International Journal of Modern Computer Science (IJMCS)
Volume 5, Issue 3, June, 2017
ISSN: 2320-7868 (Online)

A Framework for Privacy Aware Patient-Controlled Personal Health Record System

Umamageswari Baskaran
Assistant Professor
Dept. of Information Technology
New Prince Shri Bhavani College of Engineering and Technology
Chennai, Tamil Nadu, India
umamage@gmail.com

Abstract - With the development of medical technology and information technology,"Personal Health Records (PHR)" is gradually developed as medical information exchange system. Patient - controlled personal health record systems helps to make health care -safer, cheaper, and more convenient. In this paper, we present the framework for Privacy-aware Patient-controlled Personal Health Record (P3HR) system through which a patient can view their health history, and share their health information with health care professional. Access to the health information of a particular patient is completely controlled by that patient. In P3HR database, no quasi identifiers are stored and it uses secret pseudonym for linking records, which is known only to the respective patients. The resulting database becomes completely anonymous. Our approach makes it very unlikely that patients could be identified by an attacker from their anonymous health records in the P3HR system.

Keywords — Cloud storage, Patient Health Record, quasi identifiers, pseudonym.

I. INTRODUCTION

The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet based on user demand. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications.

Electronic form of personal health records is both a problem and an opportunity. It opens new kind of threats to information leakage because electronic data are easy to copy. For every healthcare center, there are separate systems to record patients' health information.

Each time a patient visits a new healthcare center, they may need to request for old health records from several previously visited healthcare centers, which is a time consuming and tedious job. If the patients can have full control over their own health records, they can share the appropriate part of their health records with appropriate caregivers when necessary. Thus, a patient-controlled health record (PCHR) system is necessary. The goal of a PCHR is to assemble the patient's complete health history and let the patient control whom to give access to his information.

In P3HR database, no quasi-identifiers are stored and it uses secret pseudonym for linking records with their respective patients. The relationship between a patient and her pseudonym is known only to the patient. A patient lets healthcare professionals access her anonymous health records without revealing her secret pseudonym. Even if the records are exposed to unauthorized parties it is very unlikely that they would be able to identify the respective patients from their health records i.e., patients' privacy is preserved.

II. RELATED WORKS

Dharanya et al. proposed PHR outsourcing to the third party servers for the wide database management and for the security[5]. The third party servers are semi-trusted servers and hence it is important to provide encryption before outsource the PHR to the third party servers. Here they proposed Attribute Based Encryption (ABE) technique for the personal health records stored in the semi-trusted servers. ABE is used to enable fine-grained and scalable access control for PHRs. To reduce the key distribution complexity, they divide the system into multiple security domains, where each domain manages only a subset of the users.

Chia-Hui Liu et al. proposed a proper patient-centered PHR system [1] to offer correct and complete personal health and medical summary through the Internet under the demands of privacy and security, and integrate personal medical information from different sources. With the appearance of Cloud computing, a secure protection scheme is required to encrypt the medical records of each patient for storing personal health records into Cloud server. Therefore, they proposed a new PHR access control scheme based on Lagrange interpolation polynomial under Cloud computing environments. This proposed scheme provides legitimate authorities to access to PHR, and dynamically supports multi-users in Cloud computing environments with personal privacy.

Kim et al. proposed evaluation critetria for measuring the functionality and utility of PHRs[2].

Maha TEBAA et al. proposed Cloud computing security challenges [3] and it's also an issue to many researchers; first priority was to focus on security which is the biggest concern of organizations that are considering a move to the cloud. When the data transferred to the Cloud they use standard encryption methods to secure the operations and the storage of the data. But to process data located on a remote server, the Cloud providers need to access the raw data. They have proposed an application of a method to execute operations on encrypted data without decrypting them which will provide us with the same results after calculations as if they have worked directly on the raw data.

Ming et al. proposed a system for scalable and secured sharing of PHRs in a cloud environment by using Attribute Based Encryption [4].

 ISSN: 2320-7868 (Online)

Shaheen Taj et al. explains the development in the field of PHR[7] and makes an attempt to modify the conventional approach of securing PHR. Here, PHR's are stored anonymously i.e without any identifier. Therefore, it is impossible for third party to identify the PHRs.

Schartner et al. proposed an approach for anonymization of PHRs by using user generated pseudonyms [6].

III. PROPOSED ARCHITECTURE

The architecture of the proposed system is shown in Figure1.

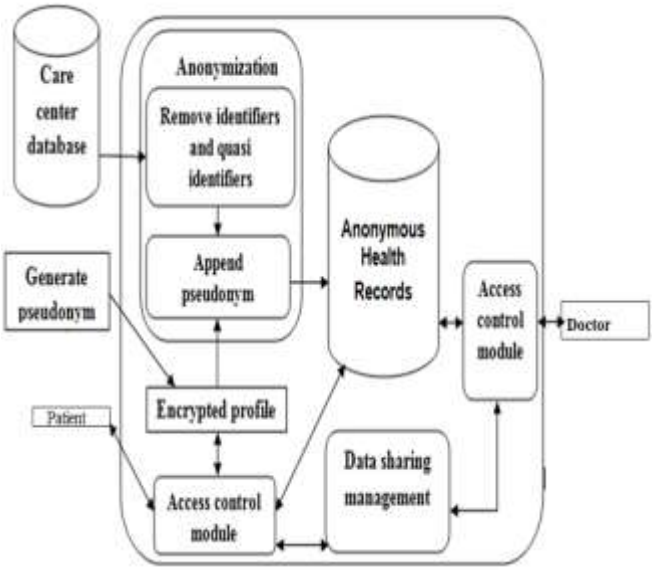

Figure. 1 Proposed System Architecture

Patient - controlled Personal Health Record System helps to make health care -safer, cheaper, and more convenient. Access to the health information of a particular patient is completely controlled by that patient. In P3HR database, no quasi identifiers are stored and it uses secret pseudonym for linking records, which is known only to the respective patients. The resulting database becomes completely anonymous. Our approach makes it very unlikely that patients could be identified by an attacker from their anonymous health records in the P3HR system.

