Tester and Timing Enabled Proxy Re-Encryption Function on E-Health Clouds by Conjunctive Keyword Search

P.Nagalakshmi[1], N.Bhaskar[2]

[1]Dept of CSE, CMR TECHNICAL CAMPUS, Hyderabad, Telangana (501401), INDIA.
Email:Nagalakshmi0206@gmail.com
[2]Dept of CSE, CMR TECHNICAL CAMPUS, Hyderabad, Telangana (501401), INDIA.
Bhaskar4n@gmail.com

Abstract—*An electronic health (e-health) record system is a novel application that will bring great accomodation in healthcare. The privacy and security of the sensitive personal information are the major concerns of the users, which could obstruct further development and widely adoption of the systems. The searchable encryption (SE) scheme is a technology to incorporate security aegis and propitious operability functions together, which can play a consequential role in the e-health record system. In this paper, we introduce a novel cryptographic primitive designated 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 constrained duration. The length of the duration for the delegatee to probe and decrypt the delegator's encrypted documents can be controlled. Moreover, the delegatee could be automatically deprived of the access and search ascendancy after a designated period of efficacious time. It can additionally support the conjunctive keywords search and resist the keyword conjecturing attacks. By the solution, only the designated tester is able to test the*
sse 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, conjunctive keywords, designated tester, e-health, resist offline keyword guessing attack.

I. INTRODUCTION

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR accommodation sanctions a patient to engender, manage, and control her personal health data in a centralized place through the web, from anywhere and at any time (as long as they have a web browser and Internet connection), which has made the storage, retrieval, and sharing of the the medical information more efficient. Especially, each patient has the full control of her medical records and can efficaciously share her health data with a wide range of users, including staffs from healthcare providers, and their family members or friends. In this way, the precision and quality of care are amended, while the healthcare cost is lowered. Concurrently, cloud computing has magnetized an abundance of attention because it provides storage-as-a-accommodation and software-as-a accommodation, by which software accommodation providers can relish the virtually illimitable and elastic storage and computing resources [1]. As such, the PHR providers are more and more disposed to shift their PHR storage and application accommodations into the cloud in lieu of building specialized data centers, in order to lower their operational cost. For example, two major cloud platform providers, Google and Microsoft are both providing their PHR accommodations, Google Health1 and Microsoft HealthVault[2] respectively.

II. HEADINGS

1.Introduction
2. Related Work
2.1. Subsisting system.
2.2. Disadvantages of Subsisting System.
2.3. Proposed system.
2.4. Advantages of Proposed System.
3.Implementation
4.Experimental Result
5. Conclusion
6. Acknowledgement

III. FIGURES AND TABLES

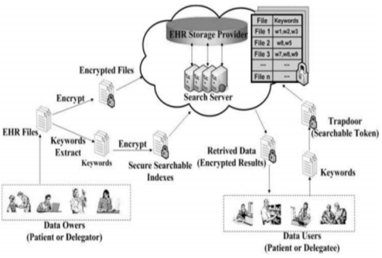
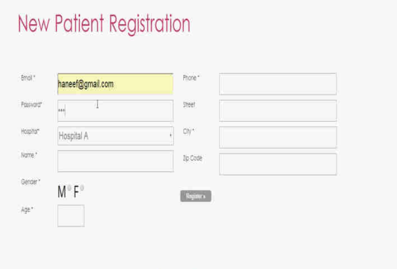


Fig .1: System Model.



New Patient Registration

Email * haneef@gmail.com

Password* ***

Hospital* Hospital A

Name *

Gender * M ○ F ○

Age *

Phone *

Street

City *

Zip Code

Register »

Fig.2: New Patient Info.

In fig.2. the patient register their information by giving email-id, name, gender, age, phone no, street , city and zip-code to consult a doctor and access rights to others to operate search functions over their records in a limited time period and only the designated tester is able to test the existence of certain keywords.

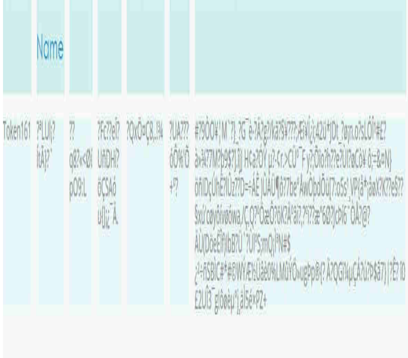


Fig.3: Encryption of Data in Cloud

In fig.3. the proxy re-encryption (PRE) method can be introduced to fulfill the requirement. A novel mechanism proposed to automatically revoke the delegation right after a period of time designated by the data owner. The data owner is capable to preset effective access time periods for different users.

IV. CONCLUSION

In this paper, we have proposed a novel Re-dt PECK scheme to realize the timing enabled privacy-preserving keyword search mechanism for the EHR cloud storage, which could fortify the automatic delegation revocation. The experimental results and security analysis designate that our scheme holds much higher security than the subsisting solutions with a plausible overhead for cloud applications. To the best of our erudition, until now this is the first searchable encryption Scheme with the timing enabled proxy re-encryption function and the designated tester for the privacy–preserving HER cloud record storage. The solution could ascertain the confidentiality of the EHR and the resistance to the KG attacks. It has withal been formally proved secure predicated on the standard model under the hardness posit of the truncated decisional l-ABDHE quandary and the DBDH quandary. Compared with other classical searchable encryption schemes, the efficiency analysis shows that our proposed scheme can achieve high computation and storage efficiency besides its higher security. Our simulation results have additionally shown that the communication and computation overhead of the proposed solution is feasible for any authentic world application scenarios.

ACKNOWLEDGEMENT

The Successful Completion of any task would be incomplete without expression of simple gratitude to the people who encouraged our work. The words are not enough to express the sense of gratitude towards everyone who directly or indirectly helped in this task. I thankful to this Organization CMR Technical Campus, which provided good facilities to accomplish my work and would like to sincerely thank to our chairman Ch. Gopal Reddy Sir, Director Dr. A. Raji Reddy Sir, HOD K SrujanRaju sir, my guide Mr.N.Bhaskar sir, my faculty members and my family for giving great support, valuable suggestions and guidance in every aspect of my work.

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.