Secured My Personal Health Record Sharing and Data Translation via Virtual Machines in the Cloud

M. Surja
P.G Scholar
P. S. R Engineering College

***Abstract:*-Personal Health Records (PHRs) should remain the lifelong property of patients and should be show able conveniently and securely to selected caregivers. Regarding interoperability, current solutions for PHRs focus on standard data exchange formats and transformations to move data across health information systems. In this paper we propose MyPHRMachines, a patient-centric system that takes a radically new architectural solution to health record interoperability. We propose to deploy besides the medical data also the related software to the PHR system. After uploading their medical data to MyPHRMachines, patients can access them again from remote virtual machines that contain the right software to visualize and analyze them without any conversion. Patients can share their remote virtual machine session with a selected health provider, who will need only a Web browser to access the pre-loaded fragments of the lifelong PHR.**

Index Terms:*- *Electronic health Record, personalized medicine, Radiology, Virtualization Security System, Authorization policies.

1. INTRODUCTION

In a recent review paper, Kaelber et al. define a Personal Health Record (PHR) as “a set of computer-based tools that allow people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it” [6]. We adopt a refinement of this definition by distinguishing between the actual PHRs (health related data, owned by individual patients) and the PHR system that offers functionality to upload, analyze and share PHR data. PHR systems differ from Electronic Health Record (EHR [5]) systems, being patient-oriented rather than caregiver-oriented. While EHR systems, in fact, store the information produced by health providers, mostly to guarantee legal compliance, PHR systems make patients responsible for their health information. PHRs should be portable, i.e. remain with the patient, contain lifelong information, and should not be restricted by file formats or other local issues [2]. Kaelber et al. conclude from their survey that the four top PHR research opportunities reside in (i) function evaluation, (ii) adoption and attitude analysis, (iii) privacy and security solutions, and (iv) architectural solutions.

Regarding function evaluation, successful PHR systems enable patients to enter their own health information and then provide fine-grained controls to share that information with others. Adoption and attitude analysis reveals that patients are eager to use PHR systems but fail to do this effectively so far [4]. Regarding security and architecture, the relative benefits of free-standing (third-party) PHR systems should be analyzed against those of provider- (e.g., hospital-) tethered PHR systems. We argue that free standing systems have more potential since they enable a patient to organize his/her data irregardless of a particular health provider’s concerns. Kaelber et al. also call for architectural research on interoperability and stress that evaluating the relative benefits and costs of different PHR architectural models represents a key research priority. In this paper we present MyPHRMachines, a patient owned health record system prototype based on remote virtual machines hosted in the cloud. Virtualizing medical software along with medical data has various advantages. First of all, it makes the PHR information trustworthy. Medical specialists are generally rather skeptic to new information technologies [7]. PHR systems in which PHR data have been manipulated by conversion software and displayed also by non-original viewer software are likely to generate additional resistance to adoption, making PHR systems medically irrelevant in many cases. A second argument for incorporating the software for viewing the original data in PHR systems is of economic nature: it is much more efficient to reuse valuable legacy software than to re-build it upon each technology change.

2. LITERATURE SURVEY

Personal Health Records -A personal health record (PHR) is collection of health-related information that is documented and maintained by the individual it pertains to According to the Department of Health and Human Services, a personal health record (PHR) is similar document maintained by the owner of the record. But the access can be given to limited people like doctor. . In an electronic health record system [1], patients, healthcare providers, and medical devices can upload health records and retrieve and view them at a later time. Furthermore, patients may delegate access rights and allow family, friends, and designated healthcare providers to view or to edit parts of their record. Patients and their delegates may wish to efficiently perform searches in an efficient manner over part or all of the record. Figure1 represents the model of EHealth system. The PHR is managed by the third party service provider i.e. cloud data storage provider [6]. **Fig1: secure PHR in cloud computing** The major research area is about the security of PHR system. First the access control of the PHR record is to be well defined. Second the PHR data is to be saved in encrypted form because the PHR is stored in a cloud maintained by the third party. Conventional encryption algorithms are not suitable to encrypt the PHR data. Attribute based encryption is the technique which can concentrate both the problems.

Cloud Computing:

Cloud computing is an efficient technique by which the user can access any data from anywhere and anytime through internet. Thus it's providing the new world of computing technology to the world. The personal health records are thus also using this cloud computing technology for the efficient storage and retrieval system. But there is still a comparison is going on with the electronic health record and personal health record. Electronic health record is the electronic version of the medical record of the care and treatment the patient receives. It is maintained and managed by the health care organizations. But our PHR is the collection of important information that the patient maintain about their health or the health of someone they are caring for. It may be short and simple or very detailed. The traditional PHR was in the form of paper documents, electronic files Maintained by their computer, but now the PHR is created by using the tools available in the internet. So which make the facility to use the health information across any distances, and to share with the selective users with special read and write access.