IV. PROPOSED SYSTEM

Our proposed algorithm has four modules:

- Anonymization module.
- Encryption and Data Storage.
- PHR retrieval.
- Privacy control module.

A. Anonymization module:

The anonymization module removes all identifiers and quasi-identifiers from the records so that a particular record cannot be associated with specific identifiable individuals.

Input: Health record of a patient.
Output: Anonymous form of health record.
Algorithm:
Step 1: Patient select record to upload.
Step 2: The uploaded record is read using "PdfReader".
Step 3: If the identifiers in the uploaded record matches to the patient profile then it removes the identifiers from record.
Step 4: An unique pseudonym is created using patient details.
Step 4.1: Data from patient details are stored in an ArrayList. Using RANDOM function the pseudonym is created randomly.
Step 5: The pseudonym is appended with the record and stored in database anonymously.

B. Encryption and Data Storage:

For providing general personal information conveniently to newly visited centers, P3HR system allows a patient to store her profile, consisting of general identifiable information, encrypted with a shared key.

Input: Basic profile.
Output: Encrypted profile.
Algorithm:
Step 1: After the basic details are collected, they are encrypted using the Advanced Encryption standard using the below method,
AES_ENCRYPT('"+puser+"','"+key+"')
Step2: Encrypted profile is stored in the database. And also the basic profile will be viewed in encrypted form.
Step 3: To view the decrypted profile, patient should get the key from the mail.
Step 4: Then the basic profile is decrypted using the key and viewed.

C. PHR retrieval:

There are separate access control modules for patients and healthcare professionals. Each patient and health care professional who wants to use the system needs to register into the system. In the registration process of doctors, their true identity is verified by external means.

Input: Details are collected from user, hospital and doctor for registration.
Output: Access to their respective profile.
Algorithm:
Patient login:
Step 1: Account for patient is created and stored in database.
Step 1.1: Patient can view her encrypted profile by giving a key.
Hospital login:
Step 2: In hospital login, the respective hospitals acts has an admin.
Step 2.1: The admin adds the doctor in the hospital.
Step 2.2: The admin can view and delete the doctors.

Doctor login:
Step 3: Doctor is allowed to create an account only if hospital admin adds the doctor.
Step 3.1: The doctor can view shared record sent by the patient.
Step 3.2: The doctor can send the appointment to patient.

D. Privacy Control Module

Data sharing management allows a patient to select health care professionals (based on individual or role) for granting access to her selected health records. The patient can also specify specific time duration for which the shared data would be accessible to the selected healthcare professional.

Input: Health record of patient.
Output: List of shared data.
Algorithm:
Step 1: Patient select the doctor and he can set the duration for how long the doctor can view the patient records.
Step 2: Patient can select the respective fields or records and send to doctor.
Step 3: The doctor can view only the selected fields or records sent by the patient.
Step 4: If the duration has been expired, the doctor cannot view the patients shared record.

E. Implementation

Implementation of proposed system is done using J2EE and MS-SQL is used as back-end.

V. CONCLUSION & FUTURE WORK

In P3HR system, the stored data is made anonymous so that an intruder cannot associate a record with a specific individual. We use secret pseudonym that is known only to the respective patient. The advantage of our system is that our stored database becomes most likely completely anonymous and it is highly unlikely that the data subject could be identified from the stored records. Thus, our system allows patients to have control over their health records which in turn helps makes health care safer, cheaper, and more convenient. Most of all, it supports the necessary functionalities for current healthcare industry with a complete privacy protection mechanism for patients.

In future, we try to provide Smart cards with strong authentication. The embedded chip of a smart card usually implements some cryptographic algorithm. Each patient is issued a personalized smart IC card which stores patients profile information in encrypted form. Also, healthcare providers are issued Healthcare Professional Cards. Card readers (installed at healthcare centers) can decrypt and read the information from a card.

REFERENCES

[1] Chia-Hui Liu, Tzer-Long Chen (2013). Secure PHR Access Control Scheme in Cloud Computing, Han-Yu Lin, Fong-Qi Lin, Chih-Ming Liu, En-Ping Wu, Yu-Fang Chung, and Tzer-Shyong Chen.

[2]Kim M. I. and Johnson K. B. (2002). Personal health records: evaluation of functionality and utility. Journal of the American Medical Informatics Association, Vol. 9(2), 171–180.

[3] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI (2012). Homomorphic Encryption Applied to the Cloud Computing Security.

[4] Ming Li Member, IEEE, Shucheng Yu (2012). Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE.

[5] S.Dharanya and D.Indira priyadharshini (2013).Achieving Secure Personal Health Records Using Multiple-Authority Attribute Based Encryption.

[6] Schartner P; and Schaffer M. (2005). Unique user-generated digital pseudonyms. Springer LNC ,Vol. 3685, 194-205.

[7] Shaheen Taj S.A, Prathibha Kiran and Elavarasi (2013). A Novel Method for Patient Centric Secure and Scalable sharing of PHR in Cloud Computing using Encryption.