Hierarchies in Contextual Role- Based Access Control Model (C-RBAC)

Muhammad Nabeel Tahir m_nabeeltahir@hotmail.com
Faculty of Information Science and Technology
Multimedia University, Melaka, Malaysia

Abstract

Hierarchical representation is a natural way of organizing roles in role-based access control systems. Besides its advantages of providing a way of establishing parent-child relationships among different roles, it also provides a facility to design and organize context dependant application roles that users may activate depending on their current context (spatial, temporal) conditions. In this paper, we show that if spatial roles are organized in hierarchical relationships, it can cause the problem of disambiguation in making access control decisions especially when the user moves from one location to another location frequently in a single transaction and a single session. We extend our work of Contextual Role-Based Access Control (C-RBAC) by introducing hierarchical relationship among subject, location and purpose roles and solve the disambiguation problem in hierarchy by considering user motion direction and his/her context roles (spatial and spatial purpose) in order to make more fine grained and better access control decisions.

Keywords: Access Control, RBAC, Purpose Role, Spatial Role, Location Modeling.

1. INTRODUCTION

Patients have important roles to play in addressing privacy and security concerns. The greatest concerns regarding the privacy of health information derive from widespread sharing of patient information throughout the health care industry and the inadequate federal and state regulatory framework for systematic protection of health information. At the level of individual organizations, electronic health information is vulnerable to both authorized users who misuse their privileges to perform unauthorized actions (such as browsing through patient records) and outsiders who are not authorized to use the information systems, but break in with the intent of malicious and damaging action. Adequate protection of health care information depends on both technology and organizational practices for privacy and security.

Health care organizations have to deal with a number of processes, procedures that are controlled through different applications. They also have to make sure that all the implemented applications must follow the rules and policies that have been addressed by Health Insurance Portability and Accountability Act (HIPAA) [1] to make sure the confidentiality, integrity and secrecy of patient record. Many privacy and authorization based access control models have been proposed in past to protect organizational resources. Examples are location-based [2], [3], [4], [5], time-based [6], [7], [8]. However they have limited flexibility as none of them consider the purpose for which access is given to the user to perform various activities. Also these models lacks in partitioning organization into a domain environment as these models rely on the spatial extent defined within the total responsibility space. Thus, making difficult for the security officer to manage the authorization permissions for the whole space defined within an organization. Few purpose-based access control model [9], [10], [11] have been proposed for various applications that relies on role-based access control (RBAC). But these models do not provide the proper semantics and constraints for purposes with spatial extents. These models address only spatial and temporal characteristics of roles and some others, only purpose characteristics.

In this paper, we extend our work of recently proposed C-RBAC model [12] that relies on spatial roles with the presence of spatial purposes and spatial domains. We provide few examples to show how our model incorporates location hierarchy schema and location hierarchy instance, user motion direction and spatial purposes in order to solve the hierarchical disambiguation.

The remainder of this paper is organized as follows. Next section briefly presents C-RBAC model and some relevant definitions. We then present hierarchies in C-RBAC and define location hierarchy (schema and instance level), spatial domain hierarchy, spatial purpose hierarchy. Lastly we conclude the paper along with future research direction.

2. PRELIMINARIES

In this section, we provide some definitions for location, spatial domain, spatial role and spatial purposes that are the building blocks of our model.

Definition 1 (Location): We define the location as a set of attributes that defines the scope of some area/region and give some name to it.

Location (loc) = {attr1, attr2, attr3…attrn }, where n > 0

Definition 2 (Physical Location): Physical location ploc is a set of points that represents a polygon, line or a single point.

ploc = {<pos1, pos2…posn >, <DVAL>, dunit }

where n > 0, DVAL is a set of directional distances {m1, m2, m3, m4} representing distances of east, west, north and south; and dunit represents distance measurement unit.

PLOC is set containing all physical locations identified by the system such that

PLOC = {ploc1, ploc2…plocn}
where n > 0

Definition 3 (Logical Location): Logical location lloc is an abstract meaning of a set of physical locations. A logical location can be characterized by many physical locations such that:

lloc = {ploc1, ploc2… plocn}, where n > 0

LLOC is a set containing all the logical locations identified by the system such that

LLOC = {lloc1, lloc2…llocn}
where n > 0

Definition 4 (Relative Location): Relative location rloc is a range/perimeter defined with respect to a physical or logical location such that:

rloc = <l, dunit, dir>, such that

where l $\in$ PLOC/LLOC, dunit is a distance measurement unit, dir is a geometric or logical direction value

RLOC is a set of all relative locations identified by the systems such that

RLOC = {rloc1, rloc2…rlocn}
where n > 0

We also define the functions occurrenceploc (rloc); occurrencelloc (rloc) that generates a set of physical or logical locations with respect to the relative location rloc given.

