RESEARCH ARTICLE OPEN ACCESS

"A use of proxy based re-encryption method for health sector services on cloud."

Ms. Archana Ashok Kulkarni

Prof. A.A.Phatak
Solapur University, Solapur
Department of Computer Science & Engineering
NBNS COE, SOLAPUR
archana.a.kulkarni28@gmail.com

****

Abstract:

The across the board acknowledgment of cloud fundamentally based administrations inside the consideration part has brought about worth compelling and advantageous trade of non-general Health Records (PHRs) among many working together elements of the e-Health frameworks. However, putting away the secret wellbeing information to cloud servers is powerless against disclosure or burglary and requires the occasion of procedures that ensure the protection of the PHRs. In this manner, we tend to propose a procedure known as SeSPHR for secure sharing of the PHRs inside the cloud. The SeSPHR subject guarantees quiet driven administration on the PHRs and jelly the privacy of the PHRs. The patients store the encoded PHRs on the un-confided in cloud servers and by determination award access to contrasting sorts of clients on very surprising pieces of the PHRs. A semi-believed intermediary known as Setup and Re-encryption Server (SRS) is acquainted with line up people in general/private key sets and to give the re-encryption keys. Also, the procedure is secure against corporate official dangers and furthermore upholds an advance and in reverse access the executives. Additionally, we tend to officially dissect and confirm the working of SeSPHR system through the High Level Petri Nets (HLPN). Execution investigation identifying with time utilization demonstrates that the SeSPHR approach can possibly use for solidly sharing the PHRs inside the cloud.

Keywords - Access Control, Cloud Computing, Personal Health Records, Privacy

****

I. INTRODUCTION

Cloud computing paradigm has to emerge offer pervasive as an important and on- more formally, the PHRs are managed through the Inter- net based tools to permit patients to create and manage demand availability of various resources in the form of their health information as lifelong records that can be hardware, software, infrastructure, and storage. Made available to those who need the access. Consequently, the cloud computing paradigm facilitates frequently, the PHRs enable the

patients to effectively com- organizations by relieving them from the protracted job municate with the doctors and other care providers to of infrastructure development and has encouraged them inform about the symptoms, seek advice, and keep trust on the third-party Information Technology (IT) health records updated for accurate diagnosis and treat- services. Additionally, the cloud computing model ment. has demonstrated significant potential to increase coor-Despite the advantages of scalable, agile, cost effective, dination among several healthcare stakeholders and also and ubiquitous services offered by the cloud, various to ensure continuous availability of health information, concerns correlated to the privacy of health data also and scalability. Furthermore, the cloud computing arise.

A major reason for patients' apprehensions regard- also integrates various important entities of health caring the confidentiality of PHRs is the nature of the cloud domains, such as patients, hospital staff including the share and store the PHRs. Storing the private doctors, nursing staff, pharmacies, and clinical laboratory health information to cloud servers managed by third- personnel, insurance providers, and the service providers parties is susceptible to unauthorized access. The Health Insurance Portability and Accountability Act (HIPAA) man- dates that the integrity and confidentiality of electronic health information stored by the healthcare providers must be protected by the conditions of use and disclosure and with the permission of patients. Moreover, while the PHRs are stored on the third-party cloud storage, they should be encrypted in such a way that neither the cloud server providers nor the unauthorized entities should be able to access the PHRs. Instead, only the entities or individuals with the 'right-to-know' privilege should be able to access the PHRs. Moreover, the mechanism for granting the access to PHRs should be administered by the patients themselves to avoid any unauthorized modifications or misuse of data when it is sent to the other stakeholders of the health cloud environment.

The patients as the proprietors of the PHRs are allowed to transfer the encoded PHRs on the cloud by specifically conceding the entrance to clients over various segments of the PHRs. Every individual from the gathering of clients of later type is allowed access to the PHRs by the PHR proprietors to a certain level contingent on the job of the client. The amount of access granted to varied categories of users is defined within the Access Control List (ACL) by the PHR owner. For example, the family members or friends of the patients could also be given full access over the PHRs by the owner. So also, the agents of the insurance agency may just be prepared to get to the segments of PHRs containing data about the protection claims while the inverse classified clinical data, for example, clinical history of the patient t is confined for such clients.

