RESEARCH ARTICLE OPEN ACCESS

An Effective Security Mechanism for M-Commerce Applications Exploiting Ontology Based Access Control Model for Healthcare System

S.M. Roychoudri[1], Dr. M. Aramudhan[2]
[1]*Research Scholar, Dept. of CSE, Rayalaseema University Kurnool (A.P), India.*
[2]*Asst. Prof, Dept. of IT, Perunthalaivar Kamarajar Inst of Engg&Technology,Nedugadu,Karikal,Puducherry, India.*

ABSTRACT
Health organizations are beginning to move mobile commerce services in recent years to enhance services and quality without spending much investment for IT infrastructure. Medical records are very sensitive and private to any individuals. Hence effective security mechanism is required. The challenges of our research work are to maintain privacy for the users and provide smart and secure environment for accessing the application. It is achieved with the help of personalization. Internet has provided the way for personalization. Personalization is a term which refers to the delivery of information that is relevant to individual or group of individuals in the format, layout specified and in time interval. 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. Personal Health Records sharing is highly expected by the users for the acceptance in mobile commerce applications in health care systems.
Keywords: *Access control, Ontology, Health care , Security*

I. INTRODUCTION

In recent years, m-Commerce has been growing rapidly with the development of the mobile communications and e-business .M-Commerce is the ability to perform commercial transactions using mobile phones or other wireless devices on the move from anywhere and anytime. It is a major application domain for mobile devices where applications require a high level of security. The proposed framework architecture for m-commerce applications is shown in Figure 1. At the beginning, user received USERNAME and PASSWORD from the application authority. In each admissible range of transmission, there is one Authenticated Server (AS). AS check the validity of the user accessing devices with the application. User can submit its security policy to the AS in its admissible range. After authentication of user accessing device, submitted policy is forwarded to the PS. PS collects the history of the user from other ASs, update the policy to that specific user and inform through message to the user. Users can increases their levels of security depends on its category.

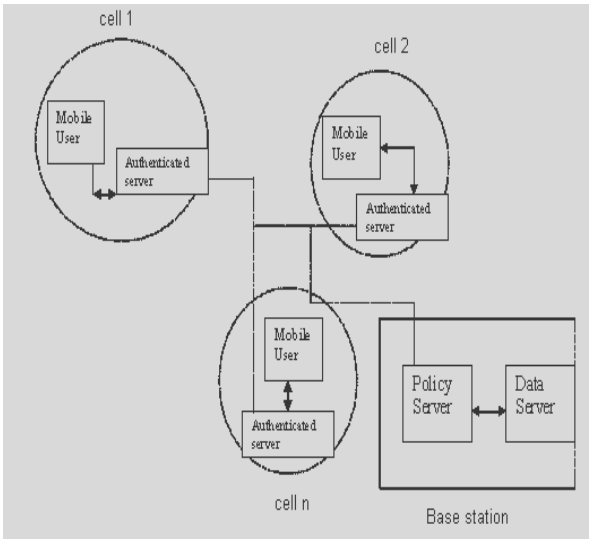

Fig: The Basic Flow Diagram.

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 mobile computing for various benefits. A mobile application promises to offer the

demands of patients and healthcare service providers. There are number of security issues need to be addressed in mobile computing service environments, 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 mobile computing environments. While accessing PHR's in mobile applications, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt their PHR data before accessing. 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. 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 mobile conceptual level and to determine PHR 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".

The proposed framework would focus on providing security and privacy in mobile computing, Proposed idea in this paper is one among the milestones in our proposed research and our research proposal , the challenges in the Mobile E-health system are addressed; the enhancement in security is essential to counter the demand of the mobile users.

II. RELATED WORK

Generally, policies are enforced by either Server Operating System or application authority for the particular user about its behavior to access the applications after authentication. In this proposed framework, users submit their policy through its mobile device to the Policy Server after preliminary authentication assigned by the application authority. The trust of user device is analyzed using authentication protocol in addition to the feasibility of user submitted policy to the application. The levels of security are also changed dynamically depending on the user type of accessing applications. User types are identified using the IP addresses that are stored in the database on the server side. User can change its policy any time from its location as well as increases its levels of security after mutual concern from the application authority. The challenges in our work is given as below

User policy submission protocol is developed for the m-commerce applications for Health system.

Different categories of policies are used in the context and flexibility is analyzed (i.e.)

- Role –based access
- Filter based access
- Collaborative Filter based access

With increasing mobility of populations, patient data may be distributed over many locations in different healthcare systems. Advance in networking technology make it possible interconnect these independent and geographically distributed e-health systems such that healthcare professionals are able to access the patient data and related information from any location at any time. However, the high sensitivity of medical information requires the protection of data integrity, availability, authenticity, confidentiality and privacy towards achieving users trust and acceptance of mobile e-health systems.