C-RBAC HIERARCHIES

The central components on which C-RBAC model relies are location, domain and purpose roles. Like subject roles in RBAC, hierarchical relationship exists among locations, domains and purposes roles. Sandhu et al. proposed [13] that hierarchical relationship can be defined by introducing the partial order $\preceq$ between roles such that ri $\preceq$ rj means that: (a) rj inherits all permissions assigned to ri; (b) users which have been assigned rj have also been assigned ri. We use this concept as a base of defining hierarchical relationship among different locations in C-RBAC model.

Location Hierarchies

In our model, the traditional hierarchical relationship is not sufficient to deal with the location in the presence of domains. Therefore, we extend the traditional hierarchical relationship by defining Location Hierarchy Schema (LHS) and Location Hierarchy Instances (LHI).

Location Hierarchy Schema (LHS)

LHS allows the security administrator to define a common name for a set of hierarchically organized logical locations within a spatial domain. Hierarchical relationship defined among logical locations within the schema represent the internal organization structure within a spatial domain. As logical locations are organized in a hierarchical manner, all the relationships defined in [14] exist among locations.

Definition 5 (Location Hierarchy Schema): A location hierarchy schema is a tuple <LHS, ls>, where LHS is the location hierarchy schema name and ls is logical locations set organized in a hierarchical relationship within the schema such that; ls → 2lloc.

Let lhsi be the location hierarchy schema name, ls is defined as, ls → occurencesls (lhsi) → 2lloc, where lloc ∈ LLOC. Because of hierarchical relationship among logical locations, relationships contains (lloc1, lloc2), disjoint (lloc1, lloc2) holds [14].

Consider a scenario of a hospital in which X-Ray, Laboratory are the departments and General Ward, Surgery and ICU are wards. We further assume that each department and ward has its own architecture, for example departments may have reception area, doctor offices and waiting room and wards may have patient rooms, doctor offices, nursing room, waiting hall and main general hall in which patients are admitted as shown in figure 1.

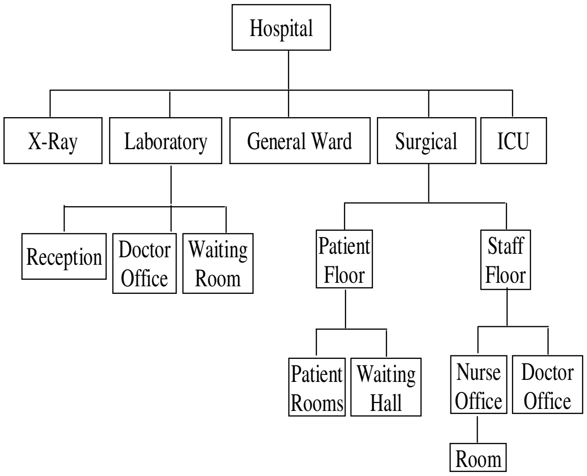

Figure 1: Hospital wards and departments.

Assume that:
- General Ward has patient and staff floor
- Patient floor has Patient Rooms, Waiting Hall
- Staff Floor has Nurse Office, Doctor Office room.

By using logical locations, we can define location hierarchy schema for a ward figure 2(a) and for a department figure (b).

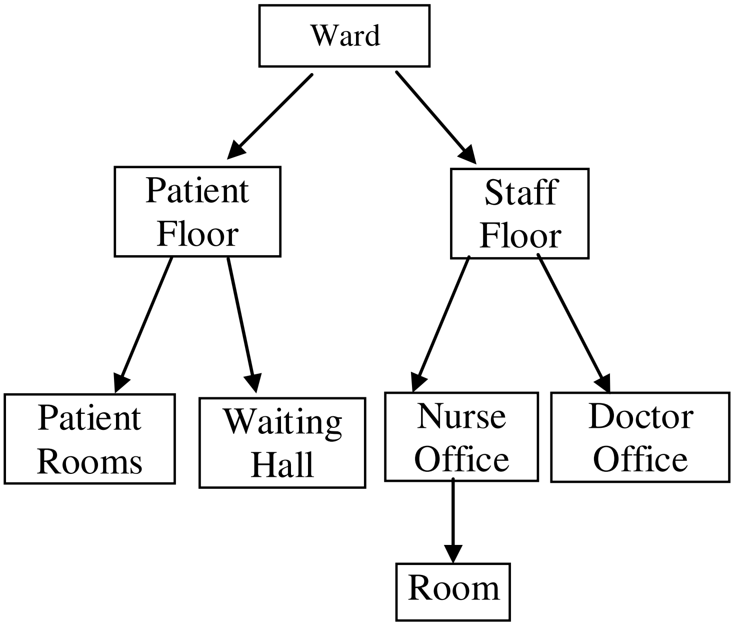

Figure 2(a): Location hierarchy schema for ward.

