Biomedical Research 2018; Special Issue: S133-S136 *ISSN 0970-938X*
www.biomedres.info

Cloud computing framework to securely share health & medical records among federations of healthcare information systems.

Sudhir Shenai[1*], M Aramudhan[2]

[1]Department of Computing, Sathyabama University, Chennai, India

[2]Department of Information Technology, Perunthalaivar Kamarajar Institute of Engineering and Technology, Karaikal, India

Abstract

In general, Healthcare information systems (HIS) majorly maintains three kinds of health & medical records such as personal Heath Record (PHR), Electronic Medical Record (EMR), and Electronic Health Record (EHR).Today's health care providers normally host their HIS at their private data centers, or with cloud service providers. Normally, the records such as EMR and EHR are maintained by the Health care providers HIS. The PHR, which contains history of the health information about the individuals is normally maintained by the patients itself. Earlier, it was maintained manually by the individual. But, nowadays, we have host of cloud applications to maintain the PHR. Thus PHR hosted in these cloud applications can be accessed from anywhere in the world by authenticated persons and can be shared with desired health care providers. But the sharing of PHR demands many requirements such as sharing only desired part of the record instead of complete record, sharing with anonymous parties of no pre-existing relationship with assured privacy and integrity of the record. A complete healthcare solution also demands timely & selective sharing of relevant EMR & EHR among the federations of healthcare providers with the grant of patient's permission. Thus sharing of various Health & Medical records among various stakeholders in a timely and selective manner is of utmost necessity for global quality healthcare treatment. In this paper, we proposed a federated cloud computing framework, which enables the sharing of Health & Medical records among the various stakeholders with ease of timely access, ensuring privacy & integrity of the records. We have validated our approach by conducting a set of rigorous evaluation study using the CloudSim toolkit.

Keywords: Cloud federation, Trust negotiation, PHR, EMR, Federal HIS.

Accepted on June 20, 2017

Introduction

Nowadays, healthcare providers rely on healthcare information systems to provide critical "healthcare service" which necessitates the following [1-7]:

1. Maintenance of Electronic Medical Records (EMRs) of patients which is critical for timely and accurate access of patient's health information.
2. Health Information exchange to enable sharing of patients clinical data across disparate EMRs
3. Activity Based Costing to enable patients specific cost estimation
4. Patient Reported Outcomes to assesses treatment quality
5. Enterprise Data Warehouse to enable analysis of data collected from the information systems

Complete and critical healthcare relies upon the capacity of the healthcare providers to promptly access a patient's test outcomes, earlier treatment notes, current medicines, etc. The absence of access to this data may postpone diagnosis and result in uncalled for treatment and expanded expenses [6]. Customarily, the medical records have comprised of information scattered among electronic and paper-based files in different areas, referenced utilizing conflicting identifiers. A great part of the data in these records has a tendency to be out of date, repetitive, or garbled to the degree that it doesn't help the patient at the purpose of care [6]. The sharing of data among various stakeholders has generally been troublesome and tedious, regularly requiring the physical duplication of paper based material. Healthcare Information systems (HIS) frameworks guarantee to address most of the current issues related to information sharing worldwide among the various stakeholders of the healthcare systems such as healthcare providers, patients, record storehouses etc. The essential components of a typical Healthcare Information Systems are as depicted in the following diagram (Figure 1) [7]. Nowadays, the HISs are taking advantage of the cloud computing paradigm because of its economies of scale, pay per use model, substantial reduction in maintenance cost, ease of information

sharing etc. Thus HIS can be hosted at private cloud or at public cloud or as hybrid cloud.