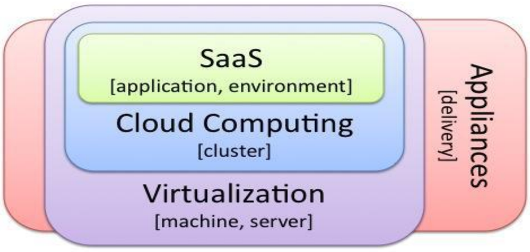

Fig1: cloud computing in virtualization security system

Virtualization: Hardware virtualization or

Platform virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources. For example, a computer that is running Microsoft Windows may host a virtual machine that looks like a computer with the Linux operating system; based software can be run on the virtual machine. In hardware virtualization, the host machine is the actual machine on which the virtualization takes place, and the guest machine is the virtual machine. The words host and guest are used to distinguish the software that runs on the physical machine from the software that runs on the virtual machine. The software or firmware that creates a virtual machine on the host hardware is called a hypervisor or Virtual Machine Manager. Hardware assisted virtualization is a way of improving the efficiency of hardware virtualization. It involves employing specially designed CPUs and hardware components that help improve the performance of a guest environment.

3. ENCRYPTION TECHNIQUES

At the early stages of the cloud computing and Personal health record the traditional encryption techniques were applied to the personal health record and now days the advanced encryption techniques such that attribute based Encryption and its different variations are used.

1) Public key encryption:

The public key encryption method was the most traditional method applied to the PHR for the security of the data. But it made the high key-management problems and also this method was very less scalable. The user revocation or break glass access and other advanced techniques were not possible with these one-to-one encryption techniques.

2) Attribute based encryption:

The attributes can define an object very efficiently just as the identity of an object works. The attribute based encryption provides the security to the database. In this system both the cipher text and secret key will be associated with the attributes. The user who is having a minimum number of attributes only can decrypt the data. So while applying this method the owner doesn't want to know about the entire list of users instead of that they can encrypt the data according to some attributes only. Using ABE, access policies expressed based on the attributes of user data which enable the patient to selectively share the PHR among a set of users by encrypting the file under a set of attributes, and so the owner don't want to know the complete list of user's .It provides data confidentiality and writes access control. But the on-demand user revocation and other techniques were not adaptable with this encryption method.

3) Cipher text policy attribute based encryption:

Cipher text-attribute based encryption is an attribute based encryption technique which allows the data owner to encrypt the data based on an access policy, which will be based on the attributes of the user or the data. So, the decryption is possible when the secret key is matching with the access control policy the key-idea of the CP-ABE is: the user secret key is associated with a set of attributes and each cipher text will embedded with an access structure. The user can decrypt the message only if the user's attribute satisfied with the access structure of the cipherext. This method has the benefits such that the third party server won't have the access on the plain data, Decryption will be possible only when the secret key Matched up with access policy defined on attributes, and every user is needed proper authentication and Authorization to access the data. And also it removes the need for knowing the identity of the patient by the patient for providing access grant. The key challenges regarding this CP-ABE scheme is that the user revocation difficulty. Whenever the owner wants to change the access right of the user, it is not possible to do efficiently with this scheme.

4) key-policy based encryption:

It is an attribute based encryption in which the Data are associated with the attributes, for each of which a public key component is defined. In this method, each user will be assigned to an access structure which will specify which type of cipher texts the key can decrypt [4]. The secret key is defined to reflect the access structure. So the user will be able to decrypt a cipher text if and only if the data attribute satisfy that user's access structure. The key-policy attribute based encryption and cipher texts-policy attribute based encryptions are almost working in a similar way, but both have some difference in terms of specifying the access policy for the users. The KP-ABE is useful for providing the fine-grained access control to the data system where it can efficiently specify that which part of data system can be accessed by which user and what are the operations they can execute over there.

5) Multi-authority attribute based encryption:

The multi-authority attribute based encryption Scheme is an advanced attribute based encryption in which it will have many attribute authority for handling the different set of users from various domains [5]. In the PHR system the users will be from different domain like the doctors from health care organizations, the friends and family from personal relations and other users from insurance domain too. So each user will be having different access control mechanism based on the relation with the patient or owner. Thus the MA-ABE scheme will highly reduce the key-management issues and overhead and thus it will provide fine-grained access control to the system.

4. THE EXISTING SYSTEM

Personal Health Record system where there are multiple Personal Health Record owners and Personal Health Record users. The owners refer to patients who have full control over their own Personal Health Record data, i.e., they can create, manage and delete it. There is a central server belonging to the Personal Health Record service provider that stores all the owners' Personal Health Record. The users may come from various aspects; for example, a friend, a caregiver or a researcher. Users access the Personal Health Record documents through the server in order to read or write to someone's PERSONAL HEALTH RECORD, and a user can simultaneously have access to multiple owners' data. A typical Personal Health Record system uses standard data formats. For example, continuity-of-care (CCR) (based on XML data structure), which is widely used in representative PERSONAL HEALTH RECORD systems including Indio, an open-source Personal Health Record system adopted by Boston Children's Hospital. Due to the nature of XML, the Personal Health Record files are logically organized by their categories in a Hierarchical way.

