ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

Conjunctive catchword scan with Designated analyser and timing enabled proxy re-encryption method for e-health clouds

[1]Koustuba A, [2] Lakshmi N, [3] Leelavathi S, [4] Salma Arifa Farzana, [5] Ravindra Prasad S
[1][2][3][4] Students of Department of Computer science and Engineering , RRIT, Karnataka, India
[5] Associate Prof , Dept of Computer Science and Engineering ,RRIT, Karnataka, India

***Abstract*— An electronic health (e-health) record framework is a novel requisition that will achieve incredible comfort in health awareness. The protections and security of the delicate data aid the major worries of the users, which will thwart further improvement and broadly reception of the frameworks. The searchable Encryption (SE) plan will be a innovation organization with fuse security protection moreover ideal operability capacities together, which plays a fundamental part in the e-health record framework. In this paper, we present a novel cryptographic primitive named as conjunctive Catchword scan with designated analyzer and timing enabled proxy re-encryption capacity, which is a sort of a time-dependent SE plan. It could empower patients to represent fractional entry privileges to others to perform search operation over their records within a restricted time period. The period of the time for the delegatee to search and decrypt the delegator's encrypted documents could be regulated. Moreover, the delegatee could be naturally denied of access power after a specified time. It can be backing the conjunctive keywords search and Oppose keyword guessing strike. We define a system model and a security model for proposed plan to indicate that it is an effective plan demonstrated secure in the standard model.**

***Keywords:* Searchable encryption, time control, Conjunctive keywords, designated tester, e-health, oppose keyword guessing strike.**

1. INTRODUCTION

THE ELECTRONIC HEATH RECORDS (EHR) framework will make restorative records to be computerized with the capacity to anticipate medical blunders [1]. It will encourage a patient to make his health data in one hospital and oversee or share the data with others in different hospitals. Numerous viable patient-driven EHR frameworks have been executed for example, Microsoft Health Vault [2] and Google Health [3]. Given the yearning prospect to send the EHR framework universally, protection worries of the patients come up. Healthcare information collected in a server may contain private data also, powerless against potential spillage and disclosure to the people or organizations who may make benefits from them. Despite the fact that the service provider can persuade the patients to trust that the protection of data will be care, the EHR could be uncovered if the server is barged in or an inside staff misbehaves. The genuine protection and security concerns are the superseding concerns that obstructs wide adoption of the frameworks.

Public key encryption scheme with keyword search (PEKS) [4]–[7] enables a user to quest on encoded data without decoding it, which is reasonable to upgrade the security of EHR frameworks. In a few circumstances, a patient might need to act as a delegator to delegate his quest privilege to a delegatee, who can be his doctor, without uncovering his own private key. The proxy re-encryption (PRE) technique can be acquainted which satisfy the requisite. The server could change over the encrypted list of the patient into a reencrypted form which can be sought by the delegatee. In any case, another issue emerges when the access right is dispersed. At the point when the patient recoups and leaves the doctor's facility or is exchanged to another hospital, he does not need the private information to be looked and utilized by his past doctors any longer. A conceivable way to deal with tackle this issue is to re-encode every one of his information with another key, which will bring a substantially higher cost. It will be more troublesome to repudiate the delegation right in a versatile size.

In this paper, we attempt to take care of the issue with a novel component proposed to naturally repudiate the designation directly after a timeframe assigned by the data owner already in the conventional time-discharge framework [28], [30], the time seal is embodied in the ciphertext at the earliest reference point of the encryption calculation. The excellence of the proposed framework is that there is no time constraint for the data owner because the time data is embodied in the re-encryption stage. The

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

data owner is fit to assign different access time period for various users when he chooses his assignment right. An effective time period set by the data owner can be provided with a start and end time (for example, 01/01/201412/01/2014). A time period server is utilized as a part of the framework, which is responsible to produce a time period token for the users. Once an effective time period T is obtained from the data owner, the time server produces a time seal ST by utilizing his own private key and public key of the delegatee. In that way, the time period T is epitomized in the time seal ST. By the re-encryption algorithm executed by the proxy server, the time period T will be implanted in the re-encrypted ciphertext. It is timing enabled proxy reencryption re-encryption capacity. At the point when the delegatee issues an, he must create a trapdoor for the questioned catchphrases utilizing his private key and time seal ST. Just if the time period typified in the trapdoor matches with the effective time period implanted in the proxy re-encrypted ciphertext, the cloud server provider will react to the pursuit inquiry. Or else, the pursuit demand will be rejected. In that way, access right of the delegatee will lapse consequently. The data owner needs not to do whatever other operation for the designation repudiation. To the best of our insight, this may be the primary worth of effort that empowers programmed assignment revoking in view of timing to a Searchable encryption framework. A conjunctive catch word scan with designated analyzer and timing enabled proxy re-encryption Capacity is proposed, which has the following merits.