II. RELATED WORK

The security of the electronic wellbeing information in the distributed computing condition is a significant issue that requires exceptional contemplations. We have introduced a best in class audit on the methodologies and systems that are at present being utilized to manage the significant issue of security. We have sorted the security saving methodologies into cryptographic and non-cryptographic methodologies. In addition, we have created scientific categorization of the methods that have been applied to save the security of the current information. Another important issue worth investigating is determining and verifying the integrity of the health data in the cloud environment. Although existing privacy preserving mechanisms offer support to maintain the integrity of data in the cloud, assimilating the integrity verification mechanism with the existing solutions

will offer the patients and the data owners to realize an increased sense of control over the data. [1]

A cloud based recommendation system for health insurance plans based on the user specified criteria and priorities. Testing the framework at a limited level depicts that the proposed framework is highly effective in offering customized recommendations about health insurance plans. Particularly, the flexibility to test the insurance plans by altering the priorities of different attributes is certainly a beneficial feature that allows comparison among various plans based on multiple criteria it's likewise anticipated that in not so distant future, the examination on protection proposal frameworks additionally will increment in setting of the PPACA when more clients will begin getting to the protection commercial center. Along these lines, the need for advancement of procedures and strategies for goliath information inside the social insurance space will. [2]

In this paper, treating doctors can further refer the patients' medical record to specialists for research purposes, while the patients' personal information remains private. In addition, cross domains operations can be supported. We provided a concrete instantiation of our system. We also gave a simulation result for it. [3]

III. ELECTRONIC HEALTH RECORD

In current social insurance area, electronic wellbeing records (EHRs) are broadly received to empower social insurance suppliers, insurance agencies and patients to make , oversee what's more, get to patients' human services data from anyplace what's more, whenever. Ordinarily, a patient may have numerous different human services suppliers including clinical consideration doctors, pros, specialists, and various clinical experts. Moreover, a patient may have contrasting kinds of protections, such as clinical protection, dental protection and vision protection, from various human services insurance agencies. Subsequently, a patient's EHRs are regularly discovered dispersed all through the entirety human services segment. From the clinical point of view, in order to convey quality patient consideration, it's basic to get to the incorporated persistent consideration data that is frequently gathered at the reason of care to ensure the freshness of time-touchy information. This further requires a productive, make sure about and ease component for sharing EHRs among numerous human services suppliers. Especially, in some crisis social insurance circumstances, prompt trade of patient's EHRs are significant to spare bunches of lives. Be that as it may, in current social insurance settings, human services suppliers for the most part build up and keep up their own electronic clinical history (EMR) frameworks for putting away and overseeing EHRs.[4]

Personal health records (PHRs) enable consumers to electronically store, manage, and share their own health information, separated from electronic or paper medical records maintained by their health care providers.1 In the United States, health care is primarily provided by private enterprises. Patients with serious illness may visit a variety of different health care providers to meet their health care needs. Each of these providers may maintain separate records of medical treatment, laboratory results, medications, and health history and personal information about the patient. [5]

IV. SECURITY AND PRIVACY IN CLOUD COMPUTING

The PHR contains several personal information that most medical information systems do not allow patients to maintain, and is instead managed by the information system. If these data is to be protected, it should be attained through information system's safety protocols. To do so, the safety mechanisms of the system should be able to withstand malicious attacks and unauthorized access. [6]

With the advancement of data innovation what's more, clinical innovation, clinical data has been created from conventional paper records into electronic clinical records, which have now been broadly applied. The new-style clinical data trade

framework "individual wellbeing records (PHR)" is continuously evolved. PHR is a sort of wellbeing records kept up and recorded by people. A perfect individual wellbeing record could incorporate individual clinical data from various sources and give total and right close to home wellbeing and clinical synopsis through the Web or compact media under the prerequisites of security what's more, security. A great deal of individual wellbeing records is being used. The patient-focused PHR data trade framework permits people in general self-rulingly keep up and oversee individual wellbeing records. Such administration is helpful for putting away, getting to, and sharing individual clinical records. With the development of Cloud registering, PHR administration has been moved to putting away information into Cloud servers that the assets could be deftly used and the activity cost can be decreased. All things considered, patients would confront security issue while putting away PHR information into Cloud. In addition, it requires a secure insurance plan to encode the clinical records of every patient for putting away PHR into Cloud server. In the encryption process, it would be a test to accomplish precisely getting to clinical records and relating to adaptability what's more, productivity. [7]

V. CONCLUSION AND FUTURE WORK

On this paper, we addressed the problem of methods provide a user-specific weight for each cloud which only coordinates the fraction of storage load for each cloud but cannot prevents the information leakage across the CSPs efficiently. So Distributing data on multiple clouds provides users with a certain degree of information leakage control in that no single cloud provider is privacy to the entire user's data. Previous paper has focused on measurement analysis of cloud storage services only. However, unplanned distribution of data chunks can lead to avoidable information leakage. To tackle this problem, this work proposed an Enhanced Data Leakage Controller (EDLC). It controls information leakage efficiently. The receiver sends the decryption request to the owner or the owner can share the required credentials through Bring Your Own Secure Channel (BYOC) or out of band procedure.
In future to reduce this time consuming limitations a novel Time Considered EDLC method needed.

