IPHV2I10009X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

PERSONAL HEALTH RECORD SHARING IN CLOUD BY IMPLEMENTING ATTRIBUTE-BASED ENCRYPTION

Sunakara Deepthi[1], M.Anjan Kumar[2]

[1]Pursuing M.Tech, Department of Computer Science, Vivekananda Institute of Technology

[2]Assistant Professor, Department of Computer Science, Vivekananda Institute of Technology

ABSTRACT:

Personal health record (PHR) is an electronic medical record of a patient which are accessed online . these patient-centric model of health information are outsourced to be stored at a third party, such as cloud providers. The data are exchanged over the network , we must add the security to the out sourced data[1] (PHRs). The issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

Key words: security, cloud, data exchange , encryption, personal health records

INTRODUCTION

The concept of **attribute based encryption** was introduce by Amit Sahai and Brent Waters in 2004.[1] It is a type of public-key encryption in which the public key of a user and the ciphertext are dependent about attributes (e.g. the country he lives, the kind of subscription he has, ...). In a such system, The decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.

Attribute based encryption can be used for log encryption.[2] Instead of encrypting each part of a log with all the key of all the recipients, it is possible to encrypt the log only with attributes which match recipients attributes. This primitive can also be used for broadcast encryption in order to decrease the number of key used.[3]

PERSONAL HEALTH RECORD

A **personal health record**, or PHR[2], is a health record where health data and information related to the care of a patient is maintained by the patient.[1] This stands in contrast with the more widely used electronic medical record, which is operated by institutions (such as a hospital) and contains data entered by clinicians or billing data to support insurance claims. The intention

of a PHR is to provide a complete and accurate summary of an individual's medical history which is accessible online. The health data on a PHR might include patient-reported outcome data, lab results, data from devices such as wireless electronic weighing scales or collected passively from a smartphone.

The term "personal health record" is not new. The earliest mention of the term was in an article indexed by PubMed dated June 1978,[2] and even earlier in 1956 reference is made to a personal health log.[3] However, most scientific articles written about PHRs have been published since 2000.

The term "PHR" has been applied to both paper-based and computerized systems; current usage usually implies an electronic application used to collect and store health data. In recent years, several formal definitions of the term have been proposed by various organizations.[4][5][6]

It is important to note that PHRs are not the same as electronic health records (EHRs). The latter are software systems designed for use by health care providers. Like the data recorded in paper-based medical records, the data in EHRs are legally mandated notes on the care provided by clinicians to patients. There is no legal mandate that compels a consumer or patient to store her personal health information in a PHR.

PHRs can contain a diverse range of data, including but not limited to:

- allergies and adverse drug reactions
- chronic diseases
- family history
- illnesses and hospitalizations
- imaging reports (e.g. X-ray)
- laboratory test results
- medications and dosing
- prescription record
- surgeries and other procedures
- vaccinations
- and Observations of Daily Living (ODLs)

There are two methods by which data can arrive in a PHR.[1] A patient may enter it directly, either by typing into fields or uploading/transmitting data from a file or another website. The second is when the PHR is tethered to an electronic health record, which automatically updates the PHR. Not all PHRs have the same capabilities, and individual PHRs may support one or all of these methods.[1]

In addition to storing an individual's personal health information, some PHRs provide added-value services such as drug-drug interaction checking, electronic messaging between patients and providers, managing appointments, and reminders.[7]

PHRs grant patients access to a wide range of health information sources, best medical practices and health knowledge. All of an individual's medical records are stored in one place instead of paper-based files in various doctors' offices. Upon encountering a medical condition, a patient's health information is only a few clicks away.

