ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Method for the Safely Exchange of Private Health Records in the Cloud

M. Ranjith
Department of Computer Science and Engineering, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana-500014, India.

Mr. Saleem
Department of Computer Science and Engineering, Malla Reddy College of Engineering and Technology, Hyderabad, Telangana-500014, India.

ABSTRACT

The widespread use of cloud services in the health sector has led to an expensive and efficient conversion of personalized health records (PHR) coincidences among several entities involved in the Health letter. However, keeping health information confidential on a cloud server is simply a disclosure or theft and is called a development method that guarantees the privacy of PHR. Therefore, we recommend a technology called SEPHR for the security of the provision of PHR in the cloud. The SEPHR control software guarantees patient-centered PHR and maintains the privacy of the PHR. Patients who place PHR encryption on a cloud server are unreliable and selectively provide services to different users in different areas of PHR. The half-trust alternative called Setup and Re-encryption server (SRS) introduced the private key/key pair and played the secret. In addition, security tactics showed threats from Go. In addition, we formally analyze and verify the technology that SEPHR has through the High-Level Petri Nets (HLPN).

1. INTRODUCTION

Cloud computing has become an important computer concept to provide broad access to the needs of more resources in the system, hardware, infrastructure, and storage. Therefore, the concept of cloud computing allows organizations through contributions from long-term infrastructure development and encourages them to trust IT services. In addition, the cloud computing model has shown great potential to improve coordination between different health actors and also ensure access to health information and scalability. In addition, cloud computing can also integrate several important components in the healthcare field, such as patients, hospital staff, including physicians, nurses, pharmacies and laboratories for clinical staff, insurance providers and suppliers. Therefore, a collaboration between institutions that facilitate environmental health reform is positive and collaboration where patients can create and organize Personal Health Records (PHR). Generally, the PHRs contain information, such as: **(a)**demographic information, **(b)**patient's medical history including the diagnosis, allergies, past surgeries, and treatments,**(c)**laboratory reports, **(d)**data about health insurance claims, and **(e)**private notes of the patients about certain important observed health conditions .

PROBLEM STATEMENT

Although the benefits are unrelated, agile, expensive and ubiquitous services offered by the cloud, some issues related to health data also occur. The most important reason for a patient concerned about PHR confidentiality is to allocate cloud assets and set PHR. private health information to store a server in the cloud is managed and a third party may be allowed to access it legally. In particular, PHR privacy stored in the cloud managed by public service providers is very risky commerce. A day can have dangerous privacy in several ways, for example, theft, loss, and leakage.

PHR on cloud storage or patient transport in the cloud or from the cloud to users who can access other illegal acts because of external malicious entities. In addition, there are also some internal threats with those who are the data authority. For example, PHR on cloud storage or patient cloud transport or from cloud users living on the ground

Cite this article as: M. Ranjith & Mr. Saleem, "A Method for the Safely Exchange of Private Health Records in the Cloud", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6 Issue 12, 2019, Page 12-17.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

is not less than they are not allowed to log in due to bad media behavior.

OBJECTIVE:

PHR is stored in the cloud layers of third parties, they must be encrypted so that the cloud services or entities not authorized can access a PHR. Like conditions, the only entity or person who has the right to "light information" should have access to the PHR services. In addition, the process provides access to the PHR should be borne by the patient himself to correct any changes that are not valid or misuse of data sent to the other stakeholders in the health care environment.

2. Literature Survey

Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues

In this paper, we present a comprehensive analysis of the data security and privacy threats, protection technologies, and countermeasures inherent in edge computing. Specifically, we first make an overview of edge computing, including forming factors, definition, architecture, and several essential applications. Next, a detailed analysis of data security and privacy requirements, challenges, and mechanisms in edge computing are presented. Then, the cryptography-based technologies for solving data security and privacy issues are summarized. The state-of-the-art data security and privacy solutions in edge-related paradigms are also surveyed. Finally, we propose several open research directions of data security in the field of edge computing.

Secure sharing of electronic health records in clouds

We propose a systematic access control mechanism to support selective sharing of composite electronic health records (EHRs) aggregated from various healthcare providers in clouds. Our approach ensures that privacy concerns are accommodated for processing access requests to patients' healthcare information.We also demonstrate the feasibility and efficiency of our approach by implementing a proof-of-concept prototype along with evaluation results.