ACKNOWLEDGMENT

I profoundly grateful to prof. for his/her expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. I would like to express my deepest appreciation towards Principal, prof., HOD department of computer engineering and PG coordinator. I must express my sincere heartfelt gratitude to all staff members of computer engineering department who helped me directly or indirectly during this course of work. Finally, I would like to thank my family and friends, for their precious support.

REFERENCES

[1] A. Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 4, pp. 1431-1441, 2014.

[2] A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach, "*Future Generation Computer Systems*, vols. 43-44, pp. 99-109, 2015.

[3] M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system," Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017.

[4] R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In *8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work- sharing Collaborate Com)*, 2012, pp. 711-718.

[5] J. Li, "Electronic personal health records and the question of privacy," *Computers*, 2013, DOI: 10.1109/MC.2013.225.

[6] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 2, pp. 1–17, Jul. 2012.

[7] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, "Secure Dynamic access control scheme of PHR in cloud computing," *Journal of Medical Systems*, vol. 36, no. 6, pp. 4005–4020, 2012.

[8] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 2, pp. 1–17, Jul. 2012.

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYP-TO 84 on Advances Cryptology*, 1985, pp. 10-18.

[10] W. Diffie, and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, 1976, pp. 644-654.

[11] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud, "*Future Generation Computer Systems*, vol.35, 2014, pp. 102-113.

[12] S. U. R. Malik, S. U. Khan, and S. K. Srinivasan, "Modeling and Analysis of State-of-the-art VM-based Cloud Manage-ment Platforms, "*IEEE Transactions on Cloud Computing*, vol. 1, no. 1, pp. 50-63, 2013.

[13] T. Murata, "Petri Nets: Properties, Analysis and Applications, "*Proceedings of the IEEE*, vol. 77, no. 4, pp. 541-580, Apr. 1989.

[14] L. D. Mouraand N. Bjørner. "Satisfiability modulo theories: An appetizer." InFormal Methods: Foundations and Applications, Springer Berlin Heidelberg, 2009, pp. 23-36.

[15] A. Biere, A. Cimatti, E. Clarke, O. Strichman, and Y. Zhu, "Bounded Model Checking," *Advances in Computers*, vol. 58, 2003, pp. 117-148.

[16] A. D. Caro, and V. Iovino, "j PBC: Java pairing based cryptography," in *IEEE Symposium on Computers and Communications (ISCC)*, 2011, pp. 850-855.

[17] L. Ibraimi, M. Asim, and M. Petkovic, *Secure management of personal health records by applying attribute-based encryption*, Technical Report, University of Twente, 2009.

[18] J. Pecarina, S. Pu, and J.-C. Liu, "SAPPHIRE: Anonymity for enhanced control and private collaboration in healthcare clouds," in *Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2012, pp. 99–106.

[19] M. Jafari, R. S. Naini, and N. P. Sheppard, "A rights manage-ment approach to protection of privacy in a cloud of electronic health records," in *11th annual ACM workshop on Digital rights management*, October 2011, pp. 23-30.

[20] F. Xhafa, Fatos, J. Feng, Y. Zhang, X. Chen, and J. Li, "Privacy-aware attribute-based PHR sharing with user accountability in

cloud computing, ”*The Journal of Supercomputing*,2014, pp. 1-13.

[21] C. Leng, H. Yu, J.Wang, and J. Huang, “Securing personal health records in the cloud by enforcing sticky policies,” *Telkomnika Indonesian Journal of Electrical Engineering*, vol. 11, no. 4, pp. 2200–2208, 2013.

[22] D.H Tran, N. H.-Long, Z. Wei, N. W. Keong, “Towards security in sharing data on cloud-based social networks,” in *8th International Conference on Information, Communications and Signal Processing (ICICS)*, 2011, pp. 1-5.

[23] X. Liang, Zhenfu Cao, Huang Lin, and Jun Shao. "Attribute based proxy re-encryption with delegating capabilities." In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, pp. 276-286. ACM, 2009.

[24] A. N. Khan, M.L. M. Kiah, S. U. Khan, Sajjad A. Madani, and Atta R. Khan. "A study of incremental cryptography for security schemes in mobile cloud computing environments." In Wireless Technology and Applications (ISWTA), 2013 IEEE Symposium on, pp. 62-67. IEEE, 2013.