# Patient–Centric Secure Data Sharing Framework for Systems

V. S. Sakharkar, K.S. Muzumdar, A.B. Pahurkar, P.P. Kadu

**Abstract**— A personal Health Record (PHR) contains the information pertinent to a patient's health. It allows a patient to make, handle, and organize his/her personal health data in one place through the web. Each patient has assured the full control of his/her personal health records. It is shared with wide range of users, such as healthcare providers, relatives or friends. Personal health information (PHI) is stored on a third-party server; the main concern is about the control of sharing of their personal information .On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates [3], cloud providers are usually not covered entities [4]. A feasible and promising approach would be to encrypt the data before outsourcing. A PHR file is given to the users who possess corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary [11].

**Index Terms**— PHI, EMR

## 1 Introduction

Now-a-days, a patient may have many medical providers which includes primary care physicians, specialists, therapists, and other medical practitioners. Currently, each provider typically has its own database for electronic medical records (EMRs).The success of tapping healthcare into the cloud is the in-depth understanding the effective enforcement of security and privacy in cloud computing. But as the maintenance cost of specialized data centers is too high, many PHR services are outsourced to or provided by third-party service providers.

## 2 Related work

Over the last few years research on the various security issues surrounding healthcare information systems has been heated. ISO/TS 18308 standard gives the definitions of security and privacy issue for EHR [5].

To investigate the issues of data protection and security within the healthcare environment a Working Group 4 of International Medical Informatics Association (IMIA) was set up. Its work to date has mainly concentrated on security in EHR networked systems and common security solutions for communicating patient data [6].

A project is initiated to address a wide spectr um of security issues within Healthcare by the European AIM/SEISMED (Advanced Informatics in Medicine/Secure Environment for Information Systems in Medicine). It also provides practical guidelines for secure healthcare establishment [7],[8] ,[9]. A report on personal health records (PHRs) was published, aiming at developing PHRs and PHR systems to put forward a vision that "would create a personal health record that patients, doctors and other health care providers could securely access through the Internet no matter where a patient is seeking medical care." They present an overview of the security and privacy issues in the PHR cloud, including the models and requirements for secure access of PHR data in clouds. We must argue that security and privacy protection of cross-institutional electronic patient records is of paramount importance.

There are three principles which are critical for ensuring privacy of patients and the content authenticity and source verifiability of electronic medical records. First, all electronic medical records, be it PHR or EHR or EMR, should be guarded through ownership controlled encryption, enabling secure storage, transmission, and access. Second, the creation and maintenance of PHRs should preserve not only content authenticity but also data integrity and customizable patient privacy throughout the PHR integration process. Third but not the least, the access and sharing of PHRs should provide end-to-end source verification through signatures and certification process against blind subpoena and unauthorized change in healthcare critical data content and user agreements.
.

## 3 Existing System

This system of PHR system model contains *multiple owners* who may encrypt according to their own ways, possibly using various cryptographic keys to allow each user obtain keys from every owner.

An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority (i.e., cause the key escrow problem).Key escrow is an arrangement in which the keys are used to decrypt encrypted data under certain circumstances, an authorized third party may gain access to those keys.

These third parties may include businesses, who may want access to employees' private communications, of encrypted communications.

## 4 PROPOSED SYSTEM

In PHR system the patient refers to the owners who have full control over their own PHR data. A central server belonging to the PHR service stores all the owners' PHRs. A typical PHR system uses standard data formats. The server is considered to be semi trusted, i.e., honest but curious as those in [20] and [18]. That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. To achieve "patient-centric" PHR sharing, a core requirement is authorized patient to access to her own PHR documents. The security and performance requirements can be ummarized as follows [21]:

### 4.1 Data Confidentiality

Unauthorized users (including the server) who do not possess sufficient attributes to satisfy the access policy or do not possess proper key access privileges should be prevented from decrypting a PHR document, even under user collusion.

### 4.2 On-Demand Revocation

Whenever a user's attribute is no longer valid, the future PHR files are inaccessible using that attribute.

### 4.3 Write Access Control

We have to protect unauthorized gain write-access to owners' PHRs, while the legitimate contributors should access the server with accountability.

### 4.4 Scalability, Efficiency, and Usability:

The set of users from the public domain may be large in size and unpredictable in key management, communication, computation and storage. The data access policies should be supple, i.e., dynamic changes to the predefined policies shall be allowed.

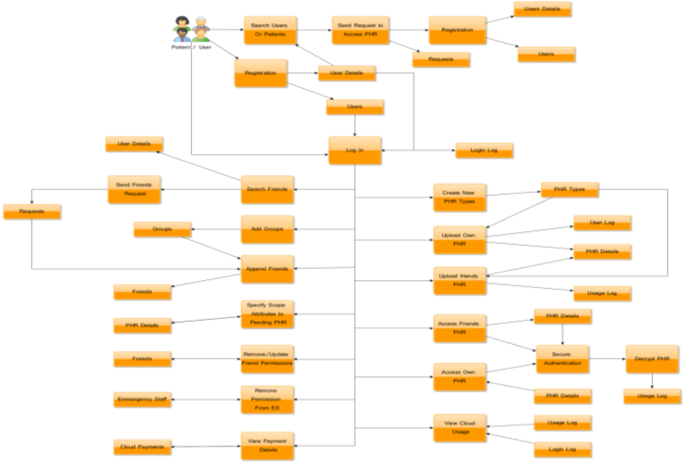

**Figure 1 Data Flow Diagram for Users**

## 5 ADVANTAGES

- Quickly find out information of patient details.
- In case of emergency doctor and other emergency department quickly get all the helpful details and start treatment.
- If in any condition doctors and medical facilities are unavailable the PHR owner itself able to take care of his health.
- To provide easy and faster access information.
- To provide user friendly environment.
- To provide data confidentiality and write access control.
- Reduces the key management complexity for owners and users.

## 6 APPLICATIONS

- Health care website
- Hospital management
- Any organization can store their employee's medical information by using this application.

## 7 CONCLUSIONS

In this paper, This system has application like Quickly finding out the information of patient details, in case of emergency doctor and other emergency department can quickly get all the informative details and start treatment, It also addresses the unique challenges brought by multiple PHR owners in which we can reduce the complexity of key management while enhance the privacy guarantees. We make use of ABE to encrypt the PHR data, so that patients can allow access by personal users, various users from public domains with different professional roles, qualifications and affiliations. We show that so our solution is both scalable and efficient in implementation and simulation.

## REFERENCES

[1] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[2] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[3] "The Health Insurance Portability and Accountability Act", 2012.

[4] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[5] ANSI, ISO/TS 18308 Health Informatics- Requirements for an Electronic Health Record Architecture, ISO 2003.

[6] R. Bakker, B. Barber, R. Tervo - Pellikka, A. Treacher, (eds.), Communicating Health Information in an Insecure World, in:

Proceedings of the Helsinki Working Conference.43:1, 1995. 2.

[7] B. Barber, D. Garwood, P. Skerman, In: Security in Hospital Information Systems, Security and data protection programme presented at the IMIA WH10 Working conference, Durham. 1994.

[8] S. M. Furnell, P.W. Sanders, Security management in the health-care environment, in: R.A. Greenes, H.E. Peterson, D.J. Protti, (eds.), MEDINFO '95, Proceedings of the eighth World Congress on Medical Informatics. Canada. p. 675– 678.

[9] A. Patel, I. Kantzavelou, Implementing network security guidelines in health-care information systems. In: MEDINFO '95. Proceedings of the eighth World Congress on Medical Informatics. Vancouver Trade and Convention Centre, Canada. p. 671–674.