

SeSPHR A Methodology for Secure Sharing of Personal Health Records in the Cloud

Mr. V. Kasthuraiah

¹Assistant Professor, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.

Sk. Noormahmed

² PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.

Abstract - The widespread acceptance of cloud-based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Nevertheless, storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs. Therefore, we propose a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi- trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore, we formally analyze and verify the working of SeSPHR methodology through the High Level Petri Nets (HLPN). Performance evaluation regarding time consumption indicates that the SeSPHR methodology has potential to be employed for securely sharing the PHRs in the cloud.

Key Words:: Access Control, Cloud Computing, Personal Health Records, Privacy.

1.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 consequently the cloud computing paradigm facilitates organizations by relieving them from the protected job of infrastructure development and has encouraged them to trust on the third party information technology services additionally the cloud computing model has demonstrated significant potential to increase coordination among several healthcare stakeholder and also to ensure continuous availability of health information and scalability.

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. Storing the private health information to servers managed by third parties is susceptible to unauthorized access. In particular privacy of the PHRs stored in public clouds that are managed by commercial service providers is extremely at risk the privacy of the PHRs can be at risk in several ways, for example theft, loss, and leakage the PHR 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.

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.[1]

The key contributions of the proposed work are given below:

- We present a methodology called SeSPHR that permits patients to administer the sharing of their own PHRs in the cloud.
- The SeSPHR methodology employs the El-Gamal 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 ACL for different groups of users.
- A semi-trusted proxy called SRS(Setup and Re-encryption Server) is deployed to ensure the access control and to generate the re- encryption keys for

different groups of users by eliminating the key management overhead at the PHR owner's end.

- The forward and backward access control is also implemented in the proposed methodology Formal analysis and verification of the proposed methodology is performed to validate its working according to the specifications.

2. RELATED WORK

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company Traffic Redundancy Elimination, once these things are satisfied, then next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system we have to know the below concepts for developing the proposed system

1) A new general framework for secure public key encryption with keyword search

Public Key Encryption with Keyword Search (PEKS), introduced by Boneh et al. in Eurocrypt'04, allows users to search encrypted documents on an untrusted server without revealing any information. This notion is very useful in many applications and has attracted a lot of attention by the cryptographic research community. However, one limitation of all the existing PEKS schemes is that they cannot resist the Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework named Dual- Server Public Key Encryption with Keyword Search (DS-PEKS). This new framework can withstand all the attacks, including the KGA from the two untrusted

servers, as long as they do not collude. We then present a generic construction of DS-PEKS using a new variant of the Smooth Projective Hash Functions (SPHFs), which is of independent interest.

2) Searchable symmetric encryption- Improved definitions and efficient constructions

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed

.In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions.

We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

3) Public Key Encryption with Keyword Search based on K-Resilient IBE

An encrypted email is sent from Bob to Alice. A gateway wants to check whether a certain keyword exists in an email or not for some reason (e.g. routing). Nevertheless Alice does not want the email to be decrypted by anyone except her including the gateway itself. This is a scenario where public key encryption with keyword search (PEKS) is needed. In this paper we construct a new scheme (KR-PEKS) the KResilient Public Key Encryption with Keyword Search. The new scheme is secure under a chosen keyword attack without the random oracle. The ability of constructing a Public Key Encryption with Keyword Search from an Identity Based Encryption was used in the construction of the KR-PEKS. The security of the new scheme was proved

by showing that the used IBE has a notion of key privacy

4) Generic constructions of secure-channel free searchable encryption with adaptive security

For searching keywords against encrypted data, public key encryption scheme with keyword search (PEKS), and its extension secure-channel free PEKS (SCF- PEKS), has been proposed. In this paper, we extend the security of SCF-PEKS, calling it adaptive SCF-PEKS, wherein an adversary (modeled as a “malicious-but- legitimate” receiver) is allowed to issue test queries adaptively. We show that adaptive SCF-PEKS can be generically constructed by anonymous identity-based encryption only.

