Pooja Mohan, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 11, November- 2017, pg. 68-75 ISSN: 2321-8363
Impact Factor: 5.515

Privacy Policies based on Context Awareness in Sensor Network Healthcare Environment

Pooja Mohan
Department of IT, GGDSD College, Panjab University, Chandigarh, India
Email: pooja.mohan@ggdsd.ac.in

Abstract

Personalized health care services have improved the quality of service. To make critical decisions in emergency situations, Hospital workers, require ubiquitous access to real-time patient data. A collaborative system incorporates the immediate alarm notification in critical situation by introducing context-awareness. It helps to support the intensive information management within a healthcare environment. These health care applications are more vulnerable to privacy risks. This study proposes development of ontology for the effective handling of healthcare system problems during an emergency situation.

Keywords: Sensor, context, OWL, SWRL, privacy

1. Introduction

Due to easy availability of information and communication technologies (ICT), ubiquitous computing, ambient intelligence, motes, sensors, and sensor networks is changing the health care. Pervasive healthcare provides services of healthcare to anyone, at anytime, and anywhere by removing restriction of time and location thereby increasing the quality of healthcare. There is scarcity of financial resources for maintenance of hospitals in underdeveloped countries. There are only limited specialized doctors to care for aging population. It is putting too much pressure on the health care system by demising the quality of services.
The only solution for providing better services to the entire population is the use of remote health care assistance. It requires the integration of hardware and software infrastructures in the home environment for collection and decimation of patients' information. The main stakeholders in the healthcare environments are patient, family as well as healthcare service providers. Every pervasive system should incorporate basic encryption to protect the patient's information.

Context-awareness will provide the services to users, by adapting itself to according to dynamically changing environment. An application can adapt itself according to environment based on the context of user. More a system is aware about the user , there are more risks to privacy. It's a prime concern in the healthcare applications where personal sensitive data has to be revealed in everyday life(Tentori, 2006).
This paper is organised as follow. The section II describes the related work on privacy in healthcare. Section III describes the ontological model for health care along with policies to perform reasoning is described. Section IV discusses a scenario to test the model. Section V sums up the conclusion and future scope of the model.

2. Related Work

The quality of healthcare is enhanced by using Ubiquitous computing that is composed of an intelligent environments and smart objects for proactive prevention and diagnosis of diseases. With an increasing use of technology i.e. embedded sensors many privacy issues arise(M. Weiser, 1993). In such an environment, users are not aware about tiny sensors which are deployed to capture their even minute information. The future robots

Pooja Mohan, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 11, November- 2017, pg. 68-75 ISSN: 2321-8363
Impact Factor: 5.515

are disrupting their privacy settings(T. Denning, 2003). The various components used in the environment are pervasive and wireless. So they are more prone to threats like data theft, spoofing and eavesdropping. This raises various privacy issues.

Most of the approaches for privacy protection focuses on enhancing privacy of information which is being collected(M. Langheinrich, 2002). They don't focus on privacy of user in the environment.

As defined by study in (Westin, A.F.,1970) privacy is "the claim of individuals, groups or institution to determine for themselves when, how and to what extent information about them is communicated to others". The study (Ahamed, S.I., 2007), proposes framework for acquisition of data intelligently thereby reducing the data leakage. But it does not talk about how a person can manage their own privacy setting. The authors in (K. Sheikh, 2008) focuses on health tele-monitoring scenario in which the privacy of users is protected through a QoC-based privacy policy framework. Some study(Hong, J.I., 2004) focuses on developing policies for setting privacy that can be used to find friends' in ubiquitous environment. Most of the work proposed privacy policies for ubiquitous computing environment. Researchers have identified various types of limitations and challenges in the solution suggested to maintain the privacy.

The authors (Hu, Jenzhe, 2004) addresses security and privacy solutions that are based on static role based access control model. According to study in (Joshi A, 2008) security-based authentication and role-based approaches are not enough in these systems. The studies propose that due to lack of common policies in ubiquitous environment the system requires dynamic privacy rules (Shankar N, 2002, Bhatti R., 2005, Bhatti R, 2006).