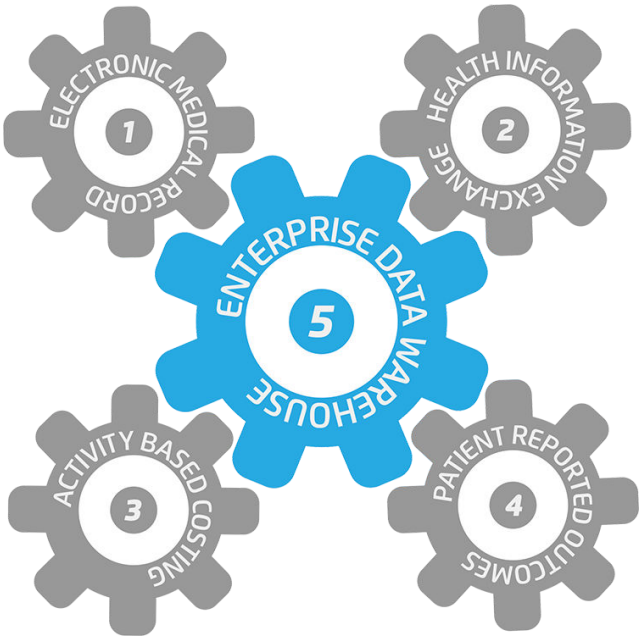

Figure 1. *Essential components of healthcare information systems [7].*

The choice of the hosting model is based on the requirements of the HIS provider such as size, scale, cost, etc. This paper proposes a federated cloud computing framework to securely share Electronic Medical Records of patients from disparate sources among HISs hosted on cloud datacenter.

Healthcare Information System: Overview

In this area we first characterize the idea of Personal Health Record (PHR), Electronic Health Record (EHR), and Electronic Therapeutic Record (EMR). At that point we quickly talk about the EMR and EHR frameworks and also the security and protection issues in getting to EMR/EHR frameworks. We likewise portray the security issues in various sorts of cloud administration models and cloud sending models for medicinal services applications.

The definitions of PHR, EMR and EHR

The terms of EHRs and EMRs are utilized reciprocally by numerous in both medicinal services industry and the press or wellbeing science writing. Entirely, these two terms depict totally unique ideas as indicated by HIMSS (Health Information and Management Framework Society) Analytics. Both EMRs and EHRs are basic to the great vision of medicinal services digitization for enhancing security, quality and furthermore, proficiency of patient care and lessening medicinal services conveyance costs. EMRs are claimed by individual medicinal services suppliers, while EHRs are commonly made out of a few subsets of EMRs. The interoperability of EHRs is a principal empowering innovation for EMRs to achieve its maximum capacity in upsetting the medicinal services conveyance with high quality and reasonable cost.

The relationship of PHR, EMR and EHR

The therapeutic records of a patient may allude to PHR, EMR and EHR. A piece of PHRs can be acquired from the EMR frameworks of various CDOs and once this EMR information is imparted to different CDOs, they get to be EHR. Due to security reason, numerous patients would prefer not to put their whole PHRs in EMR/EHR frameworks. Figure 2 shows the natural relationship of PHR, EMR, and EHR from a patient's perspective. PHR and EMR (or EHR) are halfway covered. Also, EMR and EHR are halfway covered. The level of cover contrasts from patient to tolerant because of customized security prerequisites.

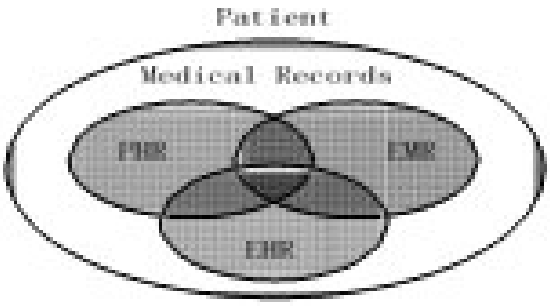

Figure 2. *Relationship of PHR, EMR and HER.*

Healthcare Cloud: Overview

Healthcare information system is available in various forms such as personal health information systems, community health information systems, health Information systems for healthcare providers, Clinical Labs etc. The Healthcare Information Systems can be well ported as cloud applications. Most of the cloud based community healthcare systems like Microsoft Health Vault, Google Health adopt common centralized model with patient centric control.