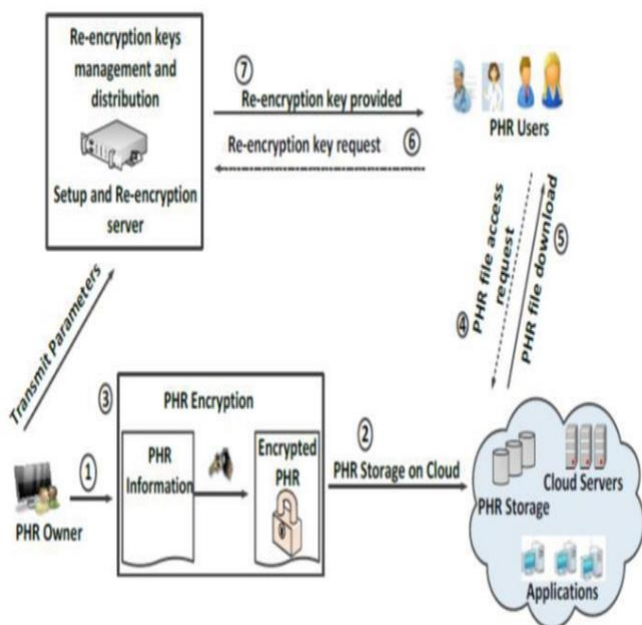
3.PROPOSED SYSTEM

The attribute based encryption algorithm first encrypt data before storing on the cloud server. In ABE there are two variants based on placing attributes and access attribute policy. Here in this research paper, we develop a model and mechanism for control of data access to PHRs stored in cloud servers. To achieve efficient and modular data access control for PHRs, we provide ABE encryption approach to encrypt each PHR file. In this system we try to focus on the multiple data owner scheme, and divide the users into security domains that highly reduce the key management complication for owners and users. In this system patient privacy is guaranteed by exploiting multi- authority.

ADVANTAGES OF PROPOSED SYSTEM:

There are only one disadvantages for the system, searching depends on the generation of keyword trapdoor, if some words generate wrong trapdoor when there is no back ground knowledge, then the system generates false positive ratio.

SYSTEM ARCHITECTURE



✚ View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

✚ PHR Owner

In this module, there are n numbers of Owners are present. Owner should register before doing any operations. Once Owner registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful Owner will do some operations like View Profile, Add Patient Details, View Patient Details, View Key Requests, and View Clinical Reports

✚ PHR User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like View Profile, Request Key, View Access Control, View Clinical Reports, and View Patient Details.

4.SYSTEM IMPLEMENTATION Module

Description:

✚ Cloud Server


In this module, the Server login by using valid user name and password. After login successful he can do some operations such as Authorize PHR User, Authorize PHR Data Owner, Clinical Report, View Patient Details, Access Control Request, Encryption Key Requests, View Key Transactions, and View Result in Chart.

5.RESULTS

host:9090/SeSPHR%20A%20Methodology%20for%20Secure%20Sharing%20of%20Personal%20Health%20Records/

SeSPHR A Methodology for Secure Sharing of Personal Health Records in the cloud

[Home](#) [Cloud Server](#) [PHR Owner](#) [PHR User](#)




Access control, cloud computing, Personal Health Records, privacy

Search our site:

Menu


- » PHR Users
- » Cloud Server
- » PHR Data Owner

Introduction



The widespread acceptance of cloud based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Nevertheless, storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs. Therefore, we propose a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and

host:9090/SeSPHR%20A%20Methodology%20for%20Secure%20Sharing%20of%20Personal%20Health%20Records/HS_Clinical_Reports.jsp



ELECTRONIC HEALTH RECORDS

Efficiency while Maintaining Patient Safety

Search our site:

Menu

- » Home
- » Logout

Clinical Reports

ID	Patient Name	Provider Name	View Report	Status
1	Ashok	Rajesh	View	Forwarded
2	Ravi	Rajesh	View	Forward To Ravi

[Back](#)

© 2022, IJSREM | www.ijrem.com

DOI: 10.55041/IJSREM15927

| Page 5

6. CONCLUSION

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 provided 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 semitrusted 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 SeSPHR methodology through the HLPN, SMT-Lib, and the Z3 solver. The performance evaluation was done on the basis of time consumed to generate keys, encryption and decryption operations, and turnaround time. The experimental results exhibit the viability of the SeSPHR methodology to securely share the PHRs in the cloud environment.

7. REFERENCES

- [1] Tambe, G. SeSPHR: A METHODOLOGY FOR SECURE SHARING OF PERSONAL HEALTH RECORDS IN THE CLOUD.
- [2] K. Gai, M. Qiu, and X. Sun, "A survey on FinTech," Journal of Network and
- [3] 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.
- [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, vols. 4344, pp. 99-109, 2015.
- [5] A. N. Khan, M. M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, "Incremental proxy re- encryption scheme for mobile cloud computing environment," The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] J. Li, "Electronic personal health records and the question of privacy," Computers, 2013, DOI: 10.1109/MC.2013.225.
- [10] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "A research agenda for personal health records (PHRs),"