Indian Journal of Science and Technology, *Vol 8(S9), 213-217, May 2015*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Ontology based Access Control Model for Healthcare System in Cloud Computing

K. Mohan[1*] and M. Aramudhan[2]

[1]Research Scholar, Faculty of Computer Science and Engineering, Sathyabama University, Chennai, India; meetmohan.k@gmail.com

[2]PKIET, Karaikal, India; aranagai@yahoo.co.in

Abstract

Personal Health Records (PHR) sharing is highly expected by the users for the acceptance of cloud in healthcare systems. In this paper we propose an Ontology Based Access Control (OBAC) Model that can address the permitted access control among the service providers and users.

Keywords: Access Control, Cloud Computing, Healthcare, PHR, Privacy, Ontology, Security

1. Introduction

Development in the field of distributed computing, web services and service oriented architecture have given a birth of new technology named Cloud Computing. It can provide information, software, computing power and other computing infrastructures which are available in different locations over a network on demand. Cloud provides services named Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and, Everything as a Service (XaaS) which are scalable, affordable and reliable[1].

In health sector digitization of patient's health records is gaining lot of importance, because patients are free from carrying their health records physically with a big file while going to hospital. Also, storing and sharing becomes much convenient due to networking and computing technologies. So, all the HSP (Healthcare Service Providers) are moving towards cloud computing for various benefits. Cloud promises to offer the demands of patients and healthcare service providers.

There are number of security issues need to be addressed in cloud computing service environments[2], including authentication, access control, identity management, privacy, application security, cryptography and trust. In particular, data access by various levels of users requires a user authentication and access control model for integrated management and control in cloud computing environments[3]. While storing PHR's in Cloud, The patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt their PHR data before uploading to the cloud servers[4]. Since patient's health details are sensitive, we must guarantee security and privacy to the patients for them to accept this electronic healthcare system. In general, systems for detecting and preventing insider intrusions are based on Role Based Access Control (RBAC) and C-RBAC (Context-aware RBAC) models. However, RBAC cannot provide dynamic access control because it includes no context-aware elements. C-RBAC does not ensure the protection of privacy and integrity because it does not consider the level of security in between[5].

Ontology is the theory of objects and their interrelationship. While focusing on PHR access control in dynamic and decentralized users, this system adopts on ontology based approach in which the users and their relationships can be represented to describe PHR content in cloud at a conceptual level and to determine PHR

**Author for correspondence*

access permission for users. The access control mechanisms used in health care to regulate and restrict the disclosure of data are often bypassed in case of emergencies. This phenomenon is called "break the glass"[6].

The proposed framework would focus on providing security and privacy in cloud computing. Since, cloud is highly complicated, we feel that it will be difficult to provide a single holistic solution to secure cloud; so, our idea is to choose a specific domain and their applications using cloud, make incremental enhancement to provide security in cloud. Proposed idea in this paper is one among the milestones in our proposed research. The organization of this paper is as follows: In chapter 2, we will discuss related works on various access control models proposed by various researchers and their drawbacks. In chapter 3, we will present of our proposed system with all explanations. In chapter 4, we will discuss about our contribution to healthcare cloud through this paper. The paper is concluded and possible future works are discussed in chapter 5.

2. Related Work

Many types of access control mechanisms are proposed by various researchers which includes Role based[7], attribute based[8], activity oriented[9], capability based[10], relationship based[11], situation based[12], and semantic based[13].

Role based access control is static which may not be suitable for dynamically changing environment. In attribute based access control the access policy is based on the users attributes. We have limited number of users in PHR sharing; hence this approach will not be suitable. In activity oriented approach the user is given with an activity, user is evaluated based on satisfactory level under a specific condition. In relationship based access control, the relationship analyses and device policies and logics to infer what could be accessed. The problem goes intractable when relationship graph and hierarchy grows. Situation schema is used to analyze the situation and give access. Situation can be mimicked by the intruder, so that he gets access.

3. Proposed Work

Our main aim is to provide secured access on users PHR. When Healthcare Service Provider (HSP) creates its account on Cloud Service Provider (CSP), the data are encrypted using ABE and stored on trusted cloud database. The HSP can also update their data sharing policy, which can be done with assistance from CSP. Data integration and sharing in cloud is a new research area with lot of issues. Architecture of the proposed system is represented in Figure 1. The policies for the system instance are collected, which is structured well through Protégé, with the health care system ontology. The access control

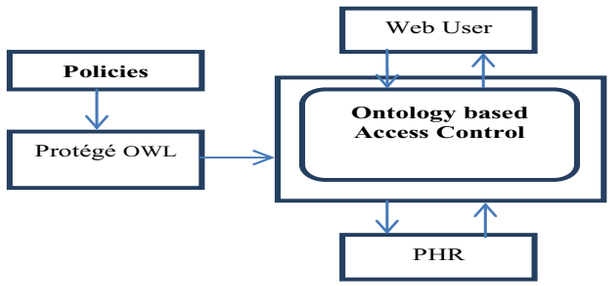

Figure 1. Access control system architecture.

layer screens the PHR with the policies defined for the web users.