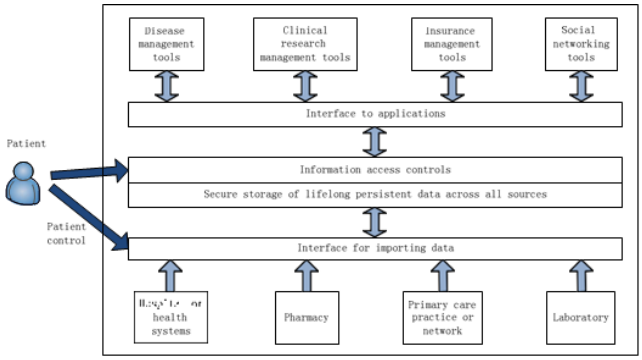

Figure 3. *Stakeholders' interactions in healthcare cloud.*

Suppose a patient maintains his health information with Microsoft HealthVault, under emergency, he got admitted with a hospital which maintains its health information system with Google, and then it necessitates both the HIS to interact with each other and share the information needed for the treatment with patient controlled access. Such situations drives the

necessity of formation of federations of cloud based HIS to share health information like PHR, EMR, EHR with various stakeholders under the patient granted access control privileges (Figure 3). Thus, in this paper we proposed a unified cloud computing framework to securely share PHR, EMR, and EHR among various stakeholders with the access control privileges granted by the patients (Figure 4). The framework ensures the complete privacy of the patient health information, and any information disclosure with the stakeholders is done under the control of patient.

Federated Cloud Framework for Health Information Systems

In this section, the framework for sharing of Health and Medical records of patients among HIS hosted in various cloud platforms are described. The HISs is federated dynamically for timely and selective sharing for records with access control grant provided by the patients. This section describes, 1) The dynamic federation methodology, 2) Privacy assured, patient-centric access controlled information sharing strategy.

Dynamic cloud federation methodology

The topological model of the Hyper-trust overlay system depends on a reasonable n-dimensional space (or hyperspace) where each facilitates speaks to the accessible amount pronounced by the hubs for a given asset or any property estimation for a particular administration or resource. Every hub is spoken to as a point in the hyperspace, and its position will change because of any organize variety, i.e. designation or arrival of assets, or any adjustments in the announcement strategy of the hub itself. The "remove" between two hubs is processed as the Euclidean separation among hub's directions, and speaks to a measure of how much two hubs are "far" as far as asset accessibility.

Overlay development is a key part of Hyper-trust and it is performed by methods for a decentralized calculation which keeps running on every hub of the system, by executing the accompanying strides:

1) Let n be a non-specific hub; hub n contacts its connected/ neighbor hubs to get, thus, their connected hubs; this operation permits a hub to acquire the arrangement of L connected hubs at 2-bounces;

2) The set L is requested by utilizing the Euclidean separation of every hub from n; on the premise of some edge parameters k and h, the hub n modifies its connections, interconnecting itself with in any event k close hubs, not most than h hubs. Hub n could surpass the edge h at whatever point the alleged "basically basic neighbors" as examined, must be saved. The means above are executed by every hub constantly (with a given period) with a specific end goal to give the connections a chance to sort out legitimately; additionally, since a hub, amid its life, may change the amount of pronounced assets, its position in the hyperspace will change. The nonstop execution of the overlay development calculation will re-organize its connection keeping in mind the end goal to protect the overlay arrange qualities.