LHS <Ward, ls> and ls → occurencesls (Ward) → 2lloc, that is ls = {PatientFloor, StaffFloor, PatientRooms, WaitingHall, NurseOffice, DoctorOffice, Room}.

Similarly, LHS for department can be defines as LHS <Department, ls> and ls → occurencesls (Department) → 2lloc, that is ls = {Reception, DoctorOffices, WaitingRoom} as shown in figure 2(b).

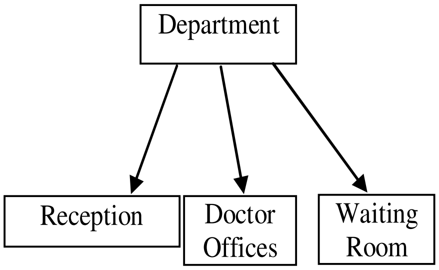

Figure 2(b): Location Hierarchy Schema for department.

Location Hierarchy Instance (LHI)

Location Hierarchy Instance is defined as an instance fulfilling the location relationship pattern defined within LHS.

Definition 6 (Location Hierarchy Instance): Given a location hierarchy schema lhs, lhi can be defined as <LHI, ps> where LHI is the location hierarchy instance name and ps is the physical locations set organized according to the hierarchical relationship among logical locations defined within the schema such that given lhi, ps → occurencesps (lhij) → 2ploc, where ploc ∈ PLOC.

By definition 2, each physical location defined in LHI is defined along with the directional distances to its east, west, north and south. For example <NurseOffice, {30, 10, 25, 46}, meter> and <DoctorOffice, {23, 30, 15, 75}, meter> shows that the distance between NurseOffice and DoctorOffice is 30 meters. By constant monitoring the current values of user position, user speed and motion direction can easily be obtained for access control decisions. We define the function DirectionalDistance (ploc, dir) that returns the distance between the physical location ploci to plocj defined in the direction dir.

Location hierarchy instance for the ward and department is shown in figure 4(a) and 4(b) respectively.

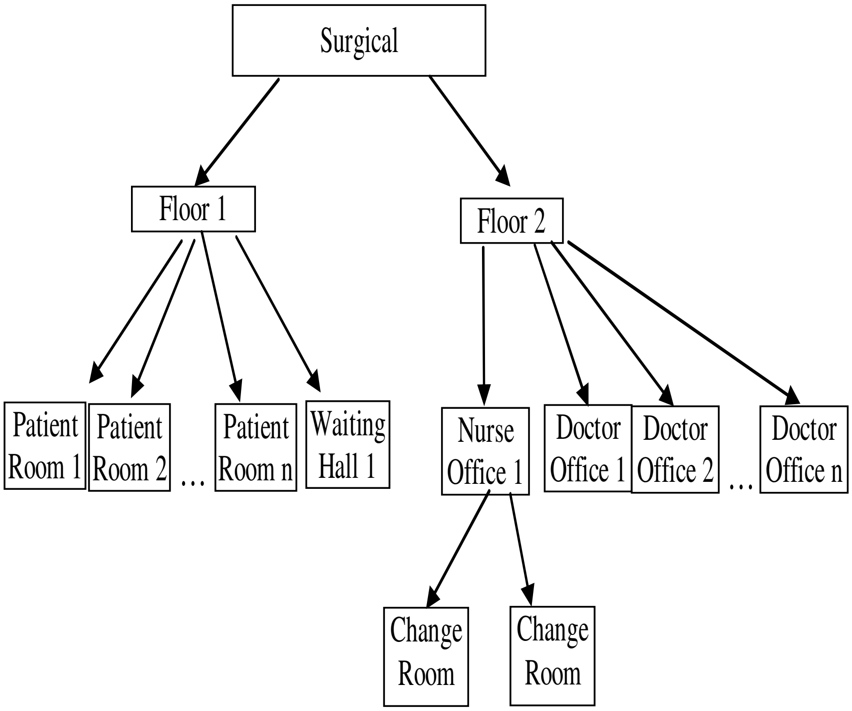

Figure 3(a): Location Hierarchy Instance for ward.

LHI <Surgical, ps> and ps → occurencesps (Surgical) → 2ploc, that is ps = { Floor1, Floor2, PatientRoom1,..PatientRoomn,WaitingHall1,NurseOffice1,ChangeRoom1,ChangeRoom2,Doctor Offices1,DoctorOffices2,DoctorOfficesn,}.