HSP may have their data on multiple CSP's. The user of PHR can be broadly classified into two categories, named personal and professional. The personal may be close relations, friends and family members of the patient, while the professional users can be doctor, nurse, researcher, insurance person, pharmacy person etc. The PHR owner may not know the professional users who may access his PHR. We are classifying the attributes of PHR with various levels of authority. Like public attributes (eg. Blood group, sex) personal attributes (eg. address, contact info, Name, SSN) and sensitive attributes (eg. income, case history, diagnosis, lab reports).

The visibilities of these attributes are restricted to a specific user in the healthcare system. Ontology based access control in healthcare system using cloud computing used to explicating the relationships among the healthcare users. The relationship among patients and other healthcare professionals are undefined and unclear. The behaviors among healthcare users, their relationship and boundaries need to be addressed explicitly for the benefit of healthcare application developers.

3.1 Ontological Definition for Health Care System

Health care system involves various entities, the specific requirement are defined alongside importing standard

ontologies eg; person details (vCard Ontology). Further could be extended by specifying the pharmacyItem (a class in our ontology defined for health care system) with standardized ontology (with owl:sameAs property) where, the pharmacyItem in health care ontology will be linked to other standard definition on how a pharmacy item would behave.

Permission (similar to authorization in data applications) is defined as the objectProperty where the entity permitted to do what and by whom.

Protégé is used to define the ontological structure of the PHR. Ontology is coded with OWL standards. Supporting ontologies are SNOMED-CT, vCard ontology which helps to link with personal data of the person, involved in the system. When the vCard is mapped onto the health care system the data of patients will be decentralized but accessed centrally. SNOMED-CT is integrated to structure the health records and laboratory reporting. The vCard ontology is mapped onto health care ontology by the hasVcard object Property whose domain is Person range is vCard. vCard ontology is defined in owl import as follows,

<owl2xml:Import>
http://www.w3.org/2006/vcard/ns
</owl2xml:Import>

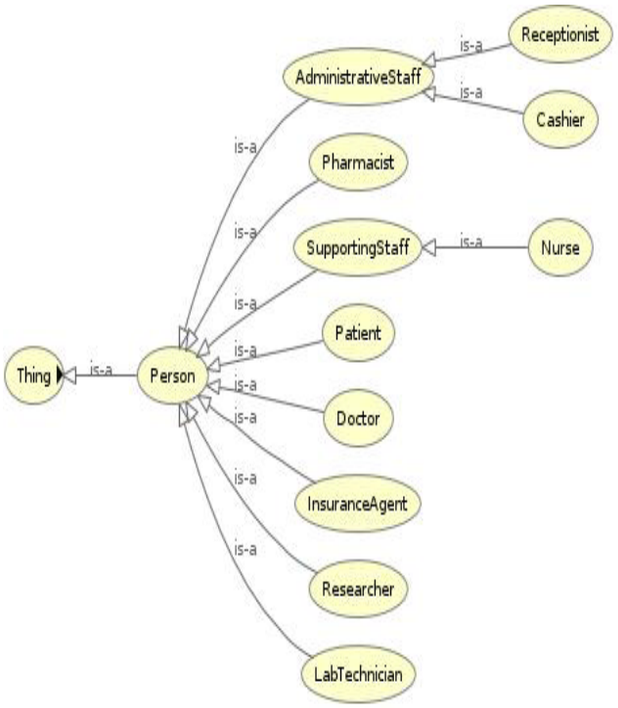

Figure 2. Definition of person in ontology.

The major entities involved in the system are Person and document, where the person could be a doctor, patient, insurance agent etc. Documents are various levels of data created when these persons interact. Ensuring that these documents are accessed only by authorized person plays major role in PHR as the data is highly sensitive and personal. Object properties that can set permission on the document are listed as Object properties in Table 1. Other members of Person class are researcher, pharmacist, lab technician, cashier which is structured as in Figure 2. Document holds lab report, diagnosis report, discharge summary, case history which is structured in Figure 3.