Moreover, PHRs can benefit clinicians. PHRs offer patients the opportunity to submit their data to their clinicians' EHRs. This helps clinicians make better treatment decisions by providing more continuous data

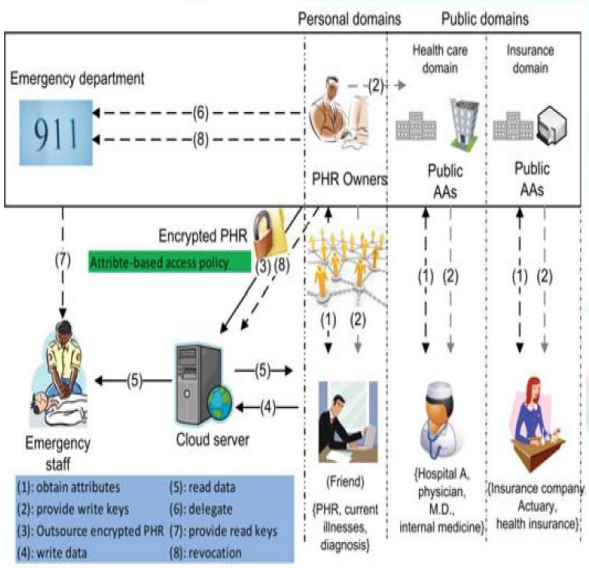
PHR benefits

PHRs have the potential to help analyze an individual's health profile and identify health threats and improvement opportunities based on an analysis of drug interaction, current best medical practices, gaps in current medical care plans, and identification of medical errors. Patient illnesses can be tracked in conjunction with healthcare providers and early interventions can be promoted upon encountering deviation of health status. PHRs also make it easier for

IPHV2I10009X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

clinicians to care for their patients by facilitating continuous communication as opposed to episodic. Eliminating communication barriers and allowing documentation flow between patients and clinicians in a timely fashion can save time consumed by face-to-face meetings and telephone communication. Improved communication can also ease the process for patients and caregivers to ask questions, to set up appointments, to request refills and referrals, and to report problems. Additionally, in the case of an emergency a PHR can quickly provide critical information to proper diagnosis or treatment.

Architecture



Privacy and ethical concerns

One of the most controversial issues for PHRs is how the technology could threaten the privacy of patient information. Network computer break-ins are becoming more common,[citation needed] thus storing medical information online can cause fear of the exposure of health information to unauthorized individuals. In addition to height, weight, blood pressure and other quantitative information about a patient's physical body, medical records can reveal very sensitive information, including fertility, surgical procedures, emotional and psychological disorders, and diseases, etc. Various threats exist to patient information confidentiality, some of which are listed below:

- Accidental disclosure: During multiple electronic transfers of data to various entities, medical personnel can make innocent mistakes to cause disclosure of data.
- Insider curiosity: Medical personnel may misuse their access to patient information out of curiosity or for another purpose.
- Insider subordination: Medical personnel may leak out personal medical information for spite, profit, revenge, or other purposes.
- Uncontrolled secondary usage: Those who are granted access to patient information solely for the purpose of supporting primary care can exploit that permission for reasons not listed in the contract, such as research.
- Outsider intrusion: Former employees, network intruders, hackers, or others may access information, damage systems or disrupt operations

Unlike paper-based records that require manual control, digital health records are secured by technological tools. Rindfleisch (1997)[19] identifies three general classes of technological interventions that can improve system security:

- Deterrents – These depend on the ethical behaviour of people and include controls such as alerts, reminders and education of users. Another useful form of deterrents has been Audit Trails. The system records identity, times and circumstances of users accessing information. If system users are

aware of such a record keeping system, it will discourage them from taking ethically inappropriate actions

- Technological obstacles – These directly control the ability of a user to access information and ensure that users only access information they need to know according to their job requirements. Examples of technological obstacles include authorization, authentication, encryption, firewalls and more.

- System management precautions – This involves proactively examining the information system to ensure that known sources of vulnerability are eliminated. An example of this would be installing antivirus software in the system

Existing works:

In Existing system a PHR system model, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner who's PHR she wants to read would limit the accessibility since patients are not always online. 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 (also known as a **"fair" cryptosystem**) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, 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, or governments, who may wish to be able to view the contents of encrypted communications.

NEW THINGS:

We endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive.

Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users.

The complexities per encryption, key generation and decryption are only linear with the number of attributes involved.

Basic Usage of MA-ABE

Setup. In particular, the AAs first generate the MKs and PK using setup as in CC MA-ABE. The k-th AA defines a disjoint set of role attributes Uk, which are relatively static properties of the public users. These attributes are classified by their types, such as profession and license status, medical specialty, and affiliation where each type has multiple possible values. Basically, each
AA monitors a disjoint subset of attribute types.