The secure mechanisms are required by the mobile e-health system to prevent and protect the confidential information and privacy sensitive patient data between healthcare consumers and providers is paramount in mobile e-health infrastructure. The challenges in the mobile e-health systems are given as detailed below

- Authentication framework is necessary for an environment consisting of distributed resources used by geographically and administratively distributed users. The proposed protocol may be based on either PKI or digital certificates. It should be user friendly access to remotely managed patient data and related information. It is also includes the trust of the user device. It is proposed that the authorization and authentication architecture integrates the new role-based and certificate method.

First, the different security threats oriented to the e-health applications are data eavesdropping and manipulation. The different mechanisms to address these specific threats are data confidentiality and integrity. The following security requirements to be addressed

- An individual should be strongly authenticated and authorized to access their health information.
- An individual should be rights to control access to their protected information.
- Information stored or in transit should be in secure.

- Privacy of the user is maintained with the help of the concept "personalization". The objective of the personalization for the purpose of delivery of information straight forwarded to the entity in the mobile e-health system. It is achieved using new content based and collaborative filtering method.

To maintain different permissions for different users is to examine personalization considerations along with security and privacy. Personalization mechanism initially gathers the health professional and patient information in order to construct a profile that demonstrates the set of descriptors essential to the mobile e-health system. Health professionals and patients permission is accomplished with the following procedures

1. Role based Permissions Individual permissions combined with Group permissions
2. Context based Permissions

Role based permissions is filtered by Team-Context.

Group permission may be combined using aggregation, current team structure and maximum/minimum. In this work, personalization issues are independently from security consideration and the implications of this concept achieves effective, secure and convenient mobile e-health system.

Many types of access control mechanisms are proposed by various researchers which includes Role based, attribute based, activity oriented, capability based, relationship based, situation based, and semantic based.

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 suit- able. 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.

III. PROPOSED WORK

Our main aim is to provide secured access on users PHR. Propose a trust model which includes privacy preserving identity management for distributed e-health system.

-Healthcare consumers maintain a pool of identifiers for use in healthcare services. Without revealing the identity of consumers, health record data from different hospitals can be collected and linked together on demand. A secure architecture is proposed to use the resource or service without disclosing the identity. The security of the interactions among the healthcare professionals is guaranteed by new certification and cryptographic technologies. The challenges in this module are

- To generate identifiers and certificates for requesting clients.
- To ensure the integrity and uniqueness of the identifiers
- To provide identity service and manage the utilization of resources without disclosing its identity.

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

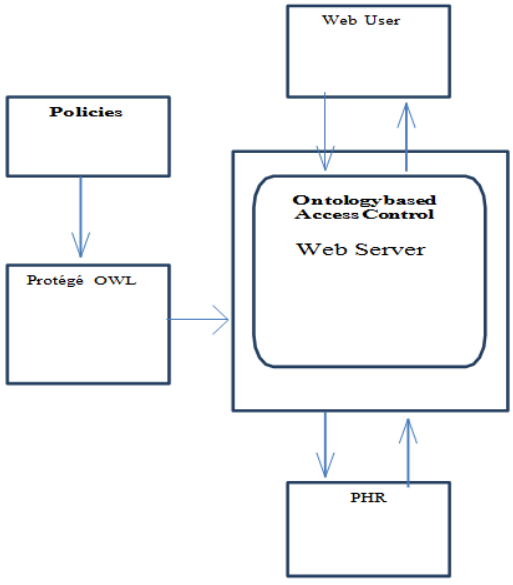

Figure 1. Access control system architecture.

The user of PHR can be broadly classified into two categories, named personal and professional. The personal may be close rela- tions, 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 vari- ous levels of authority. Like public attributes (eg. Blood group, sex) personal attributes (eg. address, contact info, Name, SSN) and sensitive attributes (eg. income, case his- tory, 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 mobile 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 pharmacy Item (a class in our ontology defined for health care system) with standardized ontology (with owl:same As property) where, the pharmacy Item 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 object Property 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 has Vcard object Property whose domain is Person range is vCard. vCard ontology is defined in owl import as follows,

