Purpose engineering for Contextual Role-Based Access Control (C-RBAC)

Muhammad Nabeel Tahir m_nabeeltahir@hotmail.com
Multimedia University, Melaka
75450, Malaysia

Abstract

Distributed and ubiquitous computing environments have brought enormous efficiency to the collection, manipulation and distribution of information and services. Although this efficiency has revolutionized countless organizations but it has also increased the threats to individual's privacy because the information stored within the collection of heterogeneous distributed components is sensitive and requires some form of access control. The way to protect privacy in this age of information technology requires such access control system that can accommodate organization requirements to protect privacy of individuals with ease in management and administration of resources. Among those requirements, purpose inference is one of the major problems as the total access control decision mainly relies on the user intentions/purposed. This work in this paper is an attempt to provide purpose engineering semantics that we use for the proposed contextual role-based access control model (C-RBAC) in order to comply with HIPAA.

Key words: Purpose Engineering, Intentions, C-RBAC, Purpose Hierarchy

1 INTRODUCTION

With the development of distributed healthcare systems and pervasive availability of information, prevention of fraud and abuse has become an ever greater issue. The introduction of HIPAA law provides a framework for ensuring the security of medical data especially the electronic versions and maintaining patients' privacy. Care is needed to ensure that every pervasive healthcare system maintains the privacy of personal health information by implementing comprehensive solutions that are both technically sound and legislatively compliant. On the other hand, unauthorized disclosure of health information can have serious consequences including refusal of prospective employment, difficulties in obtaining or continuing insurance contracts and loans, and personal embarrassment [1]. Many studies resulted frameworks, languages, models to preserve privacy of patients. Privacy in [2] has been defined as "The right of an individual to be secure from unauthorized disclosure of information about oneself that is contained in documents".

An access control model based on RBAC to protect privacy in a distributed health care information systems, based on the notion of consent, has been presented in [3]. The authors argued that constraints in RBAC do not provide an elegant solution especially with the role hierarchies. For example if a constraint is applied to the role of a doctor, then its child role (podiatrists) will also inherit the constraints of the role. Therefore it is not easy to execute a policy of the form provide access to all doctors except Dr. X. In their work, a patient's access policy have been recorded and enforced through a consumer centric role called care-team role (CTR) that consists of four main components: list of roles that has been allowed to access patient's health information, list of roles that have been denied to access to patient’s health information, the access privileges, and administrative information about the CTR such as its ID and description. A similar approach has been proposed [4]. However, their work does not provide any mechanism to ensure the mapping of patient formalized policies and consents into CTR. Overall there has been no concrete framework of RBAC with privacy-based extensions. An extended framework of RBAC with privacy based extensions to control information access in e-Health has been presented [5]. Authors proposed an aggregation decision-making layer interacted with a set of autonomous RBAC models to aggregate PHI in e-Health care informatics. Although semantic definitions of role authorization with purposes, recipients, retentions and obligations as sets of privacy-based entities has been provided, their work has not shown how these privacy-based entities can be engineered and enforced into e-Health framework. The work also has not provided any purpose driven approach, purpose hierarchies and relationships between subject roles and purposes (spatial purpose role).

The info space concept as the trust boundary and the privacy tag for privacy control in ubiquitous systems has been presented in [6]. Jiang & Landay [7] discussed how the user can be notified about data collection by sensors and how a policy can be negotiated. However these two privacy frameworks referred to a general ubiquitous computing or context-aware computing environment and have not been directly applicable to healthcare information systems. More relevantly, the work [8] analyzed the dependability issues in U-Healthcare. Beckwith [9] discussed the perception of privacy based on the case study of a sensor-rich, eldercare facility. The work in [10] presents a method to control access to any sensor data recorded by a personal ubiquitous healthcare system. Their approach has been based on the concept of mediator that logically sits between a personal healthcare system used by the patient and any clinical system used by the caregiver. However, their proposed architecture does not cope with such dynamic requirements of ubiquitous environment. On the other hand, many information privacy and security laws tailored their protections according to the purpose of the use or disclosure, rather than basing that solely to the particular characteristics of the data itself. Purposes present user’s intentions for which he/she requests access to use resources. Few definitions of purposes have been described in the literature. For example, purpose “an anticipated outcome that is intended or that guides your planned actions” [11]. Purpose in [12] has been described as the reason for which organizations’ resources are used. P3P [13] defined the purpose as “the reason for data collection and use” and specify a set of purposes including current, admin, contact, telemarketing etc.