Similarly, for department as shown in figure 3(b), LHI can be defined as LHI <Laboratory, ps> and ps → occurencesps (Laboratory) → 2ploc, such that; ps = {Reception1, DoctorOffice1, DoctorOffices2,…DoctorOfficen,,WaitingHall1}.

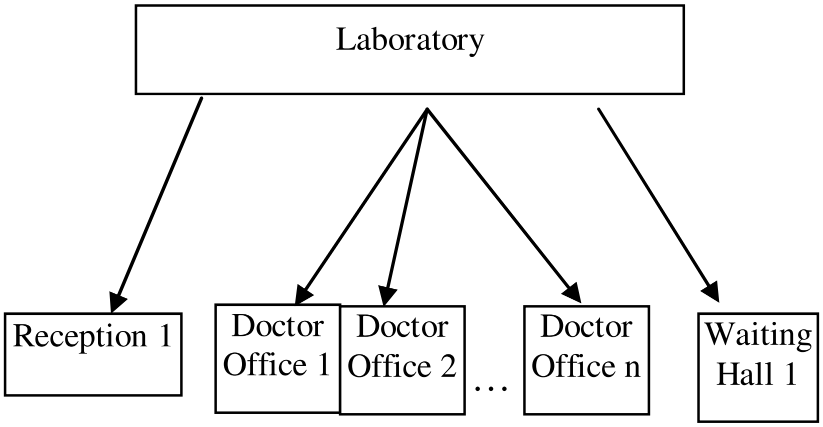

Figure 3(b): Location Hierarchy Instance for department.

Location Hierarchy Schema and Instance Functions

Let LHSS = {lhs1, lhs2,…, lhsn} be the set of location hierarchy schema and LHIS = {lhi1, lhi2 ,…, lhin} be the set location hierarchy instances. We define:
-SchemaOf (lhin) → lhsn, such that; occurencesls (lhsn) → 2lloc (definition 5.1)
-InstanceOf (lhsn) → 2lhi, such that occurencesps (lhin) → 2ploc (definition 5.2)

Location Hierarchy Schema and Instance Hierarchies (LHSH & LHIH)

Given two location hierarchy schemas, it may be possible that relationships like contains, disjoint and overlaps exist. Like location hierarchy schema, relationships also exists among physical locations e.g. contains (ploc1, ploc2), disjoint (ploc1, ploc2). We borrow the logical and physical location relationships from [14] and define the following relationships for LHS and LHI given in table 1.

Relations	***Semantics (physical locations)***	***Semantics (logical locations)***
	For all lhi, such that $lhi_n \rightarrow InstanceOf\ (lhs_n)$	
lhs_1 *contains* lhs_2	$contains(lhi_1\ ,\ lhi_2) \rightarrow (\forall ploc_2\ ,\ ploc_2 \in occurrence_{ps}\ (lhi_2) \rightarrow (\ \exists\ ploc_1,\ ploc_1 \in occurrence_{ps}\ (lhi_1)\ \Lambda\ contains\ (ploc_1, ploc_2)))$	$contains(lhs_1\ ,\ lhs_2) \rightarrow (\forall lloc_2\ ,\ lloc_2 \in occurrence_{ls}\ (lhs_2) \rightarrow (\exists lloc_1,\ lloc_1 \in occurrence_{ls}\ (lhs_1)\ \Lambda\ contains\ (lloc_1, lloc_2)))$
lhs_1 *disjoint* lhs_2	$disjoint\ (\ lhi_1\ ,\ lhi_2) \rightarrow (\forall ploc_1, ploc_1 \in occurrence_{ps}(lhi_1) \rightarrow (\exists\ ploc_2\ ,\ ploc_2 \in occurrence_{ps}\ (lhi_2)\ \Lambda\ disjoint\ (ploc_1, ploc_2)))$	$disjoint\ (lhs_1, lhs_2) \rightarrow (\forall lloc_1, lloc_1 \in occurrence_{ls}(lhs_1) \rightarrow (\exists lloc_2\ ,\ lloc_2 \in occurrence_{ls}\ (lhs_2)\ \Lambda\ disjoint(lloc_1, lloc_2)))$
lhs_1 *overlap* lhs_2	$overlap\ (\ lhi_1\ ,\ lhi_2) \rightarrow (\forall\ ploc_2\ ,\ ploc_2 \in occurrence_{ps}(lhi_2) \rightarrow (\ \exists ploc_1,\ ploc_2 \in occurrence_{ps}\ (lhi_1)\ \Lambda\ overlaps(ploc_1,\ ploc_2\ )))\ \Lambda\ (\forall\ ploc_1,\ ploc_1 \in occurrence_{ps}\ (lhi_1) \rightarrow (\exists\ ploc_2\ ,\ ploc_2 \in occurrence_{ps}\ (lhi_2)\ \Lambda\ overlaps(ploc_1,ploc_2)))$	$overlap\ (lhs_1, lhs_2) \rightarrow (\forall lloc_2\ ,\ lloc_2 \in occurrence_{ls}\ (lhs_2) \rightarrow (\exists lloc_1, lloc_2 \in occurrence_{ls}\ (lhs_1)\ \Lambda\ overlaps(lloc_1,\ lloc_2\ )))\ \Lambda\ (\forall lloc_1,\ lloc_1 \in occurrence_{ls}(lhs_1) \rightarrow (\exists\ lloc_2\ ,\ lloc_2 \in occurrence_{ls}\ (lhs_2)\ \Lambda\ overlaps(lloc_1,lloc_2)))$