Incremental proxy re-encryption scheme for mobile cloud computing environment

In this paper, we have proposed an incremental version of proxy re-encryption scheme for improving the file modification operation and compared with the original version of the proxy re-encryption scheme on the basis of turnaround time, energy consumption, CPU utilization, and memory consumption while executing the security operations on mobile device. The incremental version of proxy re-encryption scheme shows significant improvement in results while performing file modification operations using limited processing capability of mobile devices.

Privacy-preserving multi-channel communication in Edge-of-Things

This work focuses on the issue of the conflict between privacy protection and efficiency and proposes a new approach for providing higher-level security transmission using multi-channel communications. We implement experiment evaluations to examine the performance of the proposed approach.

A cloud based health insurance plan recommendation system: A user centered approach

We propose a cloud based framework that offers personalized recommendations about the health insurance plans. We use the Multi-attribute Utility Theory (MAUT) to help users compare different health insurance plans based on coverage and cost criteria, such as: (a) premium, (b) co-pay, (c) deductibles, (d) co-insurance, and (e) maximum benefit offered by a plan. To overcome the issues arising possibly due to the heterogeneous data formats and different plan representations across the providers, we present a standardized representation for the health insurance plans. The plan information of each of the providers is retrieved using the Data as a Service (DaaS). The framework is implemented as Software as a Service (SaaS) to offer customized recommendations by applying a ranking technique for the identified plans according to the user specified criteria.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

3. OVERVIEW OF THESYSTEM

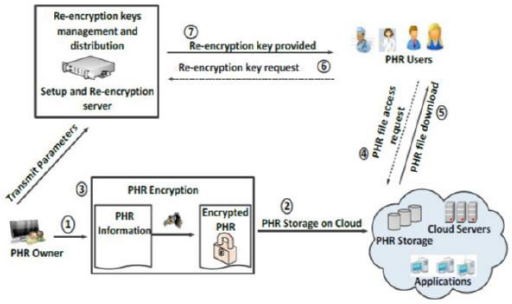

Fig 3.1 System Architecture

3.1 EXISTING SYSTEM

- Despite the advantages of scalable, agile, cost effective, and ubiquitous services offered by the cloud, various concerns correlated to the privacy of health data also arise. A major reason for patients' apprehensions regarding the confidentiality of PHRs is the nature of the cloud to share and store the PHRs
- More formally, the PHRs are managed through the Inter-net based tools to permit patients to create and manage their health information as lifelong records that can be made available to those who need the access.

3.2 DISADVANTAGE OF EXISTINGSYSTEM

- The privacy of the PHRs can be at risk in several ways, for example theft, loss, and leakage.
- The PHRseither in cloud storage or in transit from the patient to the cloud or from cloud to any other user may be susceptible to unauthorized access because of the malicious behavior of external entities.
- Moreover, there are also some threats by valid insiders to the data. For instance, the PHRs either in cloud storage or in transit from the patient to the cloud or from cloud to any other user may be susceptible to unauthorized access because of the malicious behavior of external entities.

3.3 PROPOSEDSYSTEM

- We present a methodology called SEPHR that permits patients to administer the sharing of their own PHRs in the cloud.
- The SEPHR methodology employs encryption and proxy re-encryption to ensure the PHR confidentiality.
- The methodology allows the PHR owners to selectively grant access to users over the portions of PHRs based on the access level specified in the policy for different groups of users.
- A semi-trusted proxy called SRS is deployed to ensure the access control and to generate the re-encryption keys for different groups of users there by eliminating the key management overhead at the PHR owner's end.

3.4ADVANTAGES OF PROPOSED SYSTEM

- Owner's end, the SEPHR methodology avoids the over-head by delegating the SRS for setting up the public/private key pairs and producing the decryption keys for the authorized users only.
- Moreover, the users are granted access to specific portions of the users is granted access to specific portions of the user's data.

3.5 MODULES:

Cloud Module: The scheme proposes the storage of the PHRs on the cloud by the PHR owners for subsequent sharing with other users in a secure manner. The cloud is assumed as un-trusted entity and the users upload or download PHRs to or from the cloud servers. As in the proposed methodology the cloud resources are utilized only to upload and download the PHRs by both types of users, therefore, no changes pertaining to the cloud are essential.