2 Purpose Context

There are several ways to capture purposes/intentions of the user who request to access resources. First possible method is to register each application with an access purpose. As applications have limited capabilities and can perform only specific tasks, it should be ensured that data users use them to carry out only certain actions depending on the associated access purposes. This method, however, cannot be used in distributed and ubiquitous environment for applications as it may access various data and resources for multiple purposes. Another possibility is to state access purpose(s) along with the requests to access organization resources and confidential data. Although this method is simple and can be easily implemented however, the overall privacy that the system is able to provide relies entirely on the users’ trustworthiness as it requires complete trust on the users. Lastly, the access purposes can be dynamically determined by the system based on the current context. For example, consider the case where the user with the role DayDutyDoctor sends a request to access a patient record. From this context (i.e., the job function, role, the nature of the data to be accessed, the application identification, time of the request, location of doctor), the system can reasonably infer that the purpose of the data access must be “routine checkup”. The advantage of this approach is that many access purposes can be defined for the same values of context information in order to provide a flexible way of making access control decisions. However the key challenge for implementing this method is to engineer context information accurately and efficiently. This work has defined purpose for C-RBAC model as:

Definition 1 ***(Purpose)*****:** Purpose is the intention of the user that is computed based on the contextual values of the user's current environment through which the user is requesting access to use resources.

$$Purpose\ p \rightarrow SPR{\times}T{\times}LOC\_ATR$$

where SPR ∈ Spatial purpose roles, T is time interval borrowed from Joshi, Bertino, Latif, & Ghafoor [14, 15] and LOC_ATR is a set of attributes e.g. user motion direction, motion speed, user location and distance from resource such that given the user session s, SLOC_ATR (s:SESSION) represents the current contextual values for the session s activated by the user u.

$$LOC\_ATR: \bigcup_{s \in SESSION} SLOC\_ATR(s)$$

The number of contextual variables and its values may vary based on the organizations' requirements. For example, some organizations may consider time t, and role r, of the user u to compute the purpose of the user. For example, if user u (Bob) with the role r (doctor) sends a request to access a patient record pr of patient between 7am to 7pm, then the purpose p is RoutineCheckup. Similarly, some organizations may consider time t, location l and role r of the user u to compute the purpose of the user. For example, if user u (Bob) with the role r (doctor) sends a request to access a patient record pr of patient from general ward where patient is admitted then the purpose p is RoutineCheckup. In order to elaborate further, consider the scenario in Figure 1 where there are four departments in a hospital: ICU Ward, General Ward, Laboratory and X-Ray Department. Assume that Bob, a cardiologist doctor is assigned to ICU ward. He is also attached to Laboratory as the Laboratory Head. When Bob login into the system, the system will automatically enable the roles that are assigned to Bob depending on his location. In this scenario, Bob will get all the roles that are assigned to him at the location of ICU Ward. Assume that for some reason, either for a normal routine checkup or for emergency calls, he has to go to the General Ward. When Bob walks to the General Ward, he will pass two other departments, i.e. Laboratory and X-Ray Department. The system can easily get the physical position of Bob through GPS (external), access points or sensors (internal) and computes the logical location of Bob. If the relative location overlaps between two regions for example the doctor's logical location overlaps with the Laboratory and X-Ray Department, then all the roles that are assigned to Bob will be enabled automatically although Bob is on his way to General Ward. However, if the system is capable of monitoring the user movement direction then it can easily infer that Bob's intention is to go to the General Ward rather than Laboratory or X-Ray Department.