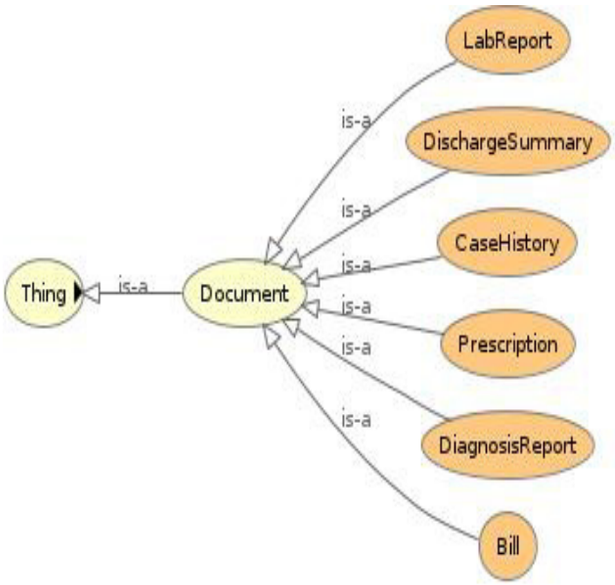

Figure 3. Definition of document in ontology.

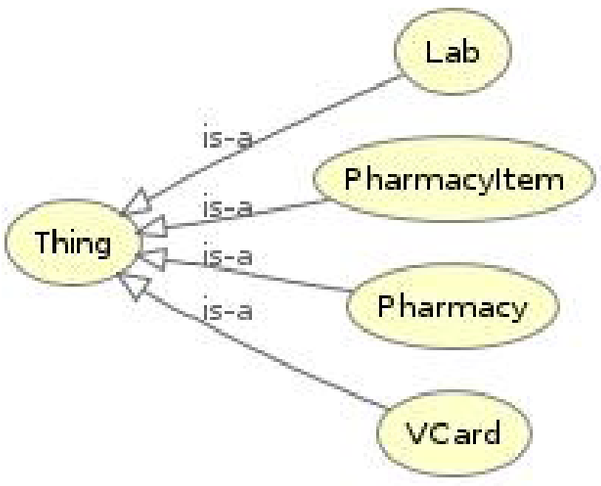

Figure 4. Few other classes defined in ontology.

The other classes like Lab, Pharmacy Item, Pharmacy and vCard are structure in Figure 4. Lab must have a lab technician and he will be the author of lab reports, these are well defined with the object properties. Interaction between the persons can be restricted with the canInteract property. Object properties in OWL is a mapping of entities where the property holds domain and range as entities itself, few properties are listed in Table 1.

Entity defined in OWL can be instantiated by is A property, eg; duri is A person defined In N-Triples format (a format where resource is defined as subject; predicate; object). The intuitive idea behind the object property is, when particular instance is selected, we have the definition of what the data is about with any selected instance, where we could traverse with other instances which are mapped with object property. Eg; when we select a researcher instance we could choose with his vCard instance and in vCard we could choose the address which is an instance and if address has a property person resides we could find who are all staying with the particular researcher, only by having the URI of the instance.

Table 1. Object Properties

(property; domain:range (description))
canInteract; person:person;
createdBy; document:person;
hasResearcher; lab:researcher (sublass of person);
hasTechnician: lab:technician (subClass of person);
hasVcard; vCard:person (links the person details with the vCard Ontology);
permitReadOnly; document:person (permisions for document);
permitReadWrite; document:person;
purchasedBy; pharmacyItem:person;
relatedAsFriend;relatedAFamily; person:person;

Table 2. Data Properties

(property; domain:range (description))
HospitalNo; Person:generatedId;
createdOn; Document:dateTime;

Data properties in OWL is mapping of an Entity with some value like String, Date, Integer. The actual data of any resource will be residing in the data properties. Few of the data properties are listed in Table 2. Table 3 is the definition of an Object Property prescribedBy, which has domain as Prescription which is a subClass of Document and range of that is doctor.

The property prescribedBy itself sub property of createdBy object property. The definition of sample class and equivalence class is given in Table 4, Cashier is a sub class of AdministrativeStaff which in turn is a subclass of Person. The DiagnosisReport is a class which is equivalent to the any object property defined on DiagnosisReportBy whose range is of Doctor.

4. Contribution

The health_care_system.owl has been structured in such a way that the policies, interaction can be defined as an instance of the ontology. The authorization strategy between role and data can lie at any node while it ensures that description of resource is unique. The vCard ontology has been well utilized in the ontology defined, where vCard itself behaves as a document while document has policies implied on it through object properties. Like vCard ontology, much new ontology can be designed based on the dynamic need and that can be used by various HSP to provide access control on users.