Setup and Re-encryption Server (SRS):

The SRS is a semi-trusted server that is responsible for setting key pairs for the users in the system. The SRS also generates the re-encryption keys for the purpose of secure PHR sharing among different user groups. The SRS in the proposed methodology is considered as semi-trusted entity.There fore, we assume it to be honest following the protocol generally but curious in nature. The keys are maintained by the SRS but the PHR data is never transmitted to the SRS. Encryption and decryption operations are performed at the users' ends. Besides the key management, the SRS also implements the access control on the shared data.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The SRS is independent server that cannot be deployed over a public cloud because of cloud being un-trusted entity. The SRS can be maintained by a trusted third-party organization or by a group of hospitals for convenience of the patients. It can also be maintained by a group of connected patients. However, SRS maintained by hospitals or by a group of patients will generate more trust due to involvement of health professionals and/or self-control over SRS by patients.

Users Module:

Generally, the system has two types of users:**(a)**the patients(owners of the PHR who want to securely share the PHRswith others) and **(b)**the family members or friends of patients, doctors and physicians, health insurance companies' representatives, pharmacists, and researchers. In SEPHR methodology, the friends or family members are considered as private domain users whereas all the other users are regarded as the public domain users. The users of both the private and public domain may be granted various levels of access to the PHRs by the PHR owners.

Moreover, the aforementioned users may be allowed full access to the PHRs if deemed essential by the PHR owner. In other words, the SEPHR methodology allows the patients to exercise the fine-grained access control over the PHRs. All of the users in the system are required to be registered with the SRS to receive the services of the SRS. The registration is based on the roles of the users, for instance, doc-tor, researcher, and pharmacist.