APPROACHES

1. Registration

IPHV2I10009X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

2. Upload files
3. ABE for Fine-grained Data Access Control
4. Setup and Key Distribution
5. Break-glass

- Registration

In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader has access to.

Two ABE systems are involved: for each PSD the revocable KP-ABE scheme is adopted for each PUD, our proposed revocable MA-ABE scheme.

- PUD - public domains
- PSD - personal domains
- AA - attribute authority
- MA-ABE - multi-authority ABE
- KP-ABE - key policy ABE

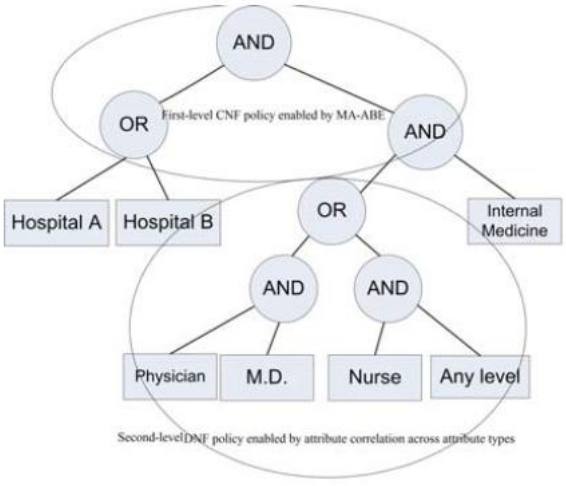


Fig. 2 An example policy realizable under our framework

using MA-ABE, following the enhanced key generation and encryption rules.

- Upload files

In this module, users upload their files with secure key probabilities. The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file encrypted both under a certain fine grained model.

- ABE for Fine-grained Data Access Control

In this module ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of un revoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.

- Setup and Key Distribution

In this module the system first defines a common universe of data attributes shared by every PSD, such as "basic profile", "medical

history", "allergies", and "prescriptions". An emergency attribute is also defined for break-glass access.

Each PHR owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-network (HSN)

There are two ways for distributing secret keys.

First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc.

Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs keygen of KP-ABE to generate the user secret key that embeds her access structure.

- Break-glass module

In this module when an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department ED to prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

CONCLUSION

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 that to fully realize the patient-centric concept, patients shall have complete control of their own privacy 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. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we
show that our solution is both scalable and efficient.

REFERENCES:

1. Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption IEEE 2012 Transactions on Parallel and Distributed Systems, Volume: PP , Issue:99
2. Attribute-based EncryptionMing Li Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior
3. The benefits of an internet-based personal health record versus a paper-based personal health record is expected to grow rapidly within the next three

years. See interview with CEO, Glen Tullman of Allscripts http://www.ehrtv.com/allscripts-glen-tullman-mar-2010/

4. http://en.wikipedia.org/wiki/Personal_health_record
5. "Computerisation of personal health records". Health visitor **51** (6): 227. Jun 1978. PMID 248054.
6. "Recordkeeping systems: personal health records". J Am Med Rec Assoc. **55** (12): 42. Dec 1984. PMID 10310901.
7. "Concepts of the Health Vault". 1999 Paper by Tom Munnecke describing an architecture for the Personal Health Record
8. "[Personal medical records and identification card, synchronized information systems] [Personal medical records and identification card, synchronized information systems]" (in French).Rev Infirm. (106): 45–6. Dec 2004. PMID 15672518.
9. Swain, M; Lawn, B (Apr 2005). "Information prescriptions (Ix): bringing internet-based health content into the treatment process; patients to your site". Internet Healthc Strateg. **7** (4): 4–8.doi:10.1016/0148-9062(76)91830-1. PMID 15929640.
10. "Report on attitudes about personal health records". Internet Healthc Strateg. **6** (9): 10–1. Sep 2004. PMID 15526437.
11. "New-age PHR comes with decision-support, multiple opportunities for DM". Dis Manag Advis. **12** (12): 140–2, 133. Dec 2006. PMID 17225631.