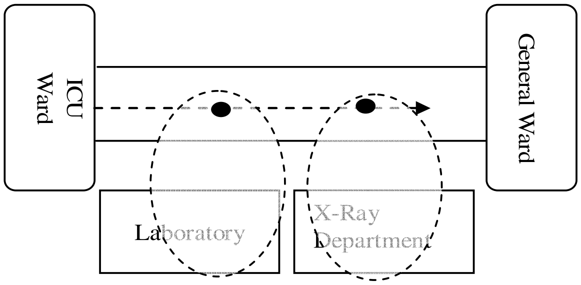


Figure 1: Relative Location Overlapping.

2.1 PURPOSE HIERARCHY

Like subject roles, purposes also have a hierarchical relationship among them. For instance, the purposes MinorOperations and MajorOperations can be grouped together by a more general purpose Operation. This suggests that purposes can be organized in hierarchical relationships to simplify the management of the purposes. The hierarchical relationship among different purposes is shown in figure 2 where each node represents the purpose and each edge represents the parent/child relationship. The next definition formalizes the above discussion.

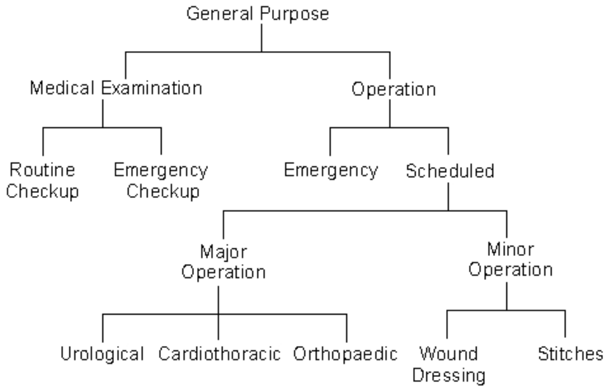


Figure 2: Purpose Hierarchy in C-RBAC.

Definition 2 ***(Purpose Hierarchy)***: Let P be a set of purposes defined within the system. A hierarchical relationship is defined with ≤ between purposes such that pi ≤ pj means that pj is child of pi or pi is a parent of pj.

Figure 2 shows an example of hierarchical relationship between purposes. MajorOperation ≤ Cardiothoracic means that purpose MajorOperation is a parent purpose of Cardiothoracic. In another words, the subject role or location assigned to the purpose MajorOperation will also be assigned automatically to Cardiothoracic.

Another novelty in this work has been the definition of relation between purposes and locations. A notion of spatial purpose (SP) is introduced that is defined as a purpose in relation with location. It must be noted that multiple spatial purposes can be defined at one particular location, LHS and LHI level.

Definition 3 ***(Spatial Purpose)***: Spatial purpose is a purpose defined over a particular location such that;

Spatial Purpose SP <sp, lloc, p>

where sp is spatial purpose name such that sp ∈ P (universal set of all spatial purposes defined in a system) and lloc is a logical location such that lloc ∈ LLOC, defining the boundaries for sp and p is a purpose such that p ∈ P.