Table1: Relationships among LHS and LHI

Domain Hierarchy

The main goal of a distributed system is to connect users and resources in a transparent, open, and scalable way. Besides its many advantages, distributed systems allow organizations to divide large problems into many small problems which are distributed to many computers. Later, the small results are reassembled into a larger solution. Similarly distributed processing require that a program be parallelized—divided into sections that can run simultaneously, distributed computing also requires that the division of the program take into account the different environments on which the different sections of the program will be running.

Because of its strewn nature, it may be possible that a single request may be divided into many small requests for parallel or distributed processing that may

require services of different resources from different locations. This result organizations not only to know the requestor identity and the spatial context of the user but also the purpose for which a request to access a resource has been made.

A lot of work have been done by many researchers on domains by answering different problems like how to define a domain [15], domain hierarchies, communication among multi-domain and multi-level domains [16], [17] and [18]. Hansen et al. proposed an extension of RBAC model that relies on the notion of spatial roles [2]. In their work, they proposed logical location domains that reflect organizational location infrastructure and security policy. However their work is very simple and does not address issues like how spatial roles can be organized within logical location domains. Furthermore their work assumes the fixed spatial granularity of the position; primary location cells; on which roles can be acquired by the user. A good effort has been made in defining spatial roles by Bertino et. al [3]. In their model, spatial feature of role relies on role extend and logical position. However, their work does not address the organization of spatial roles within the domain scope. Furthermore, their model is not compliant with privacy requirements defined by HIPAA in which user purposes/intentions also take part in access control decision process. Few other notable approaches are the work by Corradi et. al [4] and Fu et. al [5]. We extend our work of C-RBAC model [12] and show how spatial domain can make use of LHS and LHI to organize spatial roles along with spatial purposes within spatial domain boundary.

Definition 7 (Spatial Domain): Spatial domain is a logical boundary surrounding at least one or a list of object(s) that are (a) associated with the location and purpose context and (b) identifiable by the system. Spatial domains are defined through spatial domain expression such that;

Spatial Domain <SDOM, LHSS>

where, SDOM is spatial domain name and LHSS is location hierarchy schema set specifying locations covered by SDOM through LHS, such that; LHSS → SchemaDomain (SDOM) → 2lhs.

Spatial Domain <SDOM, LHIS>

where, SDOM is spatial domain name and LHIS is location hierarchy instance set specifying locations covered by SDOM at instance level, such that; LHIS → InstanceDomain (SDOM) → 2lhi. It must be noted that one LHS can be defined more than one time within the same spatial domain but LHI name must be unique within the same spatial domain. However multiple instances of same LHS can be defined in two different spatial domains.

Furthermore, we define the LHS and LHI mapping functions for spatial domains such that, SchemaDomain (SDOM) → 2lhs, and InstanceDomain (SDOM) → 2lhi. Given a spatial domain; these functions return LHS and its instances LHI used by SDOM. Once a list of LHS or LHI used by SDOM is computed, logical and physical locations used by LHS and LHI can be easily computed through occurencesLSDOM (SDOM): $\underset{x \in SchemaDomain(SDOM)}{U} occurences_{ls}(x)$

and $occurences_{LSDOM}(SDOM): \underset{x \in InstanceDomain(SDOM)}{U} occurences_{ps}(x)$

We notice that location hierarchy schema and the derived instances used by spatial domains leads us to define hierarchical relationships among spatial domains because of LHS and LHI hierarchical relationships through contains and overlaps. Similarly it may be possible that a physical location ploc defined in one schema used by SDOMi may also be defined in another schema of SDOMj. We address these issues by defining multi-level spatial domain relationships and multi-spatial domain relationships. By using relationships among LHS and LHI as defined in table 1, we define

Definition 8 (Multi-Level Spatial Domain Relationship): Without loosing generality in location relationships defined in [14], we say that two domain SDOMi and SDOMj may have a multi-level relationship such that:

$\text{multiLvlDom}(\text{SDOMi}, \text{SDOMj}) \rightarrow (\forall \text{lhsj}, \text{lhsj} \in \text{SchemaDomain}(\text{SDOMj}) \rightarrow (\exists\ \text{lhsi}, \text{lhsi} \in \text{SchemaDomain}(\text{SDOMi}) \wedge \text{contains}(\text{lhsi}, \text{lhsj})))$.

