IOSR Journal of Electronics & Communication Engineering (IOSR-JECE)
ISSN(e) : 2278-1684 ISSN(p) : 2320-334X, PP 20-23
www.iosrjournals.org

Personal Health Record Management System

Sreerenjini.P.R, Devu.M
(s2 Mtech CSE,MCET,ANAD,INDIA)
(Assistant professor,MCET,ANAD,INDIA)

Abstract
Personal Health Record Management system is a patient centric model which utilizes the myriad applications of cloud computing .It utilizes the RSA algorithm to encrypt the Health records and is stored in the cloud server. Here the health data of a patient is maintained by himself. These health records are very much different from the ordinary electronic medical records maintained by hospitals. During the last few years, there has been an increased number of applications that have "migrated to the cloud",and new cloud-based applications have become popular.

Keywords: PHRMS, PHR,cloud computing,RSA encryption,SAAS,HAAS,PAAS

I. Introduction

Personal Health record management system(PHRMS) is a patient centric model for exchanging health information in a secured way. PHRMS allows a patient to create, manage, and control his personal health data in one place through the web .This will make the storage, retrieval,and sharing of the the medical information more efficient. Each patient has full control of his medical records and can share his health information with a wide range of users, including healthcare providers, family members or friends. Each patient has full control over his health record. The cost of building and maintaining specialized data centers for storing PHR by third-party service providers were very high. This overhead was greatly reduced by the advent of cloud computing techniques.

II. Problem definition

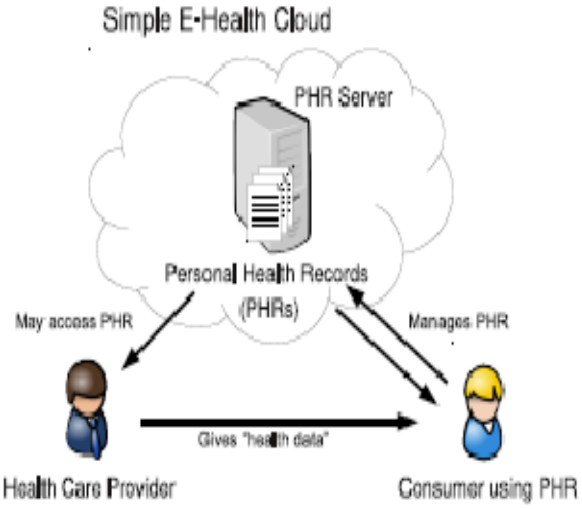
A PHR system is considered where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central cloud server belonging to the PHR service provider that stores all the PHRs of registered users. Users may be for example, a friend, a caregiver or a researcher. They may access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. However, the goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. We refer to the two categories of users as *personal* and *professional* users, respectively. The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be overwhelmed by the key management overhead. In addition, since those users' access requests are generally unpredictable, it is difficult for an owner to determine a list of them. The security and performance requirements are summarized as follows:

• *Data confidentiality*. Users who are unauthorized do not possess proper key access privileges should be prevented from decrypting a PHR document, even under user collusion.

• *On-demand revocation.* Whenever a user is no longer valid, the user should not be able to access PHR files using that userid. This is usually called *attribute- revocation*, and the corresponding security property is forward secrecy. There is also *user- revocation*, where all of the user's access privileges will be revoked.

• *Write access control*. The unauthorized users are prevented from gaining write-access to owners' PHRs, while the legitimate users can access the server with accountability. The data access policies should be flexible. Dynamic changes are allowed to the predefined policies, the PHRs should be accessible under emergency scenarios.

• *Scalability, efficiency and usability*. The PHR systems support users from both the personal domain and public domains. The set of users from the public domain may be large in size and unpredictable, the system should be highly scalable,in terms of complexity in key management, communication ,computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability



.

III. Cloud computing

Cloud provides services in a pay as u go manner,ie services are rented to registered users and they have to pay for these services. There are three types of services associated with cloud
1.Software as a service(SAAS): Software is provided as a service to authorized user.
2.Hardware as a service(HAAS): Hardware is provided as a service to authorized users.
3.Platform as a service(PAAS):Operating system is provided as a service to authorized users.

IV. RSA ALGORITHM

It is a Public key encryption algorithm introduced in 1978 by Rivest, Shamir and Adleman.In this algorithm no serious flaws were found.It uses number theory and large prime numbers.P = $D(k_{PRIV}, E(k_{PUB}, P))$ = $D(k_{PUB}, E(k_{PRIV}, P))$ where the two keys are interchangeable.

Two large prime numbers are picked (assume p=17, q=11) which are kept secret Multiply $N = p*q$ = 187 and select e such that e and (p-1)*(q-1) are relatively prime, e.g. e= 7 Publish the public key: e and N . The public key is used to encrypt message M (in numeric form) to ciphertext C ie,$C = M^e \pmod N$ [ex. M = X ($1011000_2 = 88_{10}$) $C = 88^7 \pmod{187} = 59{,}977{,}368 \pmod{187} = 11$. 11 is the encrypted message to be sent. Since receiver knows p and q, he can calculate the private key (d) $e \times d = 1 \pmod{(p-1)*(q-1)}$ ie, $7 * d = 1 \pmod{16*10}$ d = 23 Receiver decrypts the message C using $M = C^d \pmod{187}$ $M = 11^{23} \pmod{187} = 88$ (which is ASCII for X).

