OAIJSE

OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SeSPHR: A METHODOLOGY FOR SECURE SHARING OF PERSONAL HEALTH RECORDS IN THE CLOUD

Ganesh Tambe [1], *Aditya Maharnavar[2], Venkatesh Jagtap[3], Samarth Phalke[4] , Prof. Santosh Bhosale[5]*

UG Students[1,2,3,4], Computer Department, BSP,JSPM's Wagholi,pune
Professor[5], Computer Department, BSP,JSPM's Wagholi,pune
ganeshtambe1409@gmail.com [1] , adityamahanwar9@gmail.com[2], vjagtap0612@gamil.com[3], samarthphalke@gmail.com[4], santoshtbhosale@gmail.com[5]

Abstract: The broad acknowledgment of cloud based services in the healthcare sector has brought about practical and helpful trade of Personal Health Records (PHRs) among a few taking part elements of the e-Health systems. Nevertheless, putting away the secret health data to cloud servers is susceptible to revelation or theft and requires the improvement of approaches that guarantee the protection of the PHRs. Along these lines; we propose an approach called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the classification of the PHRs. The patients store the encrypted PHRs on the un-trusted in cloud servers and specifically grant access to various kinds of clients on various parts of the PHRs. A semi-trusted in proxy called Setup and Re-encryption Server (SRS) is acquainted with set up people in general/private key combines and to deliver the re-encryption keys. Besides, the strategy is secure against insider threats and furthermore authorizes a forward and in reverse access control. Moreover, we formally examine and check the working of SeSPHR strategy through the High Level Petri Nets (HLPN). Execution assessment in regards to time utilization demonstrates that the SeSPHR strategy can possibly be utilized for safely sharing the PHRs in the cloud.

Keywords: *Access Control, Cloud Computing, Personal Health Records, Privacy.*

I INTRODUCTION

Cloud computing has emerged as an important computing paradigm to offer pervasive and on demand availability of various resources in the form of hardware, software, infrastructure, and storage. The cloud computing also integrates various important entities of healthcare domains, such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service providers. Numerous methods have been employed to ensure the privacy of the PHRs stored on the cloud servers. The privacy preserving approaches make sure confidentiality, integrity, authenticity, accountability, and audit trial. Confidentiality ensures that the health information is entirely concealed to the unsanctioned parties, whereas integrity deals with maintaining the originality of the data, whether in transit or in cloud storage. Authenticity guarantees that the health-data is accessed by authorized entities only, whereas accountability refers to the fact that the data access policies must comply with the agreed upon procedures. We present a methodology called Secure Sharing of PHRs in the Cloud (SeSPHR) to administer the PHR access control mechanism managed by patients themselves.

The methodology preserves the confidentiality of the PHRs by restricting the unauthorized users. The patients as the owners of the PHRs are permitted to upload the encrypted PHRs on the cloud by selectively granting the access to users over different portions of the PHRs. Each member of the group of users of later type is granted access to the PHRs by the PHR owners to a certain level depending upon the role of the user. The levels of access granted to various categories of users are defined in the Access Control List (ACL) by the PHR owner. For example, the family members or friends of the patients may be given full access over the PHRs by the owner. Similarly, the representatives of the insurance company may only be able to access the portions of PHRs containing information about the health insurance claims while the other confidential medical information, such as medical history of the patient is restricted for such users.

II LITERATURE SURVEY

A Review on the State-of- the-Art Privacy Preserving Approaches in the e-Health Clouds

This paper aimed to encompass the state-of-the-art privacy preserving approaches employed in the e-Health clouds. Moreover, the privacy preserving approaches are classified into cryptographic and non-cryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted.

A general framework for secure sharing of personal health records in cloud system

In this paper, Author provided an affirmative answer to this problem by presenting a general framework for secure sharing of PHRs. This system enables patients to securely store and share their PHR in the cloud server (for example, to their carers), and furthermore the treating doctors can refer the patients' medical record to specialists for research purposes, whenever they are required, while ensuring that the patients' information remain private. This system also supports cross domain operations (e.g., with different countries regulations).

Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues

This paper addressed design and architectural issues of PHR systems, and focused on privacy and security issues which must be addressed carefully if PHRs are to become generally acceptable to consumers.

Achieving secure, scalable and fine-grained data access control in cloud computing

This paper addressed challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents. It achieved this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. This scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that this scheme is highly efficient and provably secure under existing security models.

III SYSTEM ARCHITECTURE

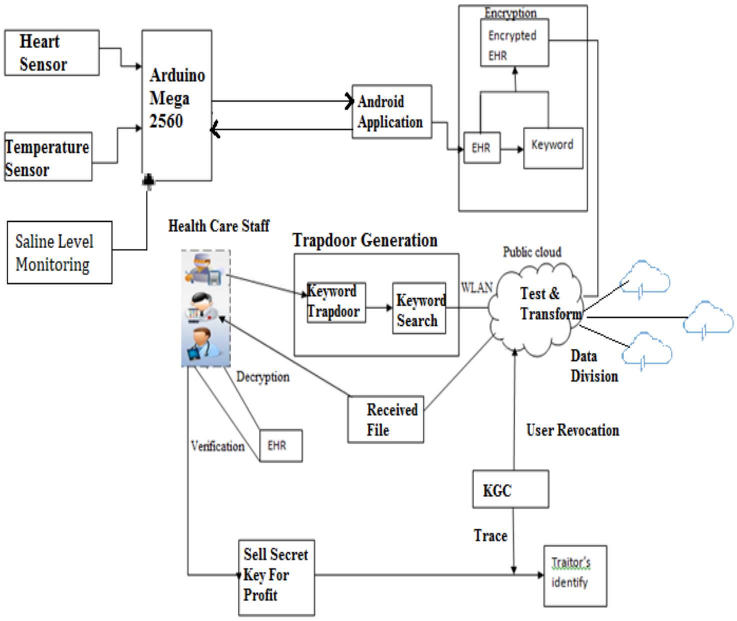
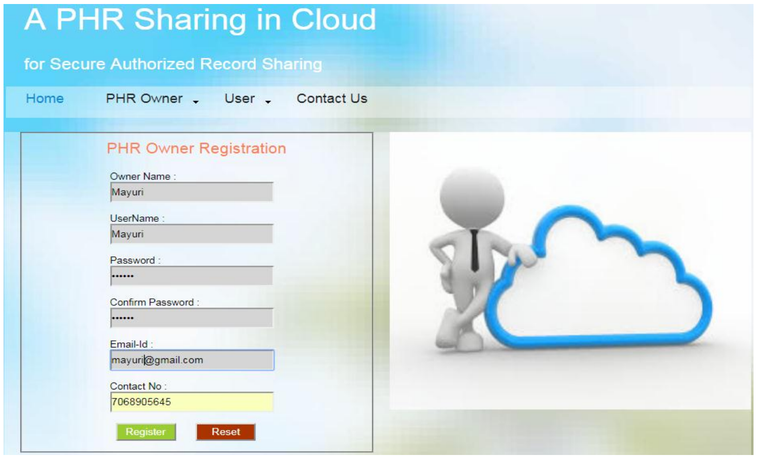