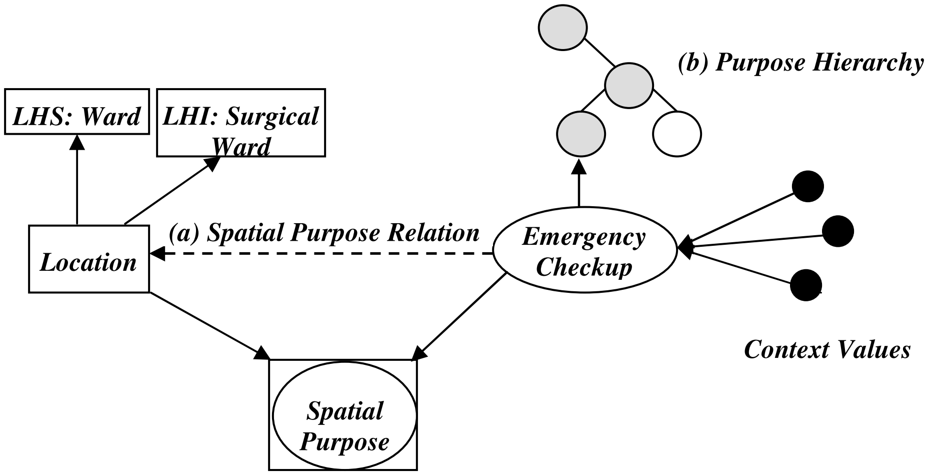


Figure 3: Spatial Purpose (*SP*) Relationship.

Figure 2 shows (a) hierarchical relation between purposes as defined in figure 3 and (b) spatial purpose relation in which purpose *EmergencyCheckup* is defined over logical or physical location.

2.2. SPATIAL PURPOSE WITH LHS AND LHI

In common business environments it is also possible to define spatial purposes for a group of hierarchically organized locations. The proposed spatial purpose engineering is flexible enough to allow security administrator to define spatial purposes for LHS in order to allow a group of users to perform common departmental activities with generalized purposes. For example if the hospital policy states that all medical staff in wards can check the availability of medical doctors in all wards for the purpose of emergency checkup then a spatial purpose can be defined at LHS:Ward level to allow all medical staff in wards to acquire EmergencyCheckup purpose. The advantage of this approach is that spatial purposes can be defined only once and assigned to LHS that propagates spatial purpose to all nodes of hierarchically organized logical locations. This reduces the overhead of defining the same spatial purposes for different logical locations. It also eases the management of spatial purposes especially in large organizations where a same purpose is required at many different locations. As LHS can have many instances (LHI) [16]; each defined with a unique name. This means that spatial purposes defined at LHS level will also be assigned to all instances (LHI) instantiated through LHS. Additionally, spatial purposes can also be defined at LHI level. This is a case where organizations want to allow users from some specific locations to acquire purposes to perform activities. For example if the hospital management wants to allow only those staff members who are on duty in surgical ward to check the availability of medical doctors for emergency checkup then spatial purpose EmergencyCheckup will be defined at LHI:SurgicalWard level only to allow staff in surgical ward only to acquire EmergencyCheckup purpose.

Figure 3 shows spatial purposes defined at LHS:Ward and LHI:SurgicalWard level along with a set of purposes (through hierarchical relationship) {MajorOperation, Scheduled, Operation and GeneralPurpose} for all wards as <EmergencyCheckup, Ward> at LHS level and for surgical ward only as <EmergencyCheckup, SurgicalWard> at LHI level.

Definition 4 ***(Spatial Purpose with LHS)*****:** Let lhs is location hierarchy schema and p is a purpose such that p $\in$ P and lhs $\in$ LHS, spatial purpose with LHS is defined as:

Spatial Purpose SPlhs <splhs, p, lhs>

where splhs is a spatial purpose name, p is a purpose defined at lhs. SPLS is defined as a spatial purpose logical location set, a set of logical locations defining the boundaries of splhs such that LhsOccurencelloc(lhs) → SPLS = {lloc1, lloc2…llocn}, where lloc ∈ LLOC.

Definition 5 ***(Spatial Purpose with LHI)*****:** Let lhi is location hierarchy schema and p is a purpose such that p ∈ P and lhi ∈ LHI, spatial purpose with LHI is defined as:

Spatial Purpose SPlhi <splhi, p, lhi>

where splhi is a spatial purpose name, p is a purpose defined at lhi. SPPS is defined as a spatial purpose physical location set, a set of physical locations defining the boundaries of splhi such that LhiOccurenceploc(lhi) → SPPS = {ploc1, ploc2…plocn}, where ploc ∈ PLOC.