Definition 9 (Multi-Spatial Domain Relationship): Let lhsi and lhsj be the LHS such that lhsi $\in$ SDOMi and lhsj $\in$ SDOMj. We define:

(i) $\text{multiDomovrlp}(\text{SDOMi},\text{SDOMj}) \rightarrow (\forall \text{lhsj}, \text{lhsj} \in \text{SchemaDomain}(\text{SDOMj}) \rightarrow (\exists \text{lhsi}, \text{lhsi} \in \text{SchemaDomain}(\text{SDOMi}) \wedge \text{overlaps}(\text{lhsi}, \text{lhsj}))) \wedge (\forall \text{lhsi}, \text{lhsi} \in \text{SchemaDomain}(\text{SDOMi}) \rightarrow (\exists\ \text{lhsj}, \text{lhsj} \in \text{SchemaDomain}(\text{SDOMj}) \wedge \text{overlaps}(\text{lhsi}, \text{lhsj})))$

(ii) $\text{multiDomdisj}(\text{SDOMi}, \text{SDOMj}) \rightarrow (\forall \text{lhsi}, \text{lhsi} \in \text{SchemaDomain}(\text{SDOMi}) \rightarrow (\exists \text{lhsj}, \text{lhsj} \in \text{SchemaDomain}(\text{SDOMj}) \wedge \text{disjoint}(\text{lhsi}, \text{lhsj})))$

Purpose Hierarchy

Purpose; in many literatures is defined as “an anticipated outcome that is intended or that guides your planned actions” [22]. Many countries have ratified legislation to protect privacy for individuals [12]. For example, Gramm-Leach-Bliley Act (GLB Act) [19] for financial sector, Health Insurance Portability and Accountability Act (HIPAA) [1] for medical sector in United States, Personal Information Protection and Electronic Documents Act (PIPEDA) [20] in Canada have made organizations keen in knowing the user intentions in order to grant permissions. These legislations protect and enhance the rights of consumer, clients and patients etc. while restricting access usage of the information based on the user’s intentions [21].

Purpose-oriented model that control the illegal flow of information between objects in object-based systems is presented by [9]. They have discussed how to validate the purpose-oriented access rules through invocation graph and flow graphs that show the information flow relation among operations and objects. Covington et al. proposed the notion of environmental roles to capture environmental contexts to secure context-aware applications [10]. They also presented a security architecture that made use of environment roles through security policies to allow access to resources especially in home environments. However, no semantics have been given to show how environmental contexts can be attached with the roles. Furthermore, their work lacks in explaining how their proposed architecture restricts a user from acquiring two conflicting roles at a same time and how a relationship can be established between environmental roles. Their work also does not explain the explicit prohibition of environment roles and context aware security policies.

Ji Won et. al proposed purpose based access control for privacy protection in relational database systems in which multiple purposes can be associated with the data element at different granularity (attribute, column, tuple and entire table level) [11]. They also proposed the notion of intended purposes (that specify the intended usage of the data) and access purposes (that

specifies the purposes for which access can be given to use data element). Their purposed model relies on conditional roles that are based on role attributes and system attributes that can hold purpose values and context values of the role respectively. This means that every time when security administrator adds a new purpose in the purpose tree, he/she needs to define a new role attributes for each of the subject roles that can use it as an access purpose to access the data objects. However in our model we define purpose roles with respect to location called spatial purpose (SP) that can be attached with the subject roles. Similarly purpose roles can also be defined for spatial domains that reflect the reasons of communication between two domains. For example spatial purpose can be attached between a hospital and a research center with the purpose of research. By adopting this approach, we can also define constraints and obligation policies for domain based on its spatial nature that can be enforced at the time of making access control decisions about resource sharing. For example, we can define constraints on domain level that no user from research domain is allowed to access HIV results from laboratory domain for the purpose of research.
Furthermore in their work, users have to state their purposes when they try to access resources. Although this approach is quite simple and easy to implement, however the main drawback is that; the overall privacy that the system provides mainly relies on the user's trustworthiness.