Context awareness can play a key role in this type of situation as it automatically changes the privacy setting assigned to a user with change in context (F. Schaub, 2012). The study in (Motta, Gustavo, 2013) focuses on using context in role based access control for providing authorization services in healthcare services.

3. Context Aware framework

According to the *home scenario*, medical sensors are placed on a patient's body as well as in the environment to sense the physiological data. The Data is being transferred via. base station to centralized server which further forwards the data to the hospital staff with the help of their mobile phones. Raw data collected by sensors are represented semantically in the form of an Ontology.

Various security and privacy policies are represented in the form of rules. Data collected through sensors as well as inferred through policy rules by an inference engine is represented as context ontology. Various decision in healthcare are taken up with the help of alarms and notifications sent by manager module as represented in the Figure 1.

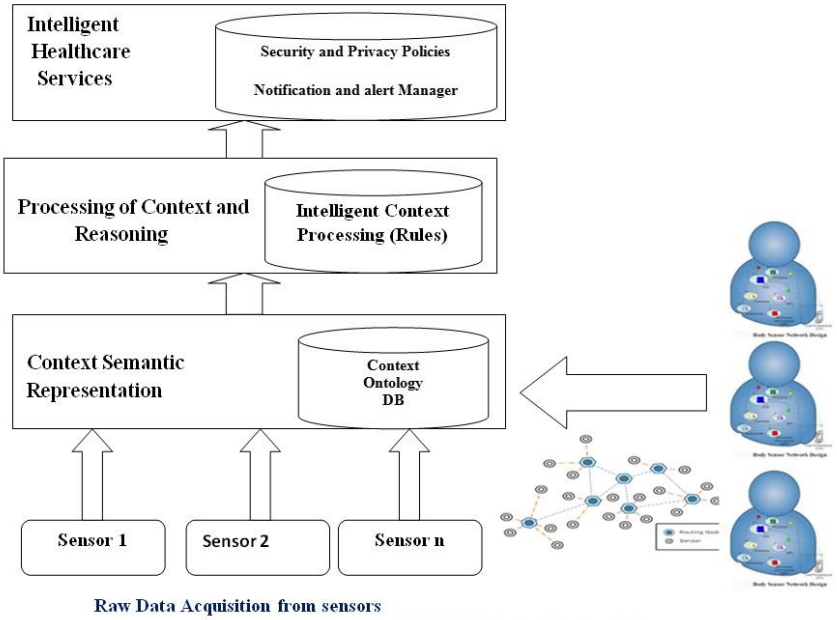

Figure 1: Intelligent Secure Context Aware Framework

Pooja Mohan, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 11, November- 2017, pg. 68-75 ISSN: 2321-8363
Impact Factor: 5.515

Different properties of sensors are captured and analysed whether they are ready to take part in communication. After recording data, they are further checked for any kind of threat. If a threat is detected, which may result in transmitted wrong information in case of an emergency. Such situation which may cause a life threatening for a patient should be avoided. Various policies are represented in the form of rules.
There are various contextual elements in this model. Let C be the set of contexts.
C= { C_1, C_2, C_3, ..., C_N}
C_1 : DeviceContext= { Energy state, Storage level, CPU usage, IP address, Bandwidth}
C_2: NetworkContext = { Network topology, Transmission capacity}
C_3:EnvrContext = {TemperatureLevel, PressureLevel, HumidityLevel, Level_of_Noise, LightingCondition, SeasonType}
C_4:CommCntext = { QualityLevel, EfficiencyLevel, SecurityLevel, FrequencyLevel, AvailabilityLevel, Packet_overhead, Throughput, link_capacity, quality_ of_service (QoS), Signal strength}
C_5 : timeContext= { Domain, time period, Exact Location, time stamp}
C_6: LocContext = { Physical coordinates, location for the user}
C_7: document = { medicalData, prescription, sensitive_health_record}
C_8: RoleContext = { doctor, nurse, physician, accountant, visitor, admin}
C_9: AccessDataContext = { ageAccess, prescriptionAccess, addressAccess}
By represented relation between these sets how they are interrelated with each other we can determine Context Conditional constraint as a Boolean expression to represent security requirements for a sensor network, which is the logical conjunction of explicit conditions.