<owl2xml:Import>
http://www.w3.org/2016/vcard/ns
</owl2xml:Import>

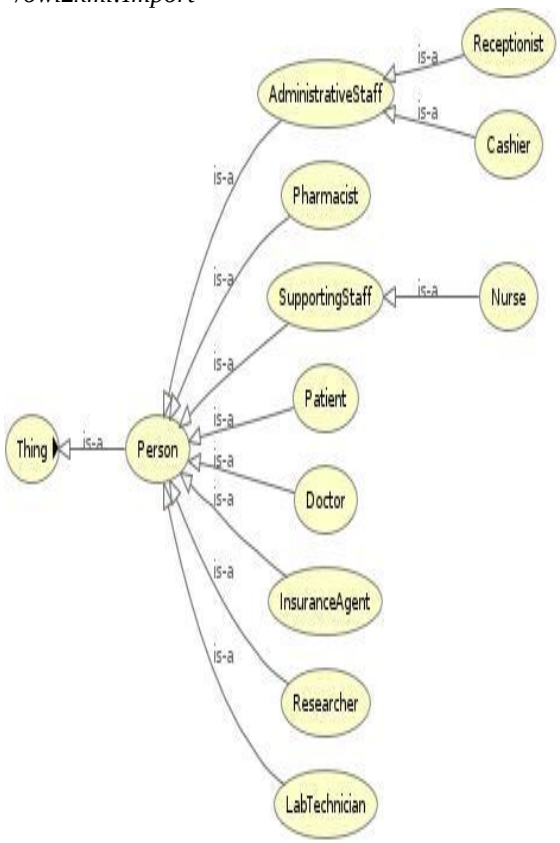

Figure 2. Definition of person in ontology.

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.

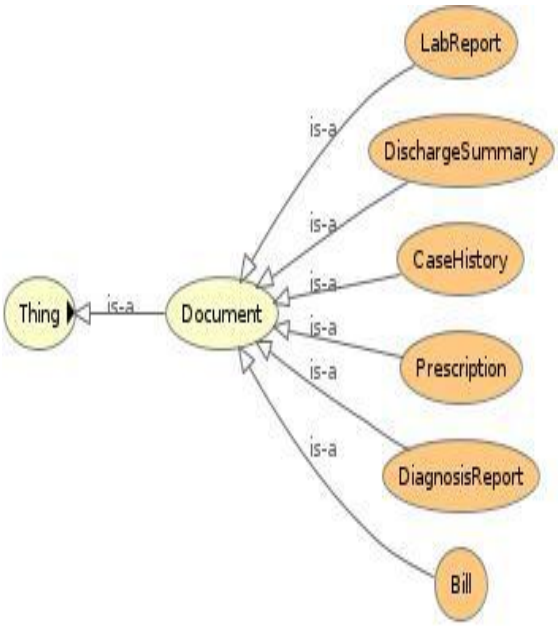

Figure 3. Definition of document in ontology.

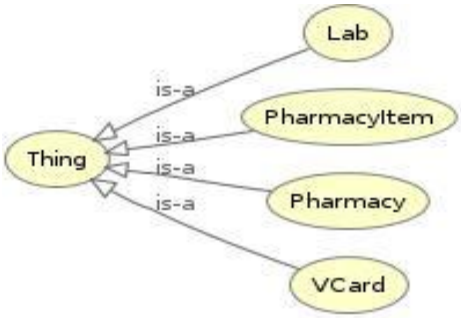

Figure 4. Few other classes defined in ontology.

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);
asVcard; 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 prescribed By, which has domain as Prescription which is a sub Class of Document and range of that is doctor.

The property prescribed By itself sub property of created By object property. The definition of sample class and equivalence class is given in Table 4, Cashier is a sub class of Administrative Staff which in turn is a subclass of Person. The Diagnosis Report is a class which is equivalent to the any object property defined on Diagnosis Report By whose range is of Doctor.

IV. 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: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>
```

V. 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.

REFERENCES

[1]. 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.

[2]. Le XH, Lee S, Lee Y-K, Lee H, Khalid M,

a. Sankar R.Activity-oriented access control to ubiquitous hospital information and services. Inform Sci. 2010; 180(16):2979–90.

[3]. Fong P. Relationship-based access control: protection model and policy language. CODASPY’11; 2011 Feb 21–23; San Antonio, Texas, USA: 2011.

[4]. X. Vila, A. Schuster, and A. Riera, "Security for a Multi-Agent System based on JADE", Computer and Security, Vol. 26, 2007, pp.391-400.

[5]. S. Vitabile, V. Conti, C. Militello and F. Sorbello, (September 2009), "An extended JADE-S based framework for developing secure MultiAgent Systems," Computer Standards & Interfaces, Vol. 31, No. 5, September 2009, pp. 913-930.

[6]. F. Giunchiglia and R. Zhang, "Ontology Driven Community Access Control", Technical Report, University of Trento, Dec. 2008.

[7]. A. Masoumzadeh, and J. Joshi, "Ontology based Access Control for Social Network Systems", Information Privacy, Security and Integrity, Vol. 1, No. 1,2011 .

[8]. H. Shen and Y. Cheng, "A Semantic Context-Based Model for Mobile Web Services Access Control", Computer Network and Information Security, Vol. 1, 2011, pp. 18-25.

[9]. A. LUPAŞC, "A Multi-Agent Platform for Developments of Accounting Intelligent Applications", Economics and Applied Informatics, No. 1, 2008, pp. 79-86.

[10]. F. Bellifemine, ,G. Caire and D. Greenwood, "Developing multi-agent systems with JADE", John Wily & Sons, Ltd, 2007.