Secure Sharing of Personal Health Records in Cloud computing using Smart card

Wagh Rohini H. 1, Pimparkar Vrushali S. 2, Pawar Pratiksha S. 3, Avhad Sonali S. 4, Prof. Kapadnis Jagdish Y. 5

1,2,3,4 Department of Computer Engineering, Pune Vidyarthi Griha’s College of Engineering, Nashik-422004, Pune, India.

Abstract: Personal Health Record (PHR) model is used to securely share the health information of the patient which is provided by or outsource to the cloud provide i.e. parse cloud. PHR allows a patient to create, maintain, deletes and controls his/ her personal health information on cloud and only authorized person can access it. To assure the patient’s control over access to their own PHR’s encrypt the health information before outsourcing. Multi-authority Attribute Based Encryption (MA-ABE) is used to encrypt each patient’s health record which result in assured Patient privacy. Our system based on the multiple data owner scenario, and divides the users in the PHR system into multiple security domains. User can make the different access based on the professional roles such as doctor, nurses and medical researchers. In this system, we are also using the smart card on which QR code is mounted. Only authorized person have rights to access the PHR's of the person by scanning the QR code depending on their professional role.

Keywords: personal health records, MA-ABE, parse cloud, secure sharing, QR code, smart card

1. Introduction

In the case of emergency, doctor does not know how to treat the patient. Sometimes patient have some allergies, diseases, medications hence it is difficult for doctor to give proper treatment to that patient. To solve this problem we develop the system in which we provide the smart card to the patient. By using this smart card doctor easily gets the health information of patient and able to give the proper treatment to that patient. Personal Health record contains the personal information, medical history, examination, Insurance information etc.

Personal Health Record (PHR) is a patient-centric model for exchange the health information of the patient which is outsource to or provided by the cloud provide i.e. parse cloud. PHR system allows a patient to create, maintain, delete and control his/ her personal health information on cloud which has been made the retrieval, storage and sharing of the medical information more efficient. Each patient have full control of his or her medical records and can share his other health data with broad range of users, including healthcare providers, friends, doctors or family members. To assure the patient’s control over access to their own PHR’s encrypt the health information before outsourcing. Multi Authority Attribute Based Encryption (MA-ABE) is used to encrypt each patient’s health record which result in assured Patient privacy. In this encryption scheme, each user is identified by the unique identity. An attribute based encryption scheme (ABE), in contrast, is a scheme in which each user is identified by the set of attributes, and some function of those attributes is used to establish decryption capability for each ciphertext. Patient privacy is maintained and guaranteed by using multi-authority ABE.

Our system based on the multiple data owner scenario, and divides the users in the PHR system into multiple security domains. User can make the different access based on the professional roles such as doctor, nurses and medical researchers. In this system, we are using the smart card on which QR code is mounted. Only authorized person have rights to access the PHR's of the person by scanning the QR code based on their professional role.

The system focuses on secure and scalable sharing of user’s health records in a multi-owner environment on the parse cloud. The system is divided into two domains i.e. public and personal domain e.g. family members and friends in personal domain, similarly medical, doctors, researchers and pharmacists in the public domain. This type of arrangement helps in easy key management. This system also supports write access control, policy updates and expert handling of emergency cases.
Multi-authority Attribute Based Encryption (MA-ABE) is used in the public domain. MA-ABE uses the concept of Attribute Authority (AA) which controls the role attributes of the different types of user [5]. In the personal domain, an owner is capable of granting access rights to the users to encrypt PHR file under its data attributes. This helps in resolving the traditional key management problems for large systems.

2. Existing system

In this system the health information is stored on the third party server. There is no encryption and decryption of health information hence there is possibility of personal health information could be uncovered to unauthorized parties and third party servers. PHR contain the sensitive personal health information (PHI). People may not fully trust when they are stored on a third-party server. Also there is chance of someone can access the personal health information without authorization.

As a well-known incident, a department of veteran’s affairs database containing sensitive PHI of 26.5 million military veterans. This PHI includes their social security numbers and health problems. This information was stolen by a worker who took the data home without authorization.

Drawback of existing system:

1. Single owner system, in which no policy management for file access. Adding the categories is not possible hence confidential information is also accessed by all types of users.
2. There is no encryption and decryption so attackers easily access the personal information. The PHR file stored in the semi trusted server or cloud can able to disclose the sensitive information to others.
3. There is no structured way to access the health information for personal professional purpose.

3. Proposed system

Personal Health Record (PHR) is the patient-centric model which can be used to exchange the health information which is outsourced to or provided by the third party service provider i.e. parse cloud. Parse handles everything you need to store data securely and efficiently in the cloud. Parse platform provides a complete backend solution for your mobile application. The main goal of parse cloud is to totally eliminate the need for writing server side or maintaining servers.

PHR allows a patient to create, maintain, deletes his/her personal health information on cloud and only authorized person can access it. Sometime doctor also permit to update the patients health record. To assure the patient’s control over access to their own PHR’s, MA-ABE method to encrypt the PHR’s before outsourcing. Multi Authority- Attribute Based Encryption (MA-ABE) is used to encrypt each patient’s PHR file which result in assured Patient privacy. User can get the information of patient based on predefined access policies.

We focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains such as public domain and private domain. User can make the different access based on the professional roles such as doctor, nurses, insurance agent, emergency department and medical researchers. In this system we are providing the smart card to each person/patient on which QR code is mounted. QR codes nothing but the Quick Response. Since the QR Code is an open code that anyone is allowed to use, it is used in countries all over the world. QR codes can be used to link directly to a URL, by scanning the QR code user automatically redirect to the webpage where owners information is stored. User can access the patient’s PHR depend on the professional roles. Basically, the PHR owner should decide how to encrypt its own files and to allow which set of users to obtain access to each file.

4. Sharing of personal health records in the secure and scalable manner by using semi trusted cloud. As cloud considered here is moderately trustworthy
patient data privacy is guarded by encrypting the data before outsourcing. [9]

5. System Architecture

In this system architecture PHR’s stored on the parse cloud and can be access through the application by the wide range of owner and user. The patient is considered as owner of the system. The system is responsible for creating the access policies based on the user’s professional role. Owner may be doctor, emergency department, insurance agent, friend, family member etc.

At the first time receptionists fill up the information of the patient on the system. Patient’s health information is stored on cloud in the encrypted format then system will generate the QR code. That QR code is mounted on the smart card. After that at any moment owner can update the record. Doctor also has authority to update the health information of the owner i.e. patient. When user scans the QR code then the information is decrypted using the key. The valid information is provided to the user based on predefined access policies. Then user can access information of patient and treat to that patient.

5.1 Working of system:

Firstly, Owner fills the information on the system. The information is encrypted and stored on the parse cloud. Then system generates the QR code, mount it on smart card. Then smart card gives to the owner. When owner wants to update his/her health record then scan the QR code on his/her smart card. Login into the system and update the information. This information is encrypted and stored on the cloud. User scans the QR code. If user is valid then based on role the information is provided to the user. Else information is remains confidential.

6. Conclusion

This system is based on the multiple data owner scenario, and divides the users in the PHR system into multiple security domains. Different user may access the owner’s health information based on their role. The information is encrypted before storing on the parse cloud so the information is more secured and easily accessible. Only authorized person can access the patients information by scanning the QR Code mounted on smart card.

References


