Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Securing the Lifelong Personal Health Data in the Cloud

Saravanan P*, Dr. T. Stephen Thangaraj Ph.D
Computer Science and Engineering
T.J. Institute of Technology
Tamil Nadu, India

Abstract— Personal Health Record system has emerged as a patient-centric model of health information exchange. A Personal Health Record service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can hare his health data with a wide range of users, including healthcare providers, family members or friends. In my proposed system, The PHR owner himself should decide how to encrypt his files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users.

Keywords— E-Health, security architecture, information flow, isolation, client platform security

I. INTRODUCTION

Storing data in the cloud has become a trend. An increasing number of clients stores their important data in remote servers in the cloud, without leaving a copy in their local computers. Sometimes the data stored in the cloud is so important that the clients must ensure it is not lost or corrupted. In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage retrieval and sharing of the medical information more efficient. But due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers. Due to the high cost of building and maintaining specialized data centers, many Personal Health Record services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing Personal Health Record in cloud computing have been proposed in. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHR owner himself should decide how to encrypt his files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users.

II. RELATED WORK

A number of works have been done to enforce the security problem on the area of Personal Health Record in Cloud Computing Environment. This section lists some of these works. The authors, proposed the problem of authorized private keyword searches (APKS) on encrypted PHR in cloud computing environments. They presented a scalable and fine-grained authorization framework for searching on encrypted PHR, where users obtain query capabilities from localized trusted authorities according to their attributes, which is highly scalable with the user scale of the system. Then they have given two solutions for APKS based on cryptographic primitive, hierarchical predicate encryption (HPE), one with enhanced efficiency and the other with enhanced query privacy. They told about the several shortcomings of current e-health solutions and standards, particularly they do not address the client platform security, which is a crucial aspect for the overall security of e-health systems. To all this they have given the security architecture for establishing privacy domains in e-health infrastructures.

To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR data. To reduce the key distribution complexity, we divide the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over their own privacy, and the key management complexity is reduced dramatically. Our solution provides client platform security and appropriately combines this with network security concepts.

III. A CLOUD-BASED PHR SYSTEM PROTOTYPE

MyPHRMachines is a prototype that leverages virtualization and remote desktop technologies to create and maintain rich and lifelong PHRs in the cloud. The prototype reuses parts of SHARE2, a mature system for making computational research results more accessible and reproducible. The key technological components have therefore already undergone various development cycles and its technical architecture is considered robust. In this section we first revisit our running example to discuss the functionality provided by my MyPHRMachines. Then, we review the main technological features embodied into our prototype. Eventually, we present the implemented use cases and discuss future developments of the prototype.

A. Running Example Revisited

Figure 1 provides a dynamic view on the MyPHRMachines architecture. In the following we clarify the architecture by means of scenarios from our running example. The top left corner of the figure shows two hospitals where PHR data is generated, for example, the RX and MRI scans discussed in Step 2 of our running example. In our example, the patient's general practitioner (GP, shown at the right) can nowadays receive a digital copy of the scan results. However, this was not the case for the first scans at the time described in Step 2 in Section 2. In order to build our example lifelong PHR, the secretary of the example patient's GP has recently contacted all the aforementioned hospitals for digital copies of the patient's scan results. As a result, the patient's GP has received digital copies of most scan interpretations and notes of the aforementioned specialists. Any Belgian patient can request nowadays a free CD copy of his radiology scans. The CDs contain image files, associated DICOM metadata as well as a Microsoft Windows-specific DICOM viewer. The companion website of this paper3 provides instructions to experiment with an example PHR consisting of some copies of such CDs. At the time of writing, the patient's GP can also directly access the PACS of some local hospitals. Problems however still arise when patients receive care from other physicians than their home GP: depending upon the region, hospitals in a different city/province/country at some point lack system integration. Using MyPHRMachines, patients can preserve their personal copy of their medical data online such that any physician (another GP or a specialist in a foreign country) can promptly access their complete PHR conveniently later. The system ensures that any type of software that happens to be needed for viewing this data can be executed transparently from a simple browser window. It should be noted that the above demo in MyPHRMachines is based on a virtual machine image that is not specific to the example patient. Instead, the image only contains Microsoft Windows. Such images are displayed at the middle right of Figure 1. MyPHRMachines ensures that when a specific patient starts a virtual machine, all of that patient's PHR data is mounted to the virtual machine behind the scenes (cfr., the arrow "mount PHR" in the figure). The DICOM example from our running example does not require specific software in the MyPHRMachines virtual machine (the CDs start their embedded DICOM viewer automatically). We envision however also the situation where insurers (or governments) provide special purpose software as a service to their customers (or citizens). MyPHRMachines supports that SaaS scenario by enabling such stakeholders to clone existing virtual machine images, install additional software and share the resulting new image to patients in a specific MyPHRMachines group. For instance, the intensive lower back revalidation program undergone by our patient has generated a large amount of data about progress in muscular strength. These data could also be stored by the patient in MyPHRMachines and the related proprietary software would be made accessible as a service via remote VMs.