5. THE PROPOSED SYSTEM

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The hypervisor serves as a platform for running virtual machines and allows for the consolidation of computing resources such as a hardware platform, operating system, storage device, or network resources. Virtualization is the process by which one computer hosts the appearance of many computers. Virtualization is used to improve IT throughput and costs by using physical resources as a pool from which virtual resources can be allocated.

Hosted virtualization architecture has the following: Hardware (CPU, memory, NIC, disk), Host Operating System, Application program, Virtualization layer Hosted (guest) operating system, Hosted (guest). Application program. A hypervisor, a.k.a., a virtual machine manager /monitor (VMM), or virtualization manager. A program that allows multiple operating systems to share a single hardware host. Another technology at the heart of system virtualization each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what are needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) cannot disrupt each other. A virtual machine is defined as a representation of a physical machine by software that has its own set of virtual hardware upon which an operating system and applications can be loaded. With virtualization each virtual machine is provided with consistent virtual Hardware regardless of the underlying physical hardware that the host server is running. When you create a VM a default set of virtual hardware is given to it. You can further customize a VM by adding or removing additional virtual hardware as needed by editing its configuration. A self-contained computing environment that behaves as if it is a separate computer. For example, Java applets run in a Java virtual machine (VM) that has no access to the host operating system. Computing Environment is a collection of computers / machines, software, and networks that support the processing and exchange of electronic information.

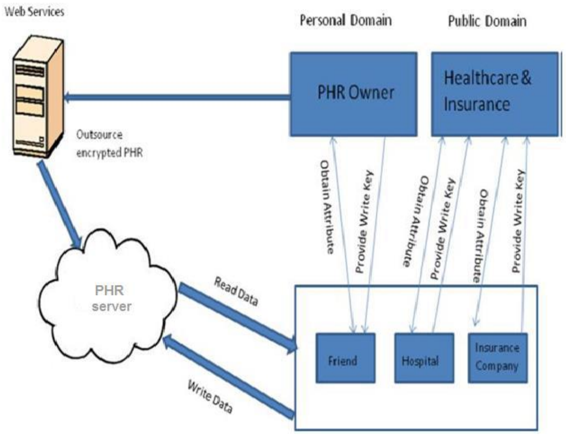

Fig. 2: Proposed System Model for AES –PHR system

The proposed system the patients' control over their own Personal Health Record, it is a promising method to encrypt the Personal Health Record before outsourcing. Yet, 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- rained, 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 Personal Health Record stored in semi-trusted servers. To achieve fine-grained and scalable data access control for Personal Health Record, we leverage attribute based encryption (ABE) techniques to encrypt each patient's Personal Health Record file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the Personal Health Record 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.

6. PERFORMANCE ANALYSIS & SIMULATION RESULTS

The scalability and efficiency of any Cryptographic system is evaluated by the following three parameters

1. Storage Cost
2. Communication cost
3. Computation Cost

Storage Cost

The existing methods only considers one domain. But the proposed consists of public and personal domain. But it is considered as only one public domain and different attributes exists for each user. For user u the secret key size in PUD id |Au|. It automatically reduces the key size which in turn reduces the revocation message size [12]. So all the message to be stored with Less size only.

Communication Cost

Since the public key size is small rekey message size is very small and is linear with the number of attributes in that user's secret key which reduces the communication cost.

Computation Cost

The public domain security level is chosen with 80 bits and paired with 160 bit elliptic curve cryptography to obtain the PUD secret key. The paining based cryptography library is used to calculate the secret.

7. CONCULSION

The security practices and the impact of virtualization on security can be extremely beneficial in personal health records. Virtualization improves security more accurate, easier to manage and less expensive to deploy than traditional physical security. Security in a virtualized data center can also be more fully automated. Virtualization security gives data canter administrators the power to automatically provision secure machines, automatically have security policies follow desktops when they move, automatically setup firewall rule sets for classes of servers and automatically quarantine compromised or out of compliance assets, amongst many examples. With the right technology and processes, virtualization has the power to make data centers even more secure and Compliant than their physical counter parts.

REFERENCES

[1] AHIMA e-HIM Personal Health Record Work Group, "Defining the personal health record," *J. AHIMA*, vol. 76, no. 6, pp. 24–25, Jun. 2005.

[2] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands,"White paper: Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption," *J. Amer.Med. Inform. Assoc.*, vol. 13, no. 2, pp. 121–126, 2006.

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

[4] 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.

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

[6] 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.