In our approach we infer the access purpose runtime based on the current context of the user such that;

$$\text{Purpose } P \rightarrow U \text{ x } R \text{ x } T \text{ x } LoC\_AtR$$

where U ∈ Users, R ∈ Roles, T is time interval and Loc_AtR is a set of attributes e.g. user motion direction, motion speed, such that;

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

Given the user session s, SLOC_ATR (s:sessIon) represents the current values of motion speed and motion direction of the session s activated by the user u with respect to its spatial context such that DirectionalDistance (ploc, dir) that returns the distance between the physical location ploci to plocj defined in the direction dir.

Definition 10 (Spatial Purpose): Spatial purpose is a purpose defined over some location context with respect to LHS such that;

Spatial Purpose SP <sp, lhs, spl>

where sp is spatial purpose name, lhs is location hierarchy schema and spl is spatial purpose location, a set of logical locations defining the boundaries for sp with respect to lhs such that; spl = {lloc1, lloc2…llocn}, where llocn ∈ occurencesls (lhsn).

Similarly, for LHI level, spatial purpose is defined as;

Spatial Purpose SP <sp, lhi, spl>

where sp is spatial purpose name, lhi is location hierarchy instance and spl is spatial purpose location, a set of physical locations defining the boundaries for sp with respect to lhi such that;

spl = {ploc1, ploc2…plocn}, where plocn ∈ occurencesps (lhin).

Like subject roles, spatial purposes also have a hierarchical relationship among them i.e. parent/child relationships. For instance, the purposes minor operations and major operations can be grouped together by a more general purpose, operation. The hierarchical relationship among different purposes is shown in figure 4 where each node represents the purpose and each edge represents the parent/child relationship.

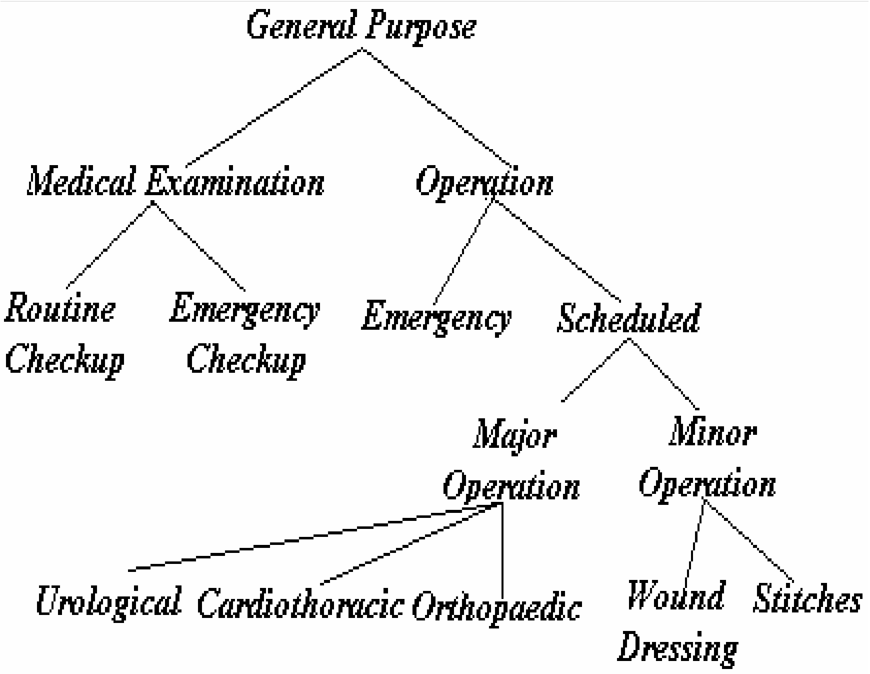

Figure 4: Purpose hierarchy

We define some functions for SP such that;

ParentPurposes (SP) → 2SP

ChildPurposes (SP) → 2SP

GetPurposeslloc (lloc) → 2SP; the function returns a set of spatial purposes defined with respect to logical location.

GetPurposesploc (ploc) → 2SP; the function returns a set of spatial purposes defined with respect to physical location.

GetPurposeslhs (lhs) → 2SP; the function returns a set of spatial purposes defined at location hierarchy schema level.

GetPurposeslhi (lhi) → 2SP; the function returns a set of spatial purposes defined at location hierarchy instance level.

IsParentPurposes (SP) → boolean, and
IsChild (SP) → boolean.