• 1) We configure a novel searchable encryption plan supporting secure Conjunctive catch word scan and commissioned assignment work. Compared with existing schemes, this worth of effort camwood attain timing enabled proxy re-encryption for viable assignment disavowal.

• 2) Owner-enforced assignment timing preset will be enabled. Dissimilar right time period might make predefined to different delegatee.

• 3) The proposed plan will be formally demonstrated secure against Chosen-keyword chosen-time strike. Furthermore, logged off catch word guessing strike could make resisted excessively awful. The test calculation could not work without data owner's private enter. Eavesdroppers could not succeed for guessing Keywords by the test algorithm.

• 4) The security of the plan meets expectations in light of the Standard model instead of irregular Prophet model. This will be the first primitive that backs over works and will be based on the standard model.

II. RELATED WORK

A. Conjunctive catch word scan

Different constructions of public key encryption for conjunctive Pivotal word scan over encrypted information have been suggested [8]– [10]. It permits the user to inquiry various keywords at the same time [11]-[12]. However, exactly for them for example, the result in [9], [10] have high communication or calculation expense. On the different hand, a few schemes such as the results done [8] and [12] needs a list of rundown queried keywords when an trapdoor is generated, which will Spill majority of the data and disable those inquiry security.

B. Searchable Encryption with Designated Tester

Over practice, the span of a catch word space is dependably no more over its polynomial level. A assailant may be potentially to propel word reference strike or logged off word guessing strike (KG. Attacks) with misuse those stowed away keywords. The EHR keywords are typically choose from a starting with a little space, particularly the therapeutic Words. Whether a foe figures that the trapdoors alternately encrypted indexes bring easier entropies, the kg strike could be started Assuming that the foe endeavors to guess those could reasonably be expected nomination keywords. Byun et al. [19] and Yau et al. [20] have broken a few established schemes Eventually Tom's perusing those kg strike. In order to stand up to the threats, the idea from claiming PEKS with. Designated analyzer (dPEKS) is suggested Previously, [21]–[25]. Main An. Designated tester, which is as a rule the server, is fit to go ahead the test calculation. The improved security models [7], [26], [27] have been place forward. However, they are not backing conjunctive keywords inquiry or delegate scan capacity.

C. Proxy Re-Encryption with public catch word scan.

Proxy re-encryption (PRE) empowers a proxy for a Reencryption key with change over a ciphertext encrypted

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

by a delegator's public key into those that can be decrypted by delegatee's private key. Proxy re-encryption with public catch word search (Re-PEKS) [13]–[15] has acquainted the thought from claiming catch word scan under PRE. The user with a catch word trapdoor can able to scan the ciphertext While hidden keywords are obscure of the proxy. The drawback on the schemes in [13]– [15] is that only single word will be permitted to scan in the encrypted documents. After Wang, et al. [16] proposed a progressed plan with backing the conjunctive catch word function. these RePEKS schemes over [13]– [16] are demonstrated secure in random oracle model. But in [17] and [18] proved that a random oracle model may bring unstable schemes. The time controlled PRE has been subjected in [28]– [30]. It wishes to encrypt a message for different beneficiaries for the same discharge time. However, the schemes in [28] and [30] foist the data owner to determine that discharge duration of the time during the beginning of encryption algorithm. Only one discharge duration of the time may be situated to all beneficiaries in spite of variable for different users, which could not satisfy the need to uniqueness. Another deficiency will be that it necessities an extensive calculation cost in both encryption and re-encryption periods [29].

