© 2015 IJSRSET | Volume 1 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Security for Medical Records Using Private Key Encryption

Devika P[1], Divya S[2], Harinipriya V S[3], M. Gayathri[4]
Department of Information Technology
Dhanalakshmi College Of Engineering, Chennai, India.
Anna University, Chennai, India

ABSTRACT

Personal Health Records (PHRs) should remain the lifelong property of patients, who should be able to show them conveniently and securely to selected caregivers and institution. In contrast to previous approaches, our solution is designed to maintain EMR availability even when the network connectivity is not available. To validate our architecture, we have implemented a prototype system using attribute based encryption algorithm. Patients will be able to share their remote virtual machine session with selected caregivers, who will need internet and a Java enabled Web browser to PHR. We discuss a prototype that enables to generate a ciphered long key string and implement a Hypervisor which is a virtual machine to maintain the PHRs.

Keywords: PHR, DICOM, HTML5, MyPHRMachines, EHR, VMs, IaaS, Cloud computing, electronic medical record (EMR), personal health record (PHR), hypervisor.

I. INTRODUCTION

Personal Health Record (PHR) is a set of computer-based tools that allow people to access their lifelong health records and make parts of it available to those who need it. PHRs should be portable, i.e., remain with the patient, contain lifelong information, and should not be restricted by any kind of issue. They are electronic health records (EHRs) that are owned by patients. These are usually opposed to hospitals' electronic medical records (EMRs), which has health data generated within one specific medical institution.

Cloud computing offers facilities to support long-term health record maintenance. In this paper, we develop MyPHRMachines, a cloud-based PHR system. One of the basic essentialities for share ability of the EHR is to break the nexus between the EHR and the EHR system. The MyPHRMachines architecture separates PHR from the software to work with these data. This paper focuses on opportunities of using PHR software services without compromising the confidentiality of PHR.

We concentrate on giving patients a (and their confidential caregivers) remote desktop with a java enabled web browser or tablet computer access to all their PHR records and support this access by the software that matches the data format. As we do not handle data integration in our paper, one can assume this as health record mobility and portability.

Government can play several predominant roles in increased usage of PHR. At the infrastructure level, the government agencies fasten development and adoption of data and interchange standards for PHR content areas. Such standards are helpful, but we debate that regardless of such evolution, patients should have been endorsed with the capability to access their own health data. We aim at the functional interoperability -i.e., the ability of two or more systems to exchange information so that it is readable by the receiver.

PHR systems positioning themselves within the cloud computing paradigm are emerging. This enables patients to upload their medical data and then selectively share these with caregivers. Unfortunately, such software-as-a-service (SaaS) systems are typically (1) specialized for a particular medical function and (2) specifically programmed for web browsers. For example, it may indeed consists of a DICOM viewer that has been programmed in HTML5.MyPHRMachines is an educational prototype that is more applicable as it exposes the infrastructure-as a-service (IaaS) tier of cloud architectures [7] to the user. Precisely, the system provides infrastructure to (1) store and share (subsets of) patient's health records and (2) deploy and use specialized software in remote virtual machines (VMs). MyPHRMachines enables to develop PHRs which are strong across the space and time dimensions.

Space: Patients simply traveling across different countries during their lifetime will always be able to access their original health records and the software required to analyse/visualize those data. This is not possible because of the high functional and architectural complexity of healthcare systems across different countries/states [8]. Time: As technology grows rapidly, application software typically becomes obsolete. On the server-side, MyPHRMachines prevents problems by virtualizing execution environments. The software to build the idealized environments on contemporary hardware and software is maintained by big vendors [9], regardless of the MyPHRMachines-specific extensions. On the client-side, MyPHRMachines depends on web technologies, to realize a remote desktop client. A client software maintenance is detached from the number and complexity of PHR software services. PHR systems offer functionalities to share, visualize, and analyse PHR data [10]. MyPHRMachines allows users to share software to work with the health-related data. Separation of data and functionality allows access to fine grained delegation of different stakeholders. Specifically, MyPHRMachines allows patients to selectively share health information to other stakeholders and it assures that, once shared with a stakeholder, it cannot be improperly stored. The software specialists deploying third party PHR services to MyPHRMachines never get access to patient information; next, person having access patient's remote VM sessions cannot access the software beyond the time frame that is given by the patient. The present PHR system imposes threat in terms of privacy, examples of which are discussed in the later section.