Patient-centric access controlled information sharing strategy

The primary objective of our system is to give secure persistent driven PHR get to and proficient key administration at a similar time. The key thought is to separate the framework into various security spaces (in particular, open areas and individual spaces) as per the diverse clients' information get to prerequisites. The PUDs comprise of clients who make get to in view of their expert parts, for example, specialists, attendants, and medicinal analysts. By and large, a PUD can be mapped to an autonomous segment in the general public, for example, the human services, government, or protection segment. For each PSD, its clients are actually connected with an information proprietor (such as relatives or dear companions), and they make gets to PHRs in light of get to rights relegated by the proprietor. In both sorts of security spaces, we use ABE to acknowledge cryptographically upheld, tolerant driven PHR. Particularly, in a PUD, multi-authority ABE is utilized, in which there are various "quality experts" (AAs), each administering a disjoint subset of qualities. Part qualities are characterized for PUDs, speaking to the expert part or commitments of a PUD client. Clients in PUDs get their characteristic based mystery keys from the AAs, without straightforwardly interfacing with the proprietors. To control access from PUD clients, proprietors are allowed to indicate part based fine-grained get to strategies for her PHR documents, while don't have to know the rundown of approved clients while doing encryption. Since the PUDs contain the greater part of clients, it significantly lessens the key administration overhead for both the proprietors and clients. Every information proprietor (e.g., patient) is a put stock in specialist of her claim PSD, who utilizes a KP-ABE framework to deal with the mystery keys and get to privileges of clients in her PSD. Since the clients are actually known by the PHR proprietor, to acknowledge patient-centric get to, the proprietor is at the best position to allow client get to benefits on a case-by-case premise. For PSD, information traits are characterized which allude to the natural properties of the PHR information, for example, the classification of a PHR record. For the motivation behind PSD get to, each PHR record is marked with its information properties, while the key size is just direct with the number of record classifications a client can get to. Since the quantity of clients in a PSD is regularly little, it lessens the weight for the proprietor. While encoding the information for PSD, all that the proprietor needs to know is the characteristic information properties. The multi-domain approach best models diverse client sorts and get to necessities in a PHR framework. The utilization of ABE makes the scrambled PHRs self-defensive, i.e., they can be gotten to by just approved clients notwithstanding while putting away on a semi-trusted server, and when the proprietor is not on the web. What's more, effective and on-request client renouncement is made conceivable by means of our ABE upgrades.

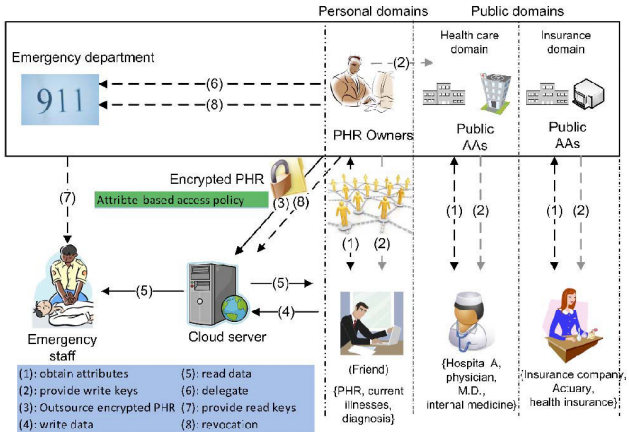

Figure 4. *Unified cloud computing framework.*

Conclusion

The sharing of medical record information of patients among the healthcare providers is absolutely essential for improving patient care, medical research, and public health. The sharing needs to be among providers with no pre-existing relationship, fast, seamless, trust worthy, secured and access rights granted by patients. The major hindrance to the implementation is the collaborations among disparate EMR systems of the health care provider. The proposed cloud computing framework for EMR systems collaborations enables sharing of medical records among the health care providers with no-pre-existing relationship on a global scale. The sharing is controlled by the selective access grants provided by the patients. The choice of collaborators is done using hyper trust overlay network of providers to speed up the process and to increase the security.

References

1. Toosi AN, Calheiros RN, Thulasiram RK, Buyya R. Resource provisioning policies to increase IaaS provider's profit in a federated cloud environment. 2011 IEEE 13th Int Conf High Performance Computing and Communications (HPCC) 2011.
2. Ramchurn S, Huynh D, Jennings N. Trust in multi-agent systems. Knowl Eng Rev 2004; 19: 1-25.
3. Rodero-Merino L, Caron E, Muresan A, Desprez F. Using clouds to scale grid resources: An economic model. Future Gener Comput Syst 2012; 28: 633-646.
4. Rosaci D. Trust measures for competitive agents. Knowl Based Syst 2012; 28: 38-46.
5. Buyya R, Ranjan R, Calheiros RN. InterCloud:Utility-oriented federation of cloud computing environments for scaling of application services. In: Algorithms and Architectures for Parallel Processing, Springer, Berlin, 2010.
6. Vawdrey DK, Sundelin TL, Seamons KE, Knutson CD. Trust negotiation for authentication and authorization in healthcare information systems. Proceed 25th Annual Int Confer IEEE 2003.
7. https://www.healthcatalyst.com/information-systems-for-accountable-care-organizations

***Correspondence to**

Sudhir Shenai

Department of Computing

Sathyabama University

India