Spatial Purpose with SDOM:

As explained in [17], domains may have multi-domain and multilevel-domain relationships among them as spatial domains are defined over LHS and LHI. Another novelty in this work is the definition of two types of relationships between purposes and spatial domains Internal Spatial Purpose relationship (INT_SPSDOM) and External Spatial Purpose relationship EXT_SPSDOM. A relationship INT_SPSDOM exists when a purpose p defined at SDOM level to be inherited to all schemas or instances within spatial domain. These relationships are represented as:

Definition 6 (Spatial Purpose with Spatial Domain): Let SDOM is spatial domain and p is purpose such that p ∈ P, we define INT_SPSDOM as:

(a) Spatial Purpose INT_SPSDOM <spSDOM, SDOM, p>

It is mentioned earlier that spatial domains are defined over LHS and LHI. In case of SDOM over LHS, SS is defined as schema set that contains location hierarchy schemas covered within SDOM such that SS → SchemaDomain(SDOM) = { lhs1, lhs2,… lhsn }, where lhs ∈ LHS and PSET as purpose set that contains purposes defined at spatial domain level such that PSET → GetParentPurposes(p) = { p1, p2,… pn }. Similarly IS as a set of location hierarchy instance covered within SDOM through LHI such that IS → InstanceDomain(SDOM) = { lhi1, lhi2,… lhin }, where lhi ∈ LHI.

EXT_SPSDOM relationship defines spatial purposes at domain level so that whenever a user from one domain such as SDOM1 sends request to access resource of another domain SDOM2, SDOM2 grants/denies access to resource based on the type of user request and the EXT_SPSDOM spatial purpose relationship defined with SDOM1. For example, a research domain may establish Research purpose relationship with laboratory domain in order to access PHI for the purpose of research. Similarly an insurance company may access patient insurance information from hospital for the purpose of InsuranceClaim as shown in figure 4.

(b) *Spatial Purpose* EXT_SP_{SDOM} $<SDOM_i, SDOM_j, p>$

where p is a purpose describing that SDOMi can access the resources of SDOMj for the purpose(s) defined in PSET.

Figure 4 shows that purposes defined through INT_SPSDOM relation over surgical and emergency domain are inherited at all respective locations (physical and logical locations through lhs and lhi) based on their inclusion within spatial domain whereas purpose defined through the relation EXT_SPSDOM between emergency ward and laboratory shows that emergency ward domain can access test results in laboratory for the purpose EmergencyCheckup.

By definition [17] (a), relationship can be defined as INT_SPSDOM <Emergency, EmergencySDOM, EmergencyPurpose> means that access request for the purpose of EmergencyCheckup can be made from all locations defined within the domain EmergencySDOM in order to access its resources. The logical location set SS in this case will be generated as SS = {Ward, Ward} and it will further propagate purposes to all logical/physical locations covered by Emergency domain such that { PatientFloor, StaffFloor, Reception, EmergencyRoom, TempObrArea, NurseOffice, DoctorOffice}. Similarly by definition of spatial purpose over domains [17] (b), EXT_SPSDOM relationship between two spatial domains can be defined as <EmergencySDOM, LaboratorySDOM, EmergencyCheckup> which means that request from EmergencySDOM to LaboratorySDOM can only be granted for the purpose EmergencyCheckup.