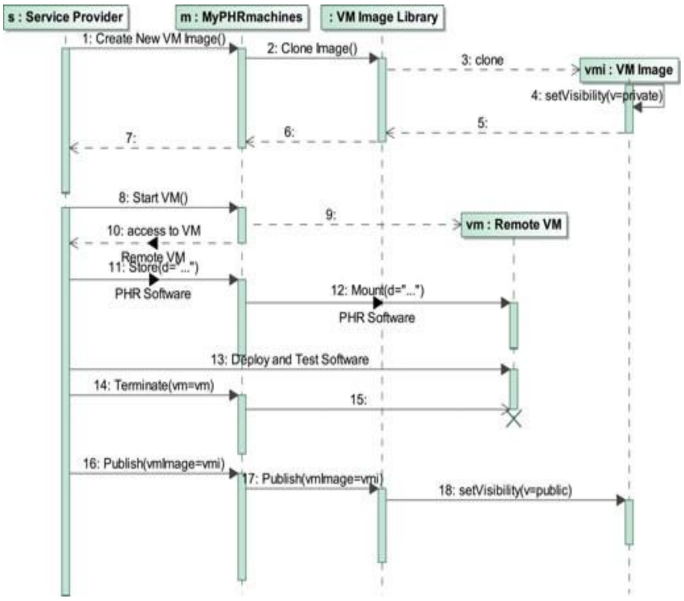
Section II presents the design and implementation of MyPHRMachines. The limitations of our approach are discussed in Section III, whereas the related literature is reviewed in Section IV. Finally, conclusions and future work is discussed in section V.

II. DESIGN AND IMPLEMENTATION OF MYPHRMACHINES

In this section, we first present the technical architecture of our prototype. The main idea behind MyPHRMachines is to use the cloud to allow the patients to build their own personal health data repository and share these data with different care institutions. In the current system, patients have to manually upload the data they obtained from care institutions, e.g., in a CD. In a near future, we ensure that care institutions could directly push patient data to the repository. Once stored in MyPHRMachines, patients can flexibly share these data with other care institution. Access to MyPHRMachines, needs only a Java-enabled browser, and access to a selected part of the VM session can be easily granted by patients to any care institution. Moreover, MyPHRMachines also allows care institutions to make available specialist software required to view and/or analyse Health-related data. In this way, caregivers does not require special software, as they can get access to this software directly from the cloud.

MyPHRMachines needs the development of functionality specific to the PHR context (e.g., access delegation to a VM session). We made the Web portal to become simpler and coherent to facilitate access by users. Each VM represents the virtualization of specific application software serving the purpose of either viewing or analysing patients' health data. Patients can decide which VM to load in a given session using a standard Web portal. The Hypervisor is a generic piece of software to start, stop, maintain VMs, and control their Internet access. We decided to use Virtual Folder, an off the-shelf hypervisor. Virtual Folder benefits from periodic functionality updates and security reviews. The VMs for special software are stateless and deprived of Internet access. VM consists of virtual disks containing a bootable operating system and additional applications. Software vendors clone an existing VM containing the right operating system and perhaps some additional libraries of interest through the MyPHRMachines Web portal. Finally, the vendor "publishes" the VM session for other users of MyPHRMachines. Users cannot change the published VM session in any personal instance of being stateless. By keeping VM instances stateless, one can deploy updates at the VM session level, which is much more scalable and securable. The cost of requesting a VM clone via the MyPHRMachines portal is negligible. Other costs relate to (1) uploading application executables to MyPHRMachines and (2) configuring them in the new VM session. The first cost is unavoidable since it becomes relevant any time a software vendor wants to deploy software to a cloud based system. For the second cost, any IaaS-based approach would provide the same level of flexibility that MyPHRMachines would provide. However, in more general IaaS platforms (e.g., Amazon EC2), VM session would have to be duplicated explicitly for each end-user. End-users would be able to change the VM sessions, introducing maintenance costs. Instead, the MyPHRMachines approach of using stateless VM sessions avoids that cost problem by design. The PHR data are stored into virtual folders, which remain private folders within the MyPHRMachines. The VM based architecture ensures that all patient data can remain on the server, on a trusted infrastructure. The latter feature, combined with stateless VMs deprived of Internet access, guarantees the privacy of the patient's data.

