a ciphertext Ci of W for Ri.
- Trapdoor(GP,pks,skr,Q):Taking GP,pks,skr and Keyword query for Q=(w1....wn), m¡l as the inputs, it outputs a trapdoor(Q,I) for Qgenerated by Ri.
- Test(GP,T,sks,Ci): Taking GP, T(Q,I) ,ssk and a ciphertext Ci of W as the inputs, the function returns 1 if W includes Q and 0 otherwise.
- If the delegation indicator equals to 1, the following operations are executed.
- ReKeyGen(GP,skri,skrj)Taking GP ,skri, skrj as the inputs, the algorithm outputs re-encryption key rkri-rkrj
- RedtPECK(GP,rkri,-Taking GP ,rkrirj ci,pki, pkj, pkts, T as the inputs the algorithm outputs a re-encryption ciphertext Cj.
- TimeSeal(GP,skts,T,Pkri,Pkrj):Taking GP,skts,T,Pkri,PKrj as the inputs, it outputs a time seal St for user Rj in order to search user Ris encrypted data.
- TrapdoorR(GPPks,Skrj,Q,St):Taking GP,Pks,Skrj,Q,St as the inputs,it outputs a trapdoor Tq,j for Rj.
- TestR(GP,Tq,j,Sks,Cj):Taking GP,Tq,j,Sks and Cj as inputs, the funtion returns ’1’ if W includes Q and the effective time contained in Tq,j is accordance with the time encapsulated in Cj.otherwise. it outputs ’0’.

VI. RESULTS AND DISCUSSIONS

Our proposed Re-dtPECK compared with other searchable encryption schemes in [4, 6, 8-10, 13-16, 21-25, 28] and the relevant proxy re-encryption schemes in [29-31] in terms of functionality, communication and computation overhead. Our proposed scheme has different useful functions and has stronger security functionality than those of most of the existing searchable encryption schemes as described in literature survey. Also proposed system shows the greater performance in terms of Time Control ,Conjunctive Keywords ,Against offline KG attack, Proxy, Standard model, No key sharing in multi-client setting, Dynamic data change. Also proposed system have low communication overhead due to the small size of public key and private key.

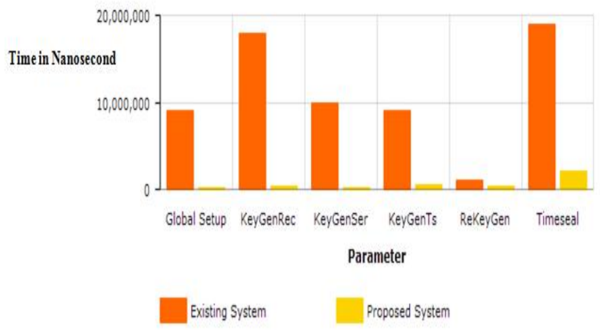

Figure 4. As in testing purpose Existing system and proposed system were compared to check the time efficiency in nanosecond proposed technique achieve high performance.

VII. CONCLUSION

In this proposed defines a novel Re-dtPECK scheme to realize the timing enabled privacy-preserving keyword search mechanism for the EHR cloud storage, which could support the automatic delegation revocation. Our proposed scheme holds much higher security than the existing solutions with a reasonable overhead for cloud applications. Our proposed system is the first searchable 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. In future work it can be applied directly to federated clouds.It is also a future work to Reduce number of Trapdoors under multi-owners setting.

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. Microsoft healthvault. http://www.healthvault.com.

[3] Google Inc. Google health. 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. 506522, 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.

[8] M. Hwang, S. Hsu, C. Lee. A New Public Key Encryption with Conjunctive Field Keyword Search Scheme, Information Technology and Control, vol. 43, no. 3, pp. 277-288, 2014.

[9] D. Boneh, B. Waters, Conjunctive subset and range queries on encrypted data, in Proc. 4th Theory of Cryptography Conference, Amsterdam, The Netherlands, February 21-24, 2007, vol. 4392, pp.53554, Springer.

[10]B. Zhang, F. Zhang, An efficient public key encryption with conjunctivesubset keywords search, Journal of Network and Computer Applications, vol. 34, no. 1, 262-267, 2011.

[11]J. Byun, D. Lee, On a security model of conjunctive keyword search over encrypted relational database, Journal of Systems and Software, vol.84, no. 8, pp. 1364-1372, 2011.