ContextCC= $\cup_{i=1}^{j}(CC_i)$, $CC = \cap_{i=1} j\ SubC_i$

SubC: = <C><OP><VAL>
Where OP={ >, <, ≤, ≥, =, ≠ }
If C= { time, location }
Ex. Patient record can be accessed from hospital between 9:00 and 4:00
ContextCC=($time$ ≥9:00 ∩ $time$ <16:00 ∩$location\ in\ hospital$)
Privacy Policy Rules can be defined as PPR=(C, P, ContextCC)
Where C is context set, P is permission which is to be assigned based on whether data object can be read, write or update. ContextCC is context conditional constraint.
Ex. Patient health record is very sensitive then only a doctor who is treating the patient located in hospital have the privilege to read it.
if C= { document, Role, location} where C1=document={prescription, medicalData, sensitive_health_record, bank_account_detail}

TABLE I: Privacy Rules based on Data Access

Role	Access Permission on the healthcare data							
	name	**Age**	**address**	**Medical Data**	**Bank Account no**	**prescription**	**location**	**Sensitive Health record**
Visitor	allow	Deny	deny	deny	deny	deny	allow	deny
Pharmacist	allow	Deny	allow	deny	deny	allow	deny	deny
Doctor/Nurse	allow	Allow	allow	allow	deny	allow	allow	allow
insuranceAgent	allow	Allow	allow	deny	deny	allow	deny	deny
Accountant	allow	Deny	allow	deny	allow	deny	deny	deny
Admin	allow	Allow	allow	allow	allow	allow	allow	allow

C2= Role= {doctor, patient, accountant, admin} C3=location= {home, hospital, OT, Ward}
P={ read, write, execute, update} on document
ContextCC=(role="doctor" ∩ document= sensitive_health_record"∩
locatedin="hospital" }
Data access Policy Rule can be defined as DAR={R, P, Dynamic_Context)
here R={doctor}, P={read},

Dynamic_context is a set of values in the Context Set. That is, Dynamic_Context = {v_1 of C_1, v_2 of C_2, …, v_n of C_n}, where C= {C_1, C_2, … C_n}

Dymamic_Context={doctor, sensitive_health_record, hospital}

A read access DAR(R, P, Dynamic_Context) is allowed only if there exists a Privacy Policy Rule PPR (C,P1, ContextCC), such that R ∈ C, P = P1, and ContextCC evaluates to true under Dynamic_Context.

4. Context Aware Ontology

4.1. Scenario

In order to verify the framework, we have taken a scenario in which a person wants to access the patient data. Healthcare systems have complex access rules because of the many persons in the system and their respective access privileges, and context-aware rules.

The members in such an environments are assigned access permission on the basis of roles they are in. A person who was in the role of a doctor and on the duty can also assume the role of a patient.

Various roles assigned are doctor, nurse, physician, pharmacist, an accountant, an administrator, an insurance agent or a visitor etc. A person who is the administrator of the hospital have all the access permission. A doctor/nurse can have different permission to access various types of devices and the information of various patients in the hospital as represented in TABLE 1.

4.2 Ontology Development

We propose a context ontology model for smart healthcare where context reasoning is performed based on semantic web technologies. Due to this feature of semantic web to link information from heterogeneous sources allow ontology to used in various application areas such as medicine, bioinformatics and e-commerce etc. To process the content of information rather than just presenting information to humans an application make use of the Web Ontology Language(OWL). Ontology allow intelligent agents to perform reasoning on contextual information using declarative semantics as predicates written in OWL. It can be used as a knowledge base for sharing information in dynamic systems as well as it also supports the reusability (M. R. Huq, 2007, Y. H. , 2010).

Knowledge Engineering Methodology which is an iterative approach used to identify the various classes, subclasses and properties. There is no specific approach for developing an ontology. It uses an iterative approach of revise and refine to evolve an ontology (F. Gandon, 2002).