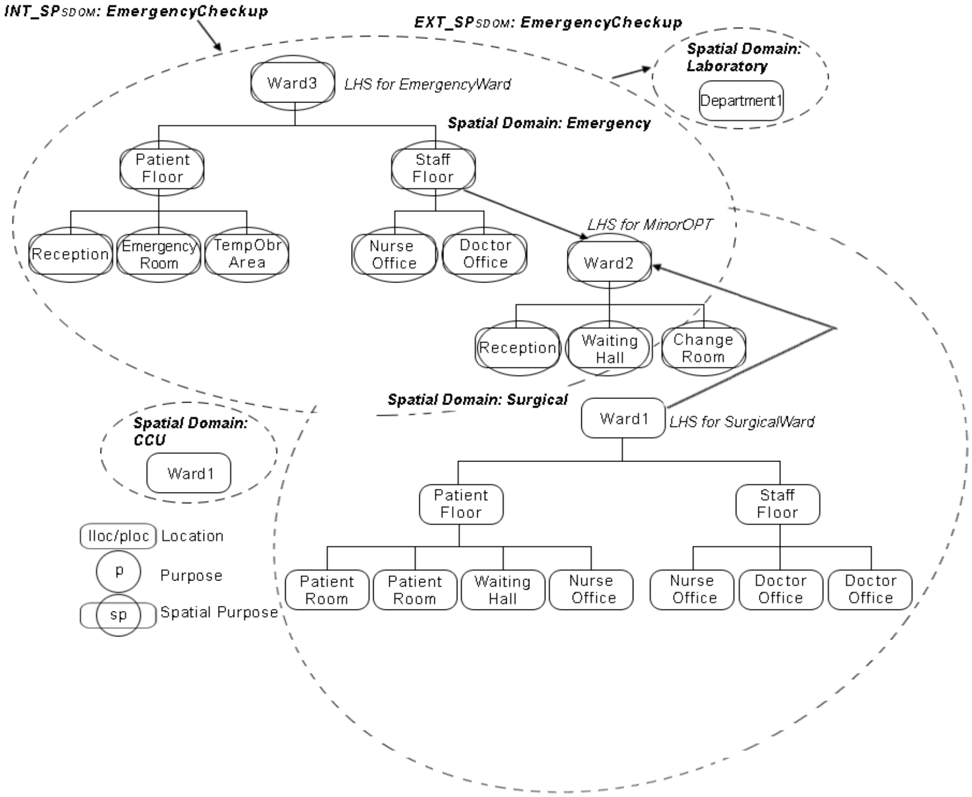
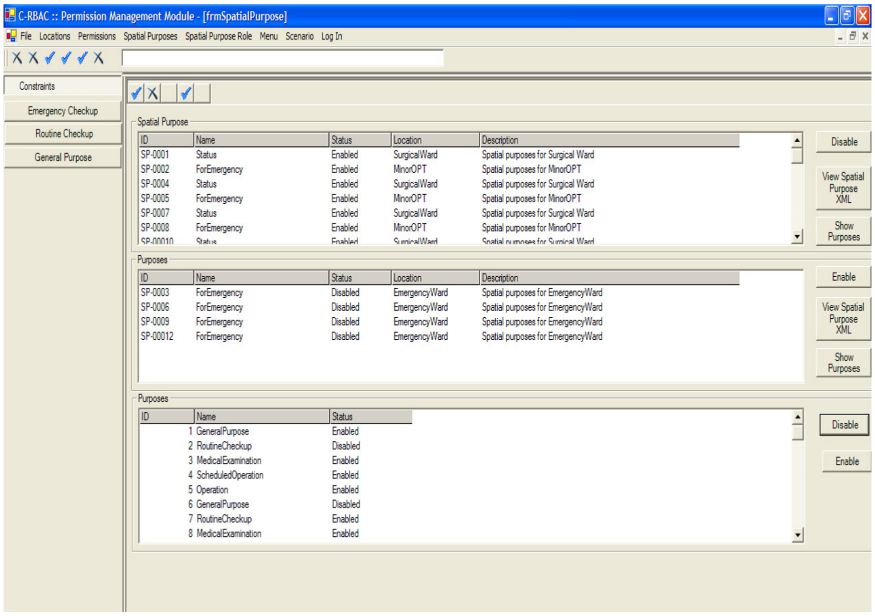


Figure 4: Spatial Purpose Relationships Defined Over Spatial Domain.