Table 3. Sample data property defined in OWL

```
<owl2xml:SubObjectPropertyOf>
<owl2xml:ObjectProperty owl2xml:URI="&health_
care_system;prescribedBy"/>
<owl2xml:ObjectProperty owl2xml:URI="&health_
care_system;createdBy"/>
</owl2xml:SubObjectPropertyOf>
<owl2xml:ObjectPropertyDomain>
<owl2xml:ObjectProperty owl2xml:URI="&health_
care_system;prescribedBy"/>
<owl2xml:ObjectSomeValuesFrom>
<owl2xml:ObjectProperty owl2xml:URI="&health_
care_system;prescribedBy"/>
<owl2xml:Class owl2xml:URI="&health_care_
system;Prescription"/>
</owl2xml:ObjectSomeValuesFrom>
</owl2xml:ObjectPropertyDomain>
<owl2xml:ObjectPropertyRange>
<owl2xml:ObjectProperty owl2xml:URI="&health_
care_system;prescribedBy"/>
<owl2xml:ObjectSomeValuesFrom>
<owl2xml:ObjectProperty owl2xml:URI="&health_
care_system;prescribedBy"/>
<owl2xml:Class owl2xml:URI="&health_care_
system;Doctor"/>
</owl2xml:ObjectSomeValuesFrom>
</owl2xml:ObjectPropertyRange>
```

Table 4. Sample class and equivalent class definition in OWL

```
<owl2xml:SubClassOf>
<owl2xml:Class owl2xml:URI="&health_care_
system;Cashier"/>
<owl2xml:Class owl2xml:URI="&health_care_
system;AdministrativeStaff"/>
</owl2xml:SubClassOf>
<owl2xml:EquivalentClasses>
<owl2xml:Class owl2xml:URI="&health_care_
system;DiagnosisReport"/>
<owl2xml:ObjectSomeValuesFrom>
<owl2xml:ObjectProperty owl2xml:URI="&health_
care_system;DiagnosisReportBy"/>
<owl2xml:Class owl2xml:URI="&health_care_
system;Doctor"/>
</owl2xml:ObjectSomeValuesFrom>
</owl2xml:EquivalentClasses>
```

5. Conclusion and Future Work

The proposed work successfully addresses the problems stated previously, with ontologically defined health care system where interaction between entities is restricted on certain rules and access control is done by permissions which is defined with object properties.

In future the ontological access control for PHR systems could be extended by inference engine. The decision of authorization based upon logics and inferred data which is defined in the policy. It is required that the policy itself to be defined as ontology constructed with certain rules. The inferred data could be accessed by using SPARQL query language in the PHR systems.

6. References

1. Beloglazov A, Buyya R. Energy efficient resource management in virtualized cloud data centers. 10th IEEE/ACM Int Conf Clust Cloud Grid Comput; IEEE; 2010. p. 826–31.
2. Neela T, Saravanan N. Privacy preserving approaches in cloud: a survey. Indian Journal of Science and Technology. 2013 Jan; 6(1):4531–5.
3. Li X, He J. A user-centric method for data privacy protection in cloud computing. International Conference on Computer, Electrical, and Systems Sciences and Engineering; 2011. p. 355–8.
4. Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans parallel Distrib Syst. 2013; 24(1):131–43.
5. Choi C, Choi J, Kim P. Ontology-based access control model for security policy reasoning in cloud computing. J Supercomput. 2013 Jul 19; 67(3):711–22.
6. Ardagna CA, De Capitani Di Vimercati S, Foresti S, Grandison TW, Jajodia S, Samarati P. Access control for smarter healthcare using policy spaces. Comput Secur. 2010 Nov; 29(8):848–58.
7. Tsai W-T, Shao Q. Role-based access-control using reference ontology in clouds. 2011 Tenth International Symposium on Autonomous Decentralized Systems; IEEE; 2011. p. 121–8.
8. Yang K, Jia X, Ren K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems. Proceedings 8th ACM SIGSAC Symp Information, Comput Commun Secur - ASIA CCS '13; New York, USA: ACM Press; 2013. p. 523–8.
9. Le XH, Lee S, Lee Y-K, Lee H, Khalid M, Sankar R. Activity-oriented access control to ubiquitous hospital information and services. Inform Sci. 2010; 180(16):2979–90.
10. Hota C, Sanka S, Rajarajan M, Nair S. Capability-based cryptographic data access control in cloud computing. Int J Advanced Networking and Applications. 2011; 3(3):1152–61.
11. Fong P. Relationship-based access control: protection model and policy language. CODASPY'11; 2011 Feb 21–23; San Antonio, Texas, USA: 2011.
12. Peleg M, Beimel D, Dori D, Denekamp Y. Situation-based access control: privacy management via modeling of patient data access scenarios. J Biomed Informat. 2008; 41:1028–40.
13. Sun L, Wang H, Yong J, Wu G. Semantic access control for cloud computing based on e-Healthcare. Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design; 2012 May. p. 512–8.