We have used Protégé tool for development of our ontology. There are some steps for developing an ontology. First of all it is important to identify the domain and scope of an ontology. It is required to limit the scope of the model that we are going to design. The next is to check whether we can use an ontology that is being defined and used by some other application. After that it's very important to develop the Vocabulary i.e. the list of all items as well as the properties. After all the classes are defined in the model, the class hierarchy is defined. The development process may be top-down, bottom-up and hybrid. Top-down process starts with the defining the most general concept and then to specific. In bottom-up it moves from specific to general. Hybrid is the combination of both approaches(S. Anand, 2010).

We then identified 130 classes during the conceptualization process. Our system adopts an OWL-DL ontology for representing the various types of classes and their relationships.. Fig. 2. shows parts of our ontology.

Pooja Mohan, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 11, November- 2017, pg. 68-75 ISSN: 2321-8363
Impact Factor: 5.515

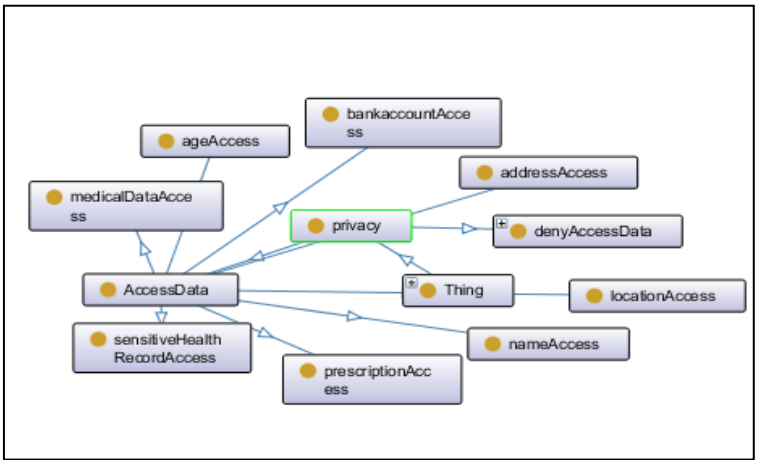

Figure 2: Graphical Representation of Ontology

4.3. Rules

We have created various policies using SWRL (Semantic Web Rule Language). A SWRL rule consists of an antecedent and a consequent. Conditions in the consequent hold whenever the conditions in the antecedent are true. We have defined various rules combining classes and attributes whose values are inferred from sensors. for example, the privacy rules Sen-DataPrivacy-01Admin, SenData-Privacy-01Doctor, and so on in TABLE II denotes the privileges for accessing patient's data.

Table 2: Data Privacy Rules

Data Privacy Rules	
Sen-DataPrivacy-01Admin	person(?x), person(?y), hasName(?y, ?n), name(?n), hasRole(?x,admin), hasRole(?y, patient) -> hasReadAccess(?x, ?n)
Sen-DataPrivacy-01Accountant	person(?x), person(?y), hasDocument(?y, bankAccountDetail), hasRole(?x,accountant), hasRole(?y, patient) -> hasReadAccess(?x, bankAccountDetail) person(?x), person(?y), hasDocument(?y, prescription), hasRole(?x,accountant), hasRole(?y, patient) -> hasnoaccess(?x, prescription)
Sen-DataPrivacy-01Pharmacist	person(?x), person(?y), address(?a), hasAddress(?y, ?a), hasRole(?x, pharmacist), hasRole(?y, patient) -> hasReadAccess(?x, ?a) person(?x), person(?y), age(?a), hasAge(?y, ?a), hasRole(?x,pharmacist), hasRole(?y, patient) -> hasnoaccess(?x, ?a)
Sen-DataPrivacy-01Visitor	Person(?x), person(?y), hasDocument(?y, sensitive_health_record), hasRole(?x, visitor), hasRole(?y, patient) -> hasnoaccess(?x, sensitive_health_record) person(?x), person(?y), hasDocument(?y, bankAccountDetail), hasRole(?x, visitor), hasRole(?y, patient) -> hasnoaccess(?x, bankAccountDetail)
Sen-DataPrivacy-01Doctor	person(?x), person(?y), hasDocument(?y, sensitive_health_record), hasRole(?x, doctor), hasRole(?y, patient) -> hasReadAccess(?x, sensitive_health_record) person(?x), person(?y), hasDocument(?y, bankAccountDetail), hasRole(?x, doctor), hasRole(?y, patient)