3. CONCLUSION AND FUTURE WORK

In this paper, we have extended our previous work on contextual role-based access control by introducing hierarchical relationships between locations, domains and purposes. We also introduce the notion of location hierarchy schema and location hierarchy instances. We emphasize that access control models cannot comply with HIPAA regulations without considering purposes/intentions of the users. We introduced the notion of spatial purposes that can be used by access control system to grant/deny permissions to the users depending on their current context values like time and location. However, separation of duty and conflicts may arise because of hierarchical relationship introduced between location schemas and instances with respect to purposes. We leave these issues for our future work.

4. REFERENCES

[1] . Health Insurance Portability & Accountability Act http://www.hipaa.org

[2] . Hansen F, Oleshchuk V. Spatial role-based access control model for wireless networks. In Proceedings of 58th IEEE Vehicular Technology Conference (VTC'03), 2093-2097, Orlando, Florida, 2003.

[3] . Bertino E, Catania B, Damiani ML, Persasca P. GEO-RBAC: A Spatially Aware RBAC. In Proceedings of 10th Symposium on Access Control Models and Technologies (SACMAT'05), 29-37, 2005

[4] . Corradi A, Montanari R, Tibaldi D. Context-based Access Control in Ubiquitous Environments. In Proceedings of 3rd IEEE International Symposium on Network Computing and Applications (NCA 2004), 253-260, 2004

[5] . Fu S, Xu C. A Coordinated Spatio-Temporal Access Control Model for Mobile Computing in Coalition Environments. In Proceedings of 19th IEEE International Conference on Parallel and Distributed Processing, 289b-289b, Denver, CA, USA, 2005.

[6] . Joshi JBD, Bertino E, Shafiq B, Ghafoor A. Dependencies and Separation of Duty Constraints in GTRBAC. In Proceedings of 8th ACM Symposium on Access Control Models and Technologies, 51-64, Como, Italy, 2003.

[7] . Joshi JBD, Bertino E, Latif U, Ghafoor A. A generalized temporal role-based access control model. IEEE Transactions on Knowledge and Data Engineering, 17(1): 4-23, 2005.

[8] . Joshi JBD, Bertino E, Ghafoor A. Analysis of Expressiveness and Design Issues for a Generalized Temporal Role Based Access Control Model. IEEE Transactions on Dependable and Secure Computing, 2(2):157-175, 2005

[9] . Yasuda M, Tachikawa T, Takizawa M. A purpose-oriented access control model. In Proceedings of 13th International Conference on Information Networking, 168-173, Cheju, Korea, 1998.

[10] . Covington MJ, Moyer MJ, Ahmad M. Generalized role-based access control for securing future applications. In Proceedings of the 23rd National Information Systems Security Conference. Baltimore, MD, USA, 2000.

[11] . Byun J, Bertino E, Ninghui L. Purpose Based Access Control for Privacy Protection in Relational Database Systems. Technical Report 2004-52, Purdue University, USA, 2004.

[12] . Tahir N. Contextual Role-Based Access Control, Ubiquitous Computing and Communication Journal, 2(3), 2007

[13] . Sandhu R, Ferraiolo D, Kuhn R. The NIST Model for Role-Based Access Control: Towards A Unified Standard. In Proceedings of 5th ACM Workshop on Role-Based Access Control, 47-63, Berlin, Germany, 2000

[14] . S. Chandaran and J. Joshi. LoT-RBAC: A location and time-based RBAC model. In Proceedings of the 6th International Conference on Web Information Systems Engineering (WISE'05). Page(s): 361-375, NewYork, USA, 2005.

[15] . Yialelis N, Sloman M. A Security Framework Supporting Domain-Based Access Control in Distributed Systems. In Proceedings of IEEE ISOC Symposium on Network and Distributed Systems Security'96 1996; 26-34, San Diego.

[16] . Lee KH. A Distributed Network Management System with Multi-level Domain Approach. In Proceedings of International Conference on Communication Systems ICCS 1994; 789-793, Singapore.

[17] . Sloman M. Policy Driven Management for Distributed Systems. Journal of Network and Systems Management; 2(4): 333-361, 1994.

[18] . Constantine E. A role-based framework for distributed systems management. PhD Thesis, University of London, July 1998.

[19] . Gramm-Leach-Bliley Act (GLB Act): U.S. Senate Committee on Banking, Housing, and Urban Affairs http://banking.senate.gov/conf

[20] . Personal Information Protection and Electronic Documents Act http://www.nymity.com/pipeda/

[21] . A. Hameed, M. N. Tahir, S. Rehman. Impact of Role-Based Access Control in e-Governance. In Proceedings of 3rd International Conference on E-Governance, Lahore, Pakistan, 2005.

[22] . http://www.google.com/search?hl=en&rlz=1T4GFRC_en___MY202&defl=en&q=define: purpose&sa=X&oi= glossary_definition&ct=title