Patients can direct MyPHRMachines to forward by e-mail, ciphered string identifier of a VM session to share with a specific care institution. Using this identifier, the user is able to access the VM with one click, even without having a system account (i.e., without the need to login). Patients may decide to shut down a VM, for instance, in case they realize that the care institution to which they granted access is misusing their PHR data. The long string is based on applying a hash function to parameters of the VM session. Moreover, even if an attacker guesses a string that secret is valid only for the lifetime of one VM session. Fortunately, care institutions are likely to have secured tools and, therefore, the access delegation can be sent securely from the MyPHRMachines web server to the caregiver. Therefore, we do not consider this as a major threat.



The workflow clarifies the details in sequence diagram. Steps 1 to 7 involve setting up a new VM image. Steps 8 to 12 involve uploading application data. Steps 13 to 15 involve the installation and configuration of these executables. MyPHRMachines enables specialization among software vendors: some may specialize in setting up developer-friendly VM session with application infrastructure (e.g., a complex web and database server environment). Steps 16 to 18 involve publishing a VM image to a library. The library concept is not only important both to separate the developer-oriented images, but also to organize end-user images in various more fine-grained structures (e.g., per medical condition or per insurance plan)

In order to achieve a solution for MyPHRMachines in terms of cost reduction and quality improvement, researchers will have to pay attention to several issues coming from the contextualization of MyPHRMachines in the complex health care ecosystem. A useful reference in this context is the one of institutional theory, which has often been used to address the short comings of technological innovation in health care. It predicates that organizations are often influenced by internal pressure, e.g., relative power of physicians and administrative managers, or at the industry level, leading them to choose legitimated elements that have the effect of directing attention from task performance and social welfare. According to institutional theory, the relationship among processes, people, business models and our proposed solution, in particular, needs further investigation.

Regarding processes, we need to investigate how MyPHRMachines will have impact on administrative and clinical processes in health care institutions. For instance, administrative processes usually driven by data available in local EMRs, which may be inconsistent with the data possessed by the patient. Another factor influencing the success of our solution can be the coexistence management of patients personally owned health care records, since we cannot assume complete penetration of such a technology without government sponsoring, at least in the initial transitory period. Regarding people, MyPHRMachines represents a technological innovation that may disrupt current medical practice and patient behaviour. As such, we need to investigate its acceptance and possible adoption by different types of users, such as patients, physicians, or administrative personnel.

Eventually, regarding business models, research is required to understand how to make economical solution profitable to the health care. While, adopting our solution may reduce the cost of data exchange, the costs related to the implementation and maintenance of patient records has to be taken into account. Moreover, MyPHRMachines can become a success only by exploiting its functionality to existing PHR and EMR systems.