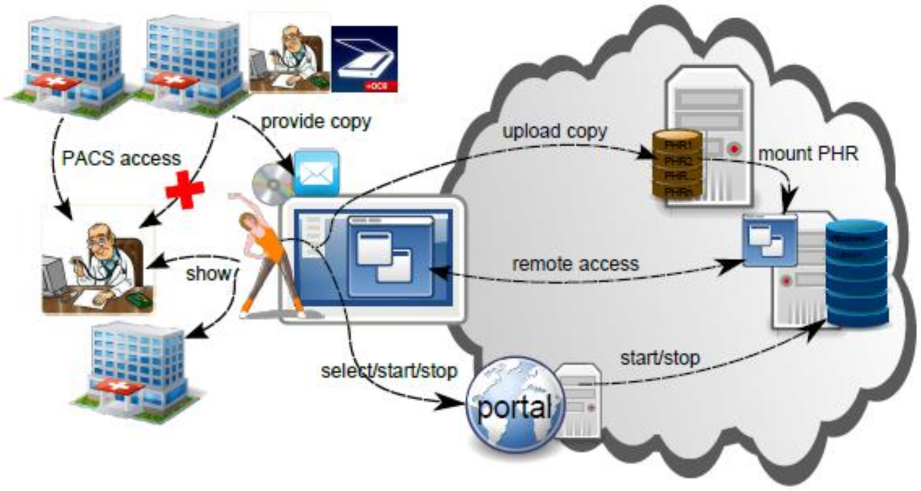

Figure 1.Archietecture for PHR in Cloud

IV. PERSONAL HEALTH RECORD FRAMEWORK

This section describes about the patient-centric secure data sharing frame work for cloud based Personal Health Record (PHR) systems.

B. Problem Definition

PHR system 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 server belonging to the PHR service provider that stores all the owners' PHRs. The users may come from various aspects; for example, a friend, Doctor, Relatives etc. Users 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.

C. Problem Definition

To achieve patient-centric PHR sharing, a core requirement is that each patient can control who are authorized to access to her own PHR documents. The security and performance requirements are as follows:

Data Confidentiality: Unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.

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

Write Access Control: The unauthorized contributors to gain write-access to owners' PHRs, while the legitimate contributors should access the server with accountability. The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenarios.

Scalability, efficiency and usability: The PHR system should support users from both the personal domain and public domains. Since 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 Owner's efforts in managing users and keys should be minimized to enjoy usability.

V. MANAGEMENT OF E-HEALTH INFRASTRUCTURE

On a larger scale, the whole infrastructure of an e-health cloud has several risks that threaten the privacy of health data. Both medical and administrative data of patients are processed at several places in the e-health cloud, and the usage of smartcards and access control mechanisms alone does not provide the necessary protection.

A. Cryptographic Key Management

Complex infrastructures must be managed and this comprises additional security and privacy issues. The usage of encryption requires management of cryptographic keys; smartcards must be personalized and issued to their users.

A naive approach would say the patient of course. But how to handle lost or stolen cards when the encryption keys are lost as well? Does the card issuer or the EHR server have backup copies of the keys? But backup strategies must also take into account the privacy requirements of health data. For example, in many European countries, and especially in Germany, it is required by law that the patients themselves have the full data sovereignty over their health data. Means no other party is allowed to circumvent privacy decisions and access rights dentitions of the patient regarding EHR data. But if the card issuer or even the EHR server providers maintain backup copies of the cryptographic keys for reasons of issuing backup smartcards in case of theft or loss, they could in principle decrypt and access the EHR data directly.

B. Management of Certificates

As in any public key infrastructure, certificates must be managed to ensure authenticity of key holders (smartcards, connectors, server, etc.). This includes issuing and distributing certificates as well as updating revocation lists.

C. Management of Hardware/Software Components

Besides the cryptographic infrastructure, other components must be managed and maintained as well. This includes the hardware and software components that are used at EHR servers, billing servers, and computing devices of health care providers. Security-critical components, such as smartcard readers or connectors to protected networks, should be certified and tested properly. The installation and update of software components requires a secure distribution mechanism. On the one hand, it must be possible to allow changes in software configuration due to legitimate updates. On the other hand, unauthorized and malicious changes (e.g., due to malware attacks), must be detectable to stop further usage or to exclude the infected components from the e-health infrastructure.