	-> hasnoaccess(?x, bankAccountDetail)
Sen-Privacy-01Insurance_agent	person(?x), person(?y), hasName(?y, ?n), name(?n), hasRole(?x, insurance_agent), hasRole(?y, patient) -> hasReadAccess(?x, ?n) person(?x), person(?y), location(?l), locatedin(?y, ?l), hasRole(?x, insurance_agent), hasRole(?y, patient) -> hasnoaccess(?x, ?l)

A person is given access to a device based on whether it's his personal device or belong to hospital. A person is given full access to use its own device. A person can use the device of his friend fully if he has the maximum level of trust. Otherwise limited access is given to a friend with minimum trust level. No access is given to a person who is not the friend. Various privacy rules relating to device access is given in TABLE III.

TABLE 3: Device Privacy Rules

Device Privacy Rules	
Sen-DevicePrivacy-01	person(?x), personalDevice(?h), hasDevice(?x, ?h) -> hasFullAccessDevice(?x, ?h)
Sen-DevicePrivacy-02	person(?x), person(?y), personalDevice(?d), hasDevice(?x, ?d), hasfriend(?x, ?y), hasTrustlevel(?y, lt1) -> hasLimitedAccessDevice(?y, ?d)
Sen-DevicePrivacy-03	person(?x),person(?y), personalDevice(?d), hasDevice(?x, ?d), nofriendof(?x, ?y) -> hasnoaccessDevice(?y, ?d)
Sen-DevicePrivacy-04	person(?x), person(?y), personalDevice(?d), hasDevice(?x, ?d), hasfriend(?x, ?y), hasTrustlevel(?y, gteq1) -> hasFullAccessDevice(?y, ?d)

4.4 Prototype for Health care environment

A prototype of virtual Simulated environment is created to test the inference. Pellet reasoning engine is used here to infer higher level concepts. The various Sensor network parameters are specified using the interface designed. A situation is inferred using inferring higher level rules using low level rules based on primitives parameters.

We implemented a prototype to test the inference and reasoning functionalities of our system. A simulated user interface environment is implemented on a desktop PC. We used the Pellet (version 2.0) reasoning engine on the Jena Platform to infer high-level situations.

The patients' physiological characteristics are specified using the user interface or the visual simulator. When a collection of primitive contexts is given as input, the server applies low level class rules to infer a situation. Then, the application rules are used to determine the patients' health condition as well as corresponding triggering of alarms. The RDF/OWL version of part of the context ontology for the study is given in Fig. 3. Sensed context is to be communicated using XML/RDF triple representation format.

```
.....
<swrl:body>
        <rdf:Description>
          <rdf:type rdf:resource="&swrl;AtomList"/>
          <rdf:first>
            <rdf:Description>
              <rdf:type rdf:resource="&swrl;ClassAtom"/>
              <swrl:classPredicate rdf:resource="&untitled-ontology-300;person"/>
              <swrl:argument1 rdf:resource="urn:swrl#x"/>
```



```
            </rdf:Description>
          </rdf:first>
          <rdf:rest>
            <rdf:Description>
              <rdf:type rdf:resource="&swrl;AtomList"/>
              <rdf:first>
                <rdf:Description>
                  <rdf:type rdf:resource="&swrl;ClassAtom"/>
                  <swrl:classPredicate rdf:resource="&untitled-ontology-300;person"/>
                  <swrl:argument1 rdf:resource="urn:swrl#y"/>
                </rdf:Description>
              </rdf:first>
              <rdf:rest>
                <rdf:Description>
                  <rdf:type rdf:resource="&swrl;AtomList"/>
                  <rdf:first>
                    <rdf:Description>
                      <rdf:type rdf:resource="&swrl;IndividualPropertyAtom"/>
                      <swrl:propertyPredicate
.....
```

Figure 3: Snapshot of ontology representation using XML/RDF

5. Conclusion

This study represents a context aware privacy policies framework for providing healthcare services to patient in a secure environment. We have used an ontology based approach to provide best care facilities to a patient without disclosing his identity. We have built an ontology and a set of rules on the basis of a scenario in which a patient is critical and requires an immediate treatment. A prototype is simulated to test the environment. The model incorporates issues relating to privacy in healthcare. The future scope of the study plans to propose an architecture for a trust based policies in the healthcare environment.