We distinguish the cons of our work from the ones related to the functionality of MyPHRMachines as currently implemented and the ones related to the research method adopted for its evaluation. About the functionality, MyPHRMachines is likely to lead to numerous personal application, in which each patient collects heterogeneous PHR data and application software. This can lead to health information and related functionality that can be very hard to maintain for the average patient. The issue can be overcome by a careful design of the interface of MyPHRMachines used by patients to upload, share, and, organize their PHR data, which should be intuitive and hide technical details. Another cons previously identified is the lack of Internet access for the VMs. This prevents a VM to call external (Web) services to combine such services together. We argue, that the same services can be deployed within the trusted domain of MyPHRMachines and available to patients to be used. Moreover, for trusted VMs, controlled access to specific Internet addresses can be configured by means of a web proxy. Users should be properly informed of the kind of VM session they are running: a session without Internet access can be trusted blindly, while a session with controlled Internet access is only as trustworthy. Another consequence of the lack of internet access in end user VM sessions is that the software inside such VM sessions cannot automatically updated. First of all, most automated internet updates are security-related and, therefore, irrelevant for VMs without internet access. Second, MyPHRMachines is designed to allow frequent updates at the level of VM session. End-users are expected to be stateless and if VM updates are provided frequently, then end-users benefit from the functional software updates. This is required to free the patient and caregivers from the burden of transferring to the PHR system all health information. In our Opinion as developers of MyPHRMachines, from the technical implementation standpoint, this extension does not represent a substantial obstacle. About the research method, MyPHRMachines is currently fully implemented using PHR data and medical application software. The system, has not yet been experimented in clinical settings by real patients. Thus, it remains at a qualitative level, based on the analysis of the literature and qualitative interviews with key health care stakeholders. Experimentation with actual patients will allow us to evaluate the people institutional factor related to MyPHRMachines adoption. It is essential as review results have already pointed out that the positive attitude of patients toward PHRs does not translate automatically into their effective adoption.

III. RELATED WORK

We can first classify current PHR solutions into free-standing (third party), provider-tethered, and integrated PHR systems. Free-standing PHR systems are stand-alone software applications that help patients maintaining their personal health information. Provider-tethered solutions are implemented and made available by a single care institution. In terms of the number of patients, the most successful PHR solutions belong to the latter category. Besides increasing efficiency, by reducing the need for patient data collection or duplicate clinical exams, provider tethered PHRs promote a more relationship between the vendor and the patient. At the same time, these types of PHRs do not address the space dimension in the continuity of care ensured for PHRs. An interoperability problem remains, when the patient seeks care from a caregiver outside the network of the PHR. MyPHRMachines can be classified as an integrated PHR solution. Integrated PHRs are free-standing solutions that collect information from a variety of information sources, such as EMRs, insurance claims, pharmacy data, or data entered directly by patients. Integrated solutions or Microsoft Health Vault are less successful in terms of adoption when compared to provider-tethered solutions. Patients are required to actively experiment with the technology without being pushed in doing so by a given vendor. The interoperability of the PHR with other systems and, more generally, the provider willingness to trust and use the PHR, are not guaranteed.

MyPHRMachines solution overcomes that second cons of integrated PHRs as follows. First, it makes the PHR information trustworthy by delivering original PHR data and related application software directly to care institutions instead of providing patient-entered information. Second, the barrier to access a MyPHRMachines session is minimal only one hyperlink needs to be clicked for accessing the trusted health data and its software. As far as the architecture is concerned, PHR systems rely on a client-server, Web-based architecture.

Although Web based access provides easy access by patients and caregivers, traditional PHR systems remain passive repositories of health related data, which requires external application software for data visualization or analysis. SaaS can be used to integrate application software with Web-based PHRs. Application software will have to be reprogrammed against the libraries and interfaces provided by the PHR platform. MyPHRMachines does not pose that barrier.