Figure 1: System Architecture

IV RESULTS



A PHR Sharing in Cloud

for Secure Authorized Record Sharing

PHR Owner Registration

Owner Name : Mayuri

UserName : Mayuri

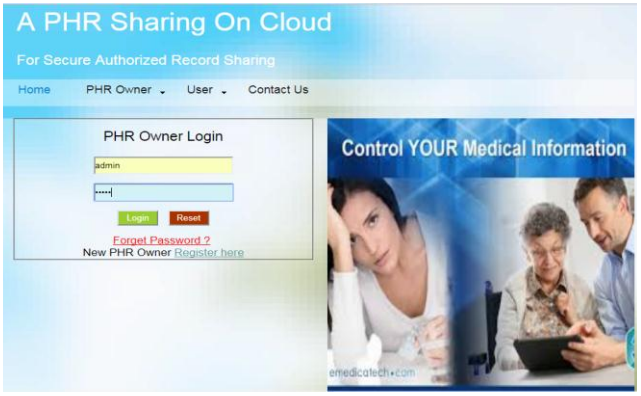
Password : ••••••

Confirm Password : ••••••

Email-Id : mayuri@gmail.com

Contact No : 7068905645

Figure 2: Registration of PHR Owner



A PHR Sharing On Cloud

For Secure Authorized Record Sharing

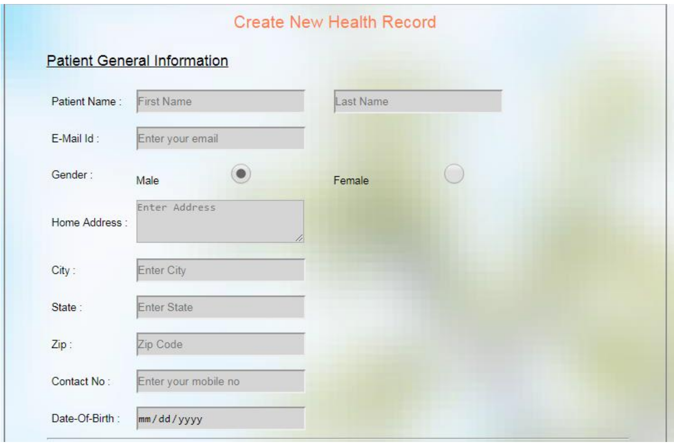
PHR Owner Login

admin

•••••

New PHR Owner Register here

Figure 3: PHR Owner Login



Create New Health Record

Patient General Information

Patient Name :	First Name		Last Name	
E-Mail Id :	Enter your email			
Gender :	Male	●	Female	○
Home Address :	Enter Address			
City :	Enter City			
State :	Enter State			
Zip :	Zip Code			
Contact No :	Enter your mobile no			
Date-Of-Birth :	mm/dd/yyyy			

Figure 4: Create PHR

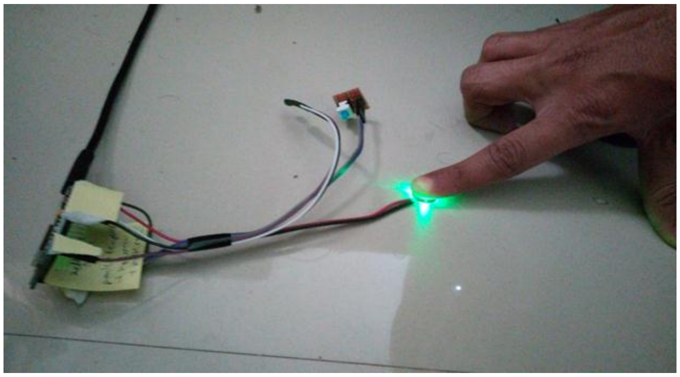


Figure 5: Collecting pulse and body temperature of patient

V CONCLUSION AND FUTURE WORK

We proposed a procedure to safely store and transmission of the PHRs to the authorized elements in the cloud. The strategy preserves the security of the PHRs and authorizes a patient-driven access control to various segments of the PHRs on the access provided by the patients. We executed a fine-grained access control technique so that even the valid system clients can't get to those segments of the PHR for which they are not authorized. The PHR owners store the encrypted information on the cloud and just the approved users having valid re-encryption keys issued by a semi-trusted authority can decrypt the PHRs. The job of the semi-trusted authority is to produce and store the public/private key sets for the clients in the system. The performance Evaluation was done on the based on time required to generate keys, encryption and decryption tasks, and turnaround time. The trial results display the reasonability of the SeSPHR system to secure share the PHRs in the cloud environment.

REFERENCES

[1] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in Edge-of-Things", Future Generation Computer Systems, 2018.

[2] K. Gai, M. Qiu, and X. Sun, "A survey on FinTech", Journal of Network and Computer Applications, 2017.

[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, 2017.

[4] 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, 2015.

[5] Assad Abbas, Samee U. Khan, Senior Member, "A Review on the State of-the-Art Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014.

[6] J. Li, "Electronic personal health records and the question of privacy", Computers, 2013.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing", in Proceedings of the IEEE INFOCOM, March 2010.

[8] David Daglish and Norm Archer, "Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues", IEEE 2009.