V. PHRMS Framework

The main goal of our framework is to provide securepatient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains

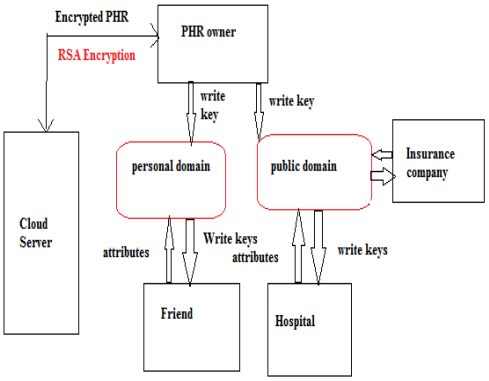


Fig 1. PHRMS Framework

The System consists of five modules:

1.PHRMS
2.PHR
3.Hospital
4.Insurance company
5.Friend

PHRMS is the service provider which provides services to other modules ,which access services and pay for it. Each of the service user has to register on PHRMS and attain their access writes. For security reasons each of the personal health records are encrypted and stored in the server.

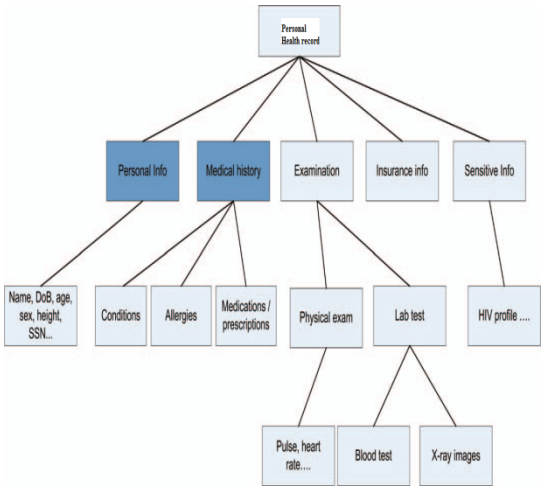


Fig 2.PHR file hierarchy

The security domains include personal domain and public domains.

We first consider a simple model that underlies commercial systems like Google Health[6], Microsoft HealthVault[7], and ICW LifeSensor[8]. In these systems patients store their own health-related data on certain web servers: the Personal Health Record (PHR). In this model, patients track, collect, and manage the information about their health at online web sites. They can enter dates and periods of sickness, their appointments with doctors, and any other data related to their health. Patients can also import data in their PHRs they get from health professionals, such as x-ray photos or laboratory tests from their family doctor or dentist. The PHRs are stored on a server of a third party in the cloud. The PHR server provider is responsible for ensuring data protection. Typically, patients can provide role-based access rights for individual health professionals. For example, full access to their family doctor, but only restricted access to some data to their fitness trainer or health coach. The advantages of such an approach are that the PHR is accessible from everywhere because of the centralized management (IT outsourcing). The patient can easily give one doctor access to data and test results that were determined by another doctor, when the data is stored.[3] in the PHR. This can help to avoid double examination. Moreover, due to the individual management of PHRs by the patients, it is expected that people are more aware of their own health. This could reduce the healthcare costs in the long term as well. However, from a technical perspective this model has a great disadvantage regarding patients' privacy. On the one hand, patients need to manage complex access rights and need to understand their implications. On the other hand, they need to rely on the robustness and correctness of the security mechanisms implemented at the PHR server provider. In general, it may be possible for the server provider to gain access to the data stored in PHRs.

VI. Conclusion

This paper suggests a secure way to exchange health record information using cloud computing. This greatly reduces the overhead of storage and thus reduces the cost. In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing.Considering partially trustworthy cloud servers, we argue to fully realize the patient-centric concept, patients shall have complete control of their own PHR through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works.

VII. References

1. Scalable and Secure Sharing of Personal Health Records in Cloud by Ming Li *Member, IEEE,* Shucheng Yu, *Member, IEEE,* Yao Zheng, *Student Member, IEEE,* Kui Ren, *SeniorMember, IEEE,* and Wenjing Lou, *Senior Member, IEEE*
2. M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained dataaccess control in multi-owner settings," in *SecureComm'10*, Sept.2010, pp. 89–106.
3. H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-healthcloud," in *Proceedings of the 1st ACM International Health InformaticsSymposium*, ser. IHI '10, 2010, pp. 220–229.
4. M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in *ICDCS '11*, Jun. 2011.
5. "The health insurance portability andaccountability act." [Online]. Available:http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp
6. www.lifesensor.com
7. www.healthvault.com