VI. SECURE E-HEALTH INFRASTRUCTURE

The problem areas above show that e-health clouds impose a variety of security and privacy risks. Ideally, all of them should be solved technically and transparently for the users. In the following we present a technical solution to address particularly the end-user platform security issue. Compared to other e orts, especially national and international standardizations, this topic is not addressed sufficiently. We propose to base a secure e-health infrastructure on Trusted Virtual Domains (TVDs) to ensure fundamental security and privacy properties. In this section, we first introduce privacy domains for healthcare systems. Then we discuss our realization based on a security kernel and TVDs.

A. Management of Hardware/Software Components

In the context of e-health, privacy protection of the patients' data is a primary concern. Technological solutions should be employed to support legal and contractual regulations. We propose to construct privacy domains for the patients' medical data as a technical measure to support the enforcement of privacy and data protection policies: Systems (e.g., a client PC) must be able to partition execution environments for applications into separate domains that are isolated from each other. Data is kept within a privacy domain, and the domain infrastructure ensures that only authorized entities can join this domain. Moreover, data leakage from the domain is prevented by the security architecture and the domain infrastructure. Therefore, the same system can be used for different workflows that are strictly isolated. Figure 2 illustrates the privacy domains applied to our e-health cloud model. An important aspect for the deployment of any new infrastructure in practice is the integration of legacy systems.

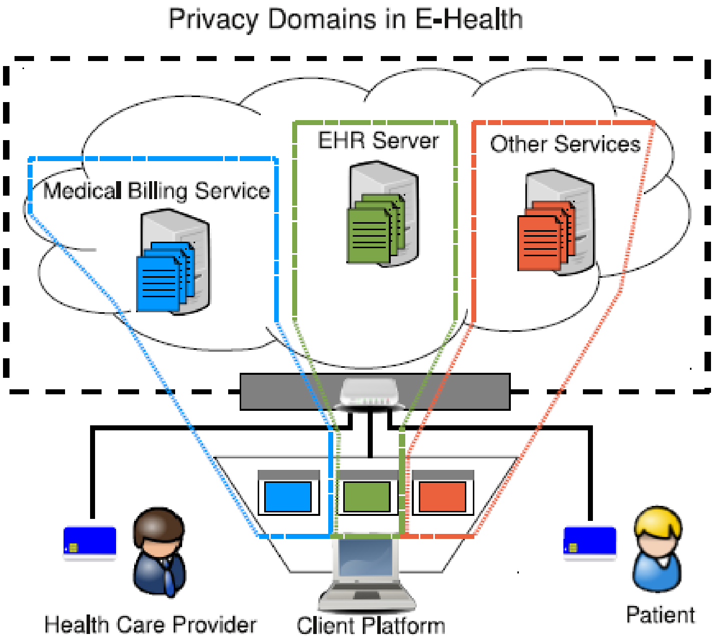

Figure 2: Privacy Domains in the E-Health Cloud.

VII. A RESEARCH AND DEVELOPMENT AGENDA

From a technical standpoint, we need to improve in several ways the system we implemented before it could be deployed in production. A first issue regards the need should look at patient-owned health records in the context of several institutional factors [3] that may hinder their success. The relationship among processes, people, business models and our proposed solutions, in particular, needs further investigation. Regarding processes, we need to investigate how MyPHRMachines will impact administrative and clinical processes currently in place in healthcare institutions. For instance, administrative processes are usually driven by data available in local EHRs, which may be inconsistent with the data possessed by the patient. Another factor influencing the success of our solutions can be the management of the coexistence of patients adopting and non-adopting personally-owned healthcare records, since we cannot assume complete penetration of such a technology, at least in the initial transitory period. Regarding people, MyPHRMachines represents a disruptive technological innovation and, as such, we need to investigate its acceptance and possible adoption by different types of users, such as patients, physicians, or administrative personnel. This is important since review results have already pointed out that the positive attitude of patients towards PHRs does not translate automatically into their effective adoption. Eventually, regarding business models, research is required to understand how to make our solution economically profitable in the healthcare ecosystem. While, in fact, adopting our solution may reduce the cost of data exchange and exam retake, the costs related to the implementation and maintenance of patient-owned records has to be taken into account. The identification of a profitable business model for our solution is object of our current work.

VIII. DISCUSSION AND 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.

REFERENCES

[1] Privacy preserving ehr system using attribute-based infrastructure-- S. Narayan, M. Gagn´e, and R. Safavi-Naini.

[2] Easier: Encryption-basedaccess control in social networks with efficient revocation--S. Jahid, P. Mittal, and N. Borisov.

[3] Distributed attribute based Encryption--S.M¨ uller, S. Katzenbeisser, and C. Eckert.

[4] Identity-based encryption with efficient revocation--A.Boldyreva, V. Goyal, and V. Kumar.

[5] Achieving secure, scalable,and fine-grained data access control in cloud computing--S. Yu, C. Wang, K. Ren, and W. Lou.