[12]M. Ding, F. Gao, Z. Jin, H. Zhang, An efficient public key encryption with conjunctive keyword search scheme based on pairings, in Proc. 3rd IEEE International Conference on Network Infrastructure and Digital Content(IC-NIDC), Beijing, China, Sept. 21-23, 2012, pp. 526-530, IEEE.

[13]J. Shao, Z. Cao, X. Liang, H. Lin, Proxy re-encryption with keyword search, Information Sciences, vol. 180, no. 13, pp. 2576-2587, 2010.

[14]W. Yau, R. Phan, S. Heng, B. Goi, Proxy Re-encryption with Keyword Search: New Definitions and Algorithms, in Proc. International Conferences on Security Technology, Disaster Recovery and Business Continuity,

Jeju Island, Korea, Dec. 13-15, 2010, vol. 122, pp. 149-160, Springer.

[15]L. Fang, W. Susilo, C. Ge, J. Wang, Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search, Theoretical Computer Science. vol. 462, pp. 39-58, 2012.

[16]X. Wang, X. Huang, X. Yang, L. Liu, X. Wu, Further observation on proxy re-encryption with keyword search, Journal of Systems and Software, vol. 85, no. 3, 643-654, 2012.

[17]R. Canetti, O. Goldreich, S. Halevi, The Random Oracle Methodology, Journal of the ACM, vol. 51, pp. 557-594, 2004.

[18]M. Bellare, A. Boldyreva, A. Palacio, An Uninstantiable Random-oracle model Scheme for a Hybrid-encryption Problem, in Proc. InternationalConference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Interlaken, Switzerland, May 2-6, 2004, vol. 3027, pp. 171-188, Springer.

[19]J. Byun, H. Rhee, H. Park, D. Lee, Off-line key-word guessing attacks on recent keyword search schemes over encrypted data, in Proc. Third VLDB Workshop on Secure Data Management (SDM), Seoul, Korea, September 10-11, 2006, vol. 4165, pp. 75-83, Springer.

[20]W. Yau, R. Phan, S. Heng, B. Goi, Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester, International Journal of Computer Mathematics, vol. 90, no. 2, pp. 2581- 2587, 2013.

[21]J. Baek, R. Safavi-Naini, W. Susilo, Public key encryption with keyword search revisited, in Proc. International Conference on Computational Science and Its Applications (ICCSA), Perugia, Italy, June 30-July 3, 2008, vol. 5072, pp. 12491259, Springer.

[22]L. Guo, W. Yau, Efficient Secure-Channel Free Public Key Encryption with Keyword Search for EMRs in Cloud Storage, Journal of medical systems, vol. 39, no. 2, pp. 1-11, 2015.

[23]H. Rhee, J. Park, W. Susilo, D. Lee, Trapdoor security in a searchable public-key encryption scheme with a designated tester, Journal of Systemsand Software, vol. 83, no. 5, pp. 763771, 2010.

[24]C. Hu, P. Liu, A Secure Searchable Public Key Encryption Scheme with a Designated Tester against Keyword Guessing Attacks and Its Extension, in Proc. International Conference on Advances in Computer Science, Environment, Ecoinformatics, and Education (CSEE), Wuhan, China, August 21-22, 2011, vol. 512, pp.131-136, Springer.

[25]C. Hu, P. Liu, An enhanced searchable public key encryption scheme with a designated tester and its extensions, Journal of Computers, vol. 7, no. 3, pp. 716-723, 2012.

[26]H. Rhee, J. Park, D. Lee, Generic construction of designated tester public-key encryption with keyword search, Information Sciences, vol. 205, pp. 93-109, 2012.

[27]W. Yau, R. Phan, S. Heng, B. Goi, Security models for delegated keyword searching within encrypted contents, Journal of Internet Services and Applications, vol. 3, no. 2, pp. 233-241, 2012.

[28]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.

[29][29] K. Emura, A. Miyaji, K. Omote, A timed-release proxy re-encryption scheme, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, vol. 94, no. 8, pp. 1682-1695, 2011.

[30]Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Information Sciences, vol.258, pp.355-370, 2014.

[31]K. Liang, Q. Huang, R. Schlegel, D. S. Wong, C. Tang, A Conditional Proxy Broadcast Re-Encryption Scheme Supporting Timed-Release, In Proc. Information Security Practice and Experience , pp. 132-146, Springer Berlin Heidelberg, 2013