References

[1] Ahamed, S.I., Talukder, N., Kameas, A.D. (2007) "Towards privacy protection in pervasive healthcare. Intelligent Environments", IE 07. 3rd IET International Conference, 296-303

[2] Bhatti R, Moidu K, Ghafoor A.(2006) "Policy-based security management for federated healthcare databases (or RHIOs)", HIKM '06 Proceedings of the International Workshop on Healthcare Information and Knowledge Management. New York, NY: ACM.

[3] Bhatti R. X-GTRBAC (2005), "An XML-based policy specification framework and architecture for enterprise-wide access control". ACM Transactions on Information and System Security ;8(2):187–227.

[4] F. Gandon(2002), "Ontology Engineering: a survey and a return on experience, Research Report of INRIA n°4396, France.

[5] F. Schaub, B. Konings, M. Weber, and F. Kargl (2012). "Towards Context Adaptive Privacy Decisions in Ubiquitous Computing". In PerCom'12 WiP. IEEE.

[6] Hong, J.I., Landay, J.A.(2004) "An architecture for privacy-sensitive ubiquitous computing". Proceedings of the 2nd international conference on Mobile systems, applications, and services. ACM, Boston, MA, USA

[7] Hu, Jenzhe, and Alfred C. Weaver (2004). "Dynamic, context-aware access control for distributed healthcare applications." *Workshop on Privacy, Security, and Trust*. 2004.

[8] Joshi A, Finin T, Kagal L, Parker J, Patwardhan A. (2008), "Security policies and trust in ubiquitous computing". Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences ;366(1881):3769–3780

[9] K. Sheikh, M. Wegdam, and M. V. Sinderen (2008). "Quality-of-Context and its use for Protecting Privacy in Context Aware Systems". Journal of Software, 3(3):83-93.

[10] M. Langheinrich (2002). "A privacy awareness system for ubiquitous computing environments". In UbiComp'02. Springer.

[11] M. R. Huq, N. Thi, T. Tuyen, and Y. Lee(2007), "Modeling an Ontology for Managing Contexts in Smart Meeting Space.", pp. 96-102

[12] M. Weiser (1993). "Some computer science issues in ubiquitous computing". Comm. of the ACM, 36(7):75-84

[13] Motta, Gustavo HMB, and Sergio S. Furuie.(2003), "A contextual role-based access control authorization model for electronic patient record." *Information Technology in Biomedicine, IEEE Transactions on* 7(3) : 202-207.

[14] S. Anand and A. Verma(2010), "Development of Ontology for Smart Hospital and Implementation using UML and RDF," 7(5), pp. 206–212.

[15] Shankar N, Balfanz D (2002). "Enabling secure ad-hoc communication using context-aware security services". Proceedings of UBICOMP 2002-Workshop on Security in Ubiquitous Computing; UBICOMP 2002; Gothenburg, Sweden.

[16] T. Denning, C. Matuszek, K. Koscher, J. R. Smith, and T. Kohno (2009). "A spotlight on security and privacy risks with future household robots". In Ubicomp'09. ACM.

[17] Tentori, Mónica, Jesús Favela, and Victor M. González(2006). "Quality of Privacy (QoP) for the Design of Ubiquitous Healthcare Applications." *J. UCS* 12.3 : 252-269.

[18] Westin, A.F. (1970). "Privacy and Freedom". The Bodley Head Ltd

[19] Y. H. -, S. K. -, and Y. J. (2010), "A Context-Aware Framework using Ontology for Smart Phone Platform," *Int. J. Digit. Content Technol. its Appl.*, 4(5), pp. 159–167.