III. PROBLEM FORMULATION

A. System Model

The nature of the proposed scheme for the EHR cloud framework is displayed in figure1. There are three sorts of elements: a data owner, user and cloud storage. The data owner needs to store his private EHR records in cloud storage provider. He extracts catchwords from the EHR records and encodes those plaintext catchwords into the secure searchable files. The EHR records are encrypted to ciphertext. At that point, the scan server is responsible to performs scan/add/erase operations as per user request. A user produces a trapdoor to look the EHR documents utilizing his private key and sends it to the scan servers. Subsequent to accepting the request, the scan server interface with the EHR storage provider to locate the requested records and returns those data to the user in an encoded form. In this model, we highlight the usage of the time controlled capacity. The data owner acts as a delegator sends a list of designations of his delegatee's which s is embodied in the time server and the proxy server. The list contains the of each delegatee and the effective time period, for example,"Rao,05/07/2017–11/16/2015". It demonstrates that the delegatee Rao is approved to issue inquiries and perform decryption operations on the encrypted information of the data owner from May 7th, 2017 to Nov. 16th, 2017. In the wake of accepting the list, the time server creates a period seal for each delegatee, which is transmitted to people. In the re-encryption operation, the proxy server will typify the successful time into the re-encrypted ciphertext. All together to diminish computing cost, the proxy server won't re-encrypted the ciphertext until they are accessed, which is supposed to called lazy re-encryption mechanism [31]. In the query stage, the data owner can lead conventional inquiry operations with his own private key. Be that as it may, the delegatee needs to produce a catchwords trapdoor with the assistance of the time seal. The cloud information server won't give back the requested documents unless the compelling time exemplified in the time seal agrees with the time in the re-encrypted ciphertext, which is not quite the same as conventional proxy reencryption SE schemes.

B. Threat Model

The EHR data server is regarded as semi-trusted, who is fair to scan data for the advantages of users yet inquisitive to spy out the private data of the patients. Then again, vindictive outside assailant could spy and investigate the data moved out in the open channel, for example, the encoded lists and trapdoors. He means to surmise security data as per this information. Moreover, the renounced delegatee's may attempt to get to information past the assigned period utilizing their private keys. As the vast majority of the storage and scan work are finished by the information server, it is accepted that the data server won't collude with the noxious outside assailant or renounced delegatees.

C. Mathematical Model

• Global Setup(k): Taking a security parameter k as an input, this function generates a global parameter GP.
• KeyGenSer(GP): TakingGP as an input, this algorithm generates a private and public key pair (skS, pkS) for the data server.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

• KeyGenRec(GP): Taking a global parameter GP as an input, this function generates a private and public key pair (sk_R, pk_R) for the receiver.
• KeyGenTS(GP): Taking a global parameter GP as an input, this function generates a private and public key pair (sk_{TS}, pk_{TS}) for the time server.
• dPECK (GP, pkS, pk_{Ri}, sk_Ri,W): TakingGP, pk_S, pk_Ri, skRi and a keyword set W = (w1,⋯,wl) as the inputs, the function returns a ciphertext CI of W for Ri. • Trapdoor (GP, pk_S, sk_Ri, Q): TakingGP, pk_S, sk_Ri and a keyword query for Q = (w1, ⋯,wm), m ≤ las the inputs, it outputs a trapdoor TQ,I for Q generated by Ri. • Test (GP, TQ, I, skS, CI): TakingGP, TQ,I, sk_S and a ciphertext CI of Was the inputs, the function returns '1' if W includes Q and '0' otherwise.

SUMMARY OF NOTATIONS

➢ Global Setup algorithm which generate global parameters.
➢ KeyGenRec generate private and public key
➢ KeyGenSer generate private and public key
➢ KeyGenTS generate private and public key
➢ ReKeyGen generate a re-encryption key and send it to proxy server
➢ Trapdoor which generate private key(token) used for matching the keyword with file keyword stored on EHD storage Server.

SYSTEM ARCHITECTURE

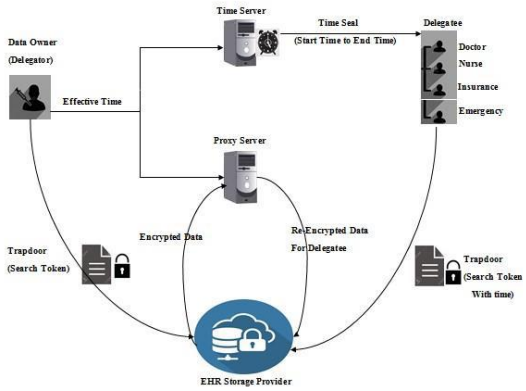

Figure:1 Timing Enabled Proxy Re-Encryption Searchable Encryption Model.