4.SYSTEMDESIGN

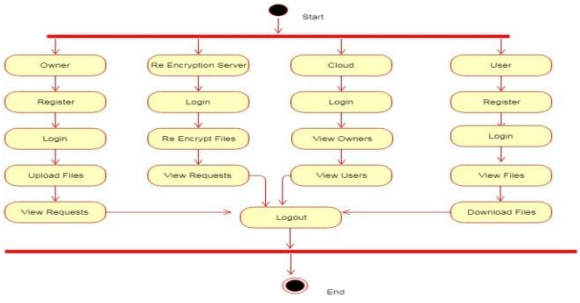

Fig 4.1: Activity Diagram

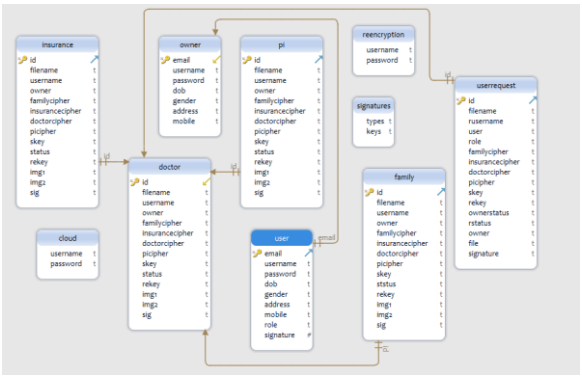

Fig 4.2: ER Diagram

5. OUTPUT SCREEN SHOTS

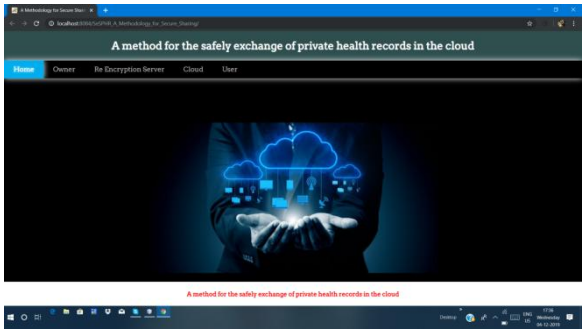

Fig 5.1:Home Page

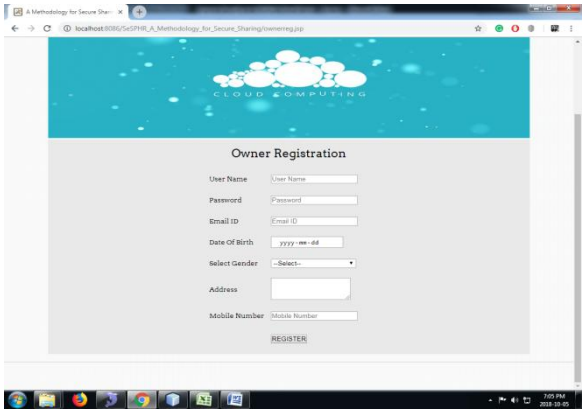

Fig5.2: Owner Registration Page

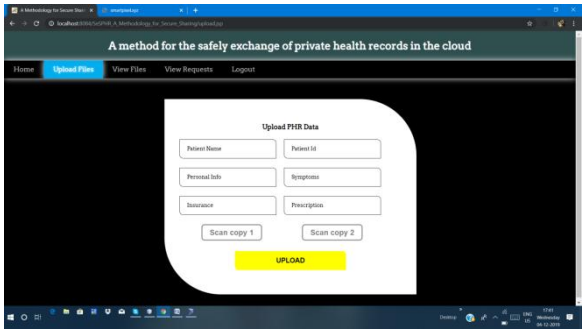

Fig5.3: Upload PHR Page

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

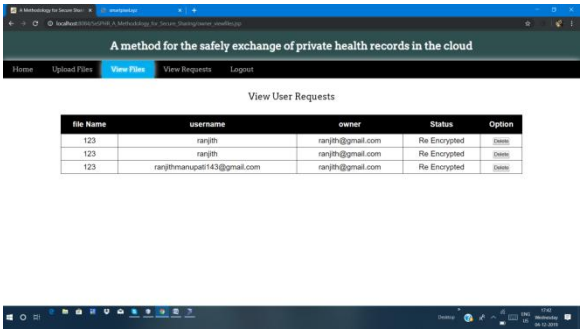

Fig5.3: View User Requests Page

6. CONCLUSION AND FUTURE ENHANCEMENT

We proposed a methodology to securely store and transmission of the PHRs to the authorized entities in the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access control to different portions of the PHRs based on the access pro-vided by the patients. We implemented a fine-grained access control method in such a way that even the valid system users cannot access those portions of the PHR for which they are not authorized. The PHR owners store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi-trusted proxy are able to decrypt the PHRs. The role of the semi-trusted proxy is to generate and store the public/private key pairs for the users in the system. In addition to preserving the confidentiality and ensuring patient-centric access control over the PHRs, the methodology also administers the forward and backward access control for departing and the newly joining users, respectively. Moreover, we formally analyzed and verified the working of SEPHR methodology through the HLPN, SMT-Lib, and the Z3 solver. The performance evaluation was done on the on the basis of time consumed to generate keys, encryption and decryption operations, and turnaround time. The experimental results exhibit the viability of the SEPHR methodology to securely share the PHRs in the cloud environment.

7. REFERENCES

[1] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in Edge-of-Things," Future Generation Computer Systems, 85, 2018, pp. 190-200.

[2] K. Gai, M. Qiu, and X. Sun, "A survey on FinTech," Journal of Network and Computer Applications, 2017, pp. 1-12.

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

[4] N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Sham-shirband, "Incremental proxy re-encryption scheme for mo-bile cloud computing environment,"The Journal of Supercom-puting,Vol. 68, No. 2, 2014, pp. 624-651.

[5] 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-

[5] A. Abbas andS. 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.

[6] 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 Comput-er and System Sciences, vol. 90, pp, 46-62, 2017.

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

[8] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "A research agenda for personal health records (PHRs)," Journal of the American Medical Informatics Association, vol.15, no. 6, 2008, pp. 729-736.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scala-ble and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9.

[10] S. Kamara and K. Lauter, "Cryptographic cloud storage," Financial Cryptography and Data Security, vol. 6054, pp. 136–149, 2010.

[11] 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.

[12] K. Gai, M. Qiu, "Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers," IEEE Transactions on Industrial Informatics, 2017, DOI: 10.1109/TII.2017.2780885..

[13] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.

[14] "Health Insurance Portability and Accountability," http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/, accessed on October 20, 2014.

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