2.3 PURPOSE MODULE AND SPECIFICATION TOOL

Figure 5 shows GUI for purpose specification tool and figure 6 shows the architectural representation of purpose module. Context Collector collects contextual values from the underlying technology. Context Generator then assigns these collected values to context attributes defined for C-RBAC model based on which Purpose Inferor deduces the purpose of the user. Purpose Manager (PM) manages all purposes within the system including addition or edition of purposes. Purpose Activator (PA) activates/deactivates purposes based on the constraints defined for context values. Based on the purposes defined through PM, Purpose Hierarchy Manager (PHM) defines and manages hierarchical relationships among purposes. SP Manager manages the Spatial Purpose (SP) relationship defined between location and purpose.

SP-LHS Allocator defines SP between LHS and purpose whereas and SP-LHI Allocator defines SP between LHI and purpose. As all purposes defined for LHS will be propagated at LHI level. This propagation of purposes from LHS to LHI is done by SP Propagator. Lastly, SP-SDOM Relationship Manager manages relationship between SDOM and purposes based on the spatial relationships (INT_SPSDOM, EXT_SPSDOM).



Spatial Purpose

ID	Name	Status	Location	Description
SP-0001	Status	Enabled	SurgicalWard	Spatial purposes for Surgical Ward
SP-0002	ForEmergency	Enabled	MinorOPT	Spatial purposes for MinorOPT
SP-0004	Status	Enabled	SurgicalWard	Spatial purposes for Surgical Ward
SP-0005	ForEmergency	Enabled	MinorOPT	Spatial purposes for MinorOPT
SP-0007	Status	Enabled	SurgicalWard	Spatial purposes for Surgical Ward
SP-0008	ForEmergency	Enabled	MinorOPT	Spatial purposes for MinorOPT
SP-00010	Status	Enabled	SurgicalWard	Spatial purposes for Surgical Ward

Purposes

ID	Name	Status	Location	Description
SP-0003	ForEmergency	Disabled	EmergencyWard	Spatial purposes for EmergencyWard
SP-0006	ForEmergency	Disabled	EmergencyWard	Spatial purposes for EmergencyWard
SP-0009	ForEmergency	Disabled	EmergencyWard	Spatial purposes for EmergencyWard
SP-00012	ForEmergency	Disabled	EmergencyWard	Spatial purposes for EmergencyWard

Purposes

ID	Name	Status
1	GeneralPurpose	Enabled
2	RoutineCheckup	Disabled
3	MedicalExamination	Enabled
4	ScheduledOperation	Enabled
5	Operation	Enabled
6	GeneralPurpose	Disabled
7	RoutineCheckup	Enabled
8	MedicalExamination	Enabled

Figure 5: GUI of Purpose Module for C-RBAC.

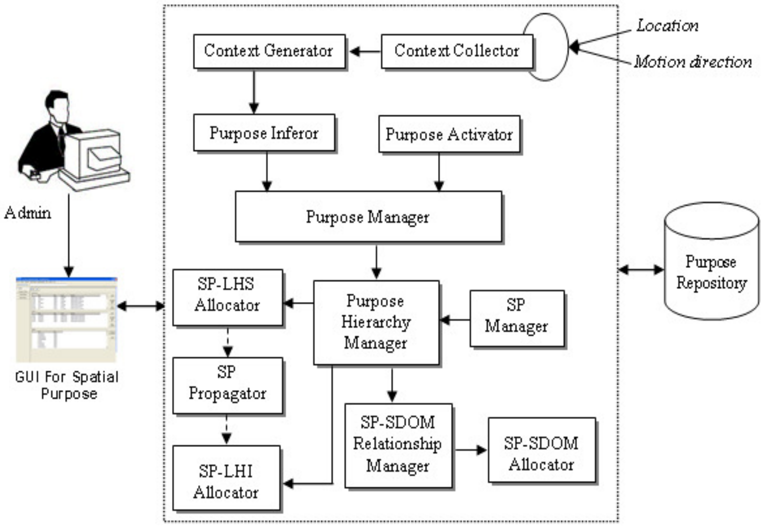


Table 1: Purpose and Spatial Purpose Functions.