IV. DISCUSSION

As encrypted data is stored in the cloud, we plan to give greater security by performing twofold encryption on encoded data. In order to decrypt the encoded data a mystery key will be sent to client by means of mail this can make work less demanding by sending mystery keys by means of messages.

V. CONCLUSION

The proposed framework bolsters the programmed assignment renouncement. The test results and security investigation show that the plan holds significantly higher security than the current solutions.This is the primary searchable encryption conspire with the planning empowered intermediary re-encryption work and the assigned analyzer for the privacy–preserving EHR cloud record stockpiling. The arrangement could guarantee the secrecy of the EHR and the imperviousness to the KG assaults. It Compared with other established searchable encryption plots, the proficiency investigation demonstrates that our proposed plan can accomplish high calculation and capacity effectiveness other than its higher security

VI. REFERENCES

[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.

[11] J. W. Byun and D. H. Lee, "On a security model of conjunctive keyword search over encrypted relational database," J. Syst. Softw., vol. 84, no. 8, pp. 1364–1372, 2011.

[12] M. Ding, F. Gao, Z. Jin, and H. Zhang, "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.

[13] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy reencryption with keyword search," Inf. Sci., vol. 180, no. 13, pp. 2576–2587, 2010.

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

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

[16] X. A. Wang, X. Huang, X. Yang, L. Liu, and X. Wu, "Further observation on proxy re-encryption with keyword search," J. Syst. Softw., vol. 85, no. 3, pp. 643 654, 2012.

[17] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," J. ACM, vol. 51, no. 4, pp. 557– 594, 2004.

[18] M. Bellare, A. Boldyreva, and A. Palacio, "An uninstantiable randomoracle- model scheme for a hybrid-encryption problem," in Proc. Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT), vol. 3027. Interlaken, Switzerland, May 2004, pp. 171–188.

[19] J. W. Byun, H. S. Rhee, H.-A. Park, and D. H. Lee, "Offline keyword guessing attacks on recent keyword search schemes over encrypted data," in Proc. 3rd VLDB Workshop Secure Data Manage. (SDM), vol. 4165. Seoul, Korea, Sep. 2006, pp. 75–83.

[20] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester," Int. J. Comput. Math., vol. 90, no. 12, pp. 2581–2587, 2013.

[21] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Proc. Int. Conf. ICCSA, vol. 5072. Perugia, Italy, Jun./Jul. 2008, pp. 1249–1259. [22] L. Guo and W. C. Yau, "Efficient secure-channel free public key encryption with keyword search for EMRs in cloud storage," J. Med. Syst., vol. 39, no. 2, pp. 1–11, 2015.

[23] H. S. Rhee, J. H. Park, W. Susilo, 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.

[24] C. Hu and P. Liu, "A secure searchable public key encryption scheme with a designated tester against keyword guessing attacks and its extension," in Proc. Int. Conf. Adv. Comput. Sci., Environ., Ecoinform., Edu. (CSEE), vol. 512. Wuhan, China, Aug. 2011, pp. 131–136.

[25] C. Hu and P. Liu, "An enhanced searchable public key encryption scheme with a designated tester and its extensions," J. Comput., vol. 7, no. 3, pp. 716–723, 2012.

[26] 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.

[27] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Security models for delegated keyword searching within encrypted contents," J. Internet Services Appl., vol. 3, no. 2, pp. 233–241, 2012.

[28] K. Emura, A. Miyaji, and K. Omote, "A timed-release proxy re-encryption scheme," IEICE Trans. Fundam. Electron., Commun. Comput. Sci., vol. 94, no. 8, pp. 1682–1695, 2011.

[29] Q. Liu, G. Wang, and J. Wu, "Time-based proxy reencryption scheme for secure data sharing in a cloud environment," Inf. Sci., vol. 258, pp. 355–370, Feb. 2014.

[30] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang, "A conditional proxy broadcast re-encryption scheme supporting timedrelease," In Information Security Practice and Experience. Berlin, Germany: Springer, 2013, pp. 132–146.

[31] J. Li, Y. Shi, and Y. Zhang, "Searchable ciphertextpolicy attribute-based encryption with revocation in cloud storage," Int. J. Commun. Syst., doi: 10.1002/dac.2942, 2015.