On the one hand, MyPHRMachines preserves the benefit of a Web-based client, i.e., patient and caregivers only need a browser to access data, but, on the other hand, MyPHRMachines extends the scope of traditional PHR systems allows to run the original application software to visualize and analyse data through virtual machines. Caregivers and software vendors will not have to reprogram their application software against a SaaS specification, e.g., Web services over SOAP, but can simply deploy their existing software in a VM session. As far as PHR data security and privacy are concerned, Web based PHR systems allow patients to collect and store digitized health information, but they usually implement only simple selective access delegation policies. About commercial systems, for instance, allows separating private and public health information and defining specific roles (e.g., provider or caregiver) to access the information classified as public. MyPHRMachines allows a finer grained sharing approach, where patients can provide access to subsets of their PHR data to individual caregivers. Such functionality may be extended with a role-based access control e.g., to share PHR data known by a patient. The existing PHR platforms does not provide any technical measures for preventing data abuse created by the plug-ins that are contributed by third party software. Instead, they provide patients with take-it-or-leave-it terms of user agreements for each individual third party plug-in. typically, in such agreements, the third party vendors promises not to abuse the data. Consequently, upon end-user permission, their software service provides download access to the patient data and it is the responsible of the external audits to verify what the terms of use are adhered to. While this architecture may be adequate for sharing information to providers whose reputation is at stake (e.g., an established hospital), it seems less adequate for a service provided from the rapidly evolving bio-informatics industry. The cloud is by nature opaque and, may pose additional data security threats. The encryption of health-related data is made particular given the number and type of care institutions with which health data will be shared. The literature suggests using Attribute Based Encryption (ABE) as the main encryption methodology for sharing EHR data. In ABE access is based on sets of attributes of users, rather than on the unique identity of users. This allows patients to selectively share their PHR data in a secure way to a set of users without the need to know their complete identity. ABE encryption is a solution that complements the current implementation of MyPHRMachines. In this paper, it describes about such generic security techniques to enable a discussion of the unique privacy protection mechanisms that are offered by MyPHRMachines.

IV. CONCLUSION

In this paper, we developed MyPHRMachines that leverages virtualization techniques. MyPHRMachines allows patients to build lifelong PHRs. The records can be shared by the patient with any stakeholders.

MyPHRMachines allows the controlled sharing of application software that is required to view and/or analyse health records. Patients taken care by caregivers in different geographical areas will be able to reproduce their original health records, no matter the limitations imposed by the heterogeneity of local health care information systems. As technology evolves, patients can use original software to view and analyse data, even when that software becomes obsolete and no longer supported by the stakeholder. A clinical experimentation that assesses patient's propensity for using such an innovative PHR system like MyPHRMachines, we are currently working on extending our proposal in several ways. One of the major extensions is to create an open App market for application software, through which medical software providers could provide the functionality required by patients. We are currently dealing with the issue of how various security measures can be employed to protect data in MyPHRMachines, such as encryption techniques at the level of VM instance logs, private key transfers between clients and remote VMs. We are surveying practitioners to understand more broadly and deeply the specific uses for which MyPHRMachines forms a unique enabler. Finally, we will deploy data translation services to MyPHRMachines. Such services will enable a smooth transition from the already provided functionality to the deeper system. The private virtual folders will be used as the blackboard for exchanging data between different VMs.

V. REFERENCES

[1] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "Viewpoint paper: A research agenda for personal health records (PHRs)," *J. Amer. Med. Inform. Assoc.*, vol. 15, no. 6, pp. 729–736, 2008.

[2] A. Rosenthal, P. Mork, J. Li, M.H. adn Stanford, D. Koester, and P. Reynolds, "Cloud computing: A new business paradigm for biomedical information sharing," *J. Biomed. Inf.*, vol. 43, pp. 342–353, 2010.

[3] Accelarad. (2012, Jul.). Seemyradiology – medical image sharing.[Online].Available: http://www.seemyradiology.com/

[4] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi,"Cloudcomputing—Thebusinessperspective,"*Decis.Supp.Syst.*,vol.51, pp. 176–189, 2011.

[5] T. J. Bittman, G. J. Weiss, M. A. Margevicius, and P. Dawson, "Magic quadrant for x86 server virtualization infrastructure," Gartner Inc., Stamford, CT, USA, RAS Core Research Note G00205369, Jun. 2011.