Table 1 shows purpose and spatial purpose functions used by purpose module. These functions are used to add a new purpose, to infer the purpose based on the context values, to check the state of the purpose that whether the given purpose is parent or child, to retrieve parent/child purposes, to retrieve purposes defined at different spatial granularities.

3 CONCLUSION

In this paper, purpose model for contextual role-based access control model has been presented for privacy access decisions. Purpose semantics and some definitions including purpose, purpose hierarchy, purpose relation with location model (spatial purpose) have been presented that will be used by C-RBAC model in order to make privacy aware access control decisions. In order to support our idea of purpose engineering, the paper then presented a system implementing the proposed purpose engineering semantics. Lastly, purpose and spatial purpose functions are presented that are used by our prototype.

4. REFERENCES

[1] Rindfleisch, T. (1997). Privacy, information technology, and health care. Communications of the ACM, 40(8), 93–100.

[2] Archives & Records Management Handbook. (2003). Retrieved January 2, 2008, from http://osulibrary.oregonstate.edu/archives/handbook/definitions/.

[3] Reid, J., Cheong, I., Henricksen, M. & Smith, J. (2003). A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems. Paper presented to Information Security and Privacy, 8th Australasian Conference, ACISP, Wollongong, Australia.

[4] Bacon, J., Lloyd, M. and Moody, K. (2001). Translating role-based access control policy within context. In Workshop on Policies for Distributed Systems and Networks, Springer-Verlag, 107–120.

[5] Patrick, C., Hung, K. and Zheng, Y. (2007). Privacy Access Control Model for Aggregated e-Health Services. Proceedings of the 2007 Eleventh International IEEE EDOC Conference Workshop, Maryland U.S.A, 12-19.

[6] Langheinrich, M. (2001). Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In "Ubicomp 2001". Retrieved January 22, 2008, from http://www.vs.inf.ethz.ch/publ/papers/privacy-principles.pdf.

[7] Jiang, X. and Landay, J. A. (2002). Modeling privacy control in context-aware systems. IEEE Pervasive Computing, 1(3), 59-63.

[8] Bohn, J., Gartner, F. and Vogt, H. (2004). Dependability Issues of Pervasive Computing in a Healthcare Environment. *Security in Pervasive Computing, First International Conference, Boppard, Germany*, 53-70.

[9] Beckwith, R. (2003). Designing for Ubiquity: The Perception of Privacy. IEEE Pervasive Computing, 2(2), 40–46.

[10] Beresford, R. and Stajano, F. (2004). Mix zones: User privacy in location-aware services. Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW04), Orlando, Florida, pp. 127.

[11] Definition of the purpose on the Web. Retrieved July 30, 2007, from: http://www.google.com/search?hl=en&rlz=1T4GFRC_en___MY202&defl=en&q=define:purpose&sa=X&oi=glossary_definition&ct=title.

[12] Byun, J. W., Bertino, E. and Li, N. (2004). Purpose Based Access Control for Privacy Protection in Relational Database Systems. Technical Report 2004-52, Purdue University, USA.

[13] World Wide Web Consortium (W3C). Platform for Privacy Preferences (P3P) Retrieved October 10, 2008, from http://www.w3.org/P3P.

[14] Joshi, J.B.D., Bertino, E. and Ghafoor, A. (2002). Temporal Hierarchies and Inheritance Semantics for GTRBAC. Proceedings of the seventh ACM symposium on Access control models and technologies, Monterey, California, USA, 74-83.

[15] Joshi, J. B. D., Bertino, E., Latif, U. and Ghafoor, A. (2005). A Generalized Temporal Role-Based Access Control Model. IEEE Transactions on Knowledge and Data Engineering, 17(1), 4–23.

[16] Tahir, M. N. (2008). Hierarchies in Contextual Role- Based Access Control Model (C-RBAC). International Journal of Computer Science and Security (IJCSS), 2(4), 28-42.

[17] Tahir, M. N. (2007). Location Modeling for C-RBAC: Contextual Role-Based Access Control Model. International Conference on Information Technology in Asia (CITA), 265-269.