[6] D. T. Mon, J. Ritter, C. Spears, and P. Van Dyke, "PHR system functional model," HL7 PHR Standard, May 2008.

[7] S. Negrini, S. Atanasio, F. Zaina, and M. Romano, "Rehabilitation of adolescent idiopathic scoliosis: Results of exercises and bracing from a series of clinical studies. Europa medicophysica-SIMFER 2007 award winner," *Eur. J. Phys. Rehab. Med.*, vol. 44, no. 2, pp. 169–176, Jun. 2008.

[8] M. L. Metzker, "Sequencing technologies—The next generation," *Nature Rev. Genet.*, vol. 11, no. 1, pp. 31–46, Jan. 2010.

[9] K. Wetterstrand. (2012, Jan.). DNA sequencing costs—Data from the NHGRI large-scale genome sequencing program. [Online]. Available: http://www.genome.gov/sequencingcosts/

[10] P. Van Gorp and P. Grefen, "Supporting the internet-based evaluation of research software with cloud infrastructure," *Softw. Syst. Model.*, vol. 11, no. 1, pp. 11–28, 2012.

[11] Microsoft Terminal Services Team. (2009 Mar.). Top 10 RDP protocol misconceptions. [Online]. Available: http://blogs.msdn.com/b/rds/archive/2009/03/03/top-10-rdp-protocol-misc onceptions-part-1.aspx

[12] Nucleics. (2012). Reviews of dna sequencing service companies & facilities. [Online]. Available: http://www.nucleics.com/DNA_sequencing_support/sequencing-service-reviews.html

[13] K. Nazi, "Veteran's voices: Use of the American customer satisfaction index survey to identify my healthevet personal health record users' characteristics, needs, and preferences," J. Amer. Med. Inf. Assoc., vol. 17, pp. 203–211, 2010.

[14] D. Detmer, M. Bloomrosen, B. Raymond, and P. Tang, "Integrated personal health records: Transformative tools for consumer-centric care," BMC Med. Inf. Decis. Mak., vol. 8, 2008.

[15] J. Halamka, K. Mandl, and P. C. Tang, "Early experiences with personal health records," J. Amer. Med. Inf. Assoc., vol. 15, no. 1, pp. 1–7, 2008.

[16] D. C. Kaelber, S. Shah, A. Vincent, E. Pan, J. M. Hook, D. Johnston, D. W. Bates, and B. Middleton, The Value of Personal Health Records. Healthcare Information & Management Systems Society, 2008.

[17] B. Adida, A. Sanyal, S. Zabak, I. S. Kohane, and K. D. Mandl, "Indivo X: Developing a fully substitutable personally controlled health record platform," in Proc. AMIA Symp., Nov. 2010, pp. 6–10.

[18] A. Sunyaev, D. Chornyi, C. Mauro, and H. Kremar, "Evaluation framework for personal health records: Microsoft healthvault vs. googlehealth," in Proc. 43rd Hawaii Int. Conf. Syst. Sci., Jan. 2010, pp. 1–10.

[19] N. Archer, U. Fevrier-Thomas, C. Lokker, K. A. McKibbon, and S. E. Straus, "Personal health records: A scoping review," J. Amer. Med. Inform. Assoc., vol. 18, pp. 515–522, Jul. 2011.

[20] I. Carrion, J. Fernandez Aleman, and A. Toval, "Personal health records: New means to safely handle our health data?," IEEE Comput., 2012, vol. pp, no. 99, p. 1, 2012.

[21] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Proc. IEEE 3rd Int. Conf. Cloud Comput., Jul. 2010, pp. 268–275.

[22] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parall. Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[23] C. Wang, X. Liu, and W. Li, "Implementing a personal health record cloud platform ciphertext-policy attribute-based encryption," in Proc. 4th IEEE Int. Conf. Intell. Network. Collaborat. Syst., Sep. 2012, pp. 8–14.