

C-RBAC: CONTEXTUAL ROLE-BASED ACCESS CONTROL MODEL

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

ABSTRACT Widely strewn resources have made organizations engrossed to know not only who, when and from where but also for what purpose an access request has been made to use the organization resources. So a flexible model for role-based access control that support the enforcement and revocation of context aware policies is needed; that not only consider temporal and location but also purposes in order to make access control decisions. In this article, we have presented contextual model that mainly rely on the role-based access control models by keeping in mind the notion of purpose. We introduce spatial purpose roles and spatial purposes, their semantics and provide core model of proposed Contextual Role-Based Access Control Model (C-RBAC) for access control. We emphasize that the privacy protection cannot be easily achieved by traditional access control models because it focuses only on which user is performing what operation on what object. By introducing our model, we show how C-RBAC can make use of purpose oriented roles to make access control decisions which is based on which user can perform what operation on which object with what purpose.

Keywords: role-based access control, purpose, context-aware computing.

1 INTRODUCTION

With the vast usage of web based applications, whole world has become a global village. Today in almost every field, Internet is being regarded as an extension of organizations and a primary medium for disseminating information all over the world. In the last few decades, organizations have implemented information systems, intelligent planning systems, decision support systems [1] and distributed systems because of which the demand of security infrastructure that maintains confidentiality, authenticity, integrity and auditing has become tremendously increased [2]. This necessity is caused by the vast range of processes and procedures used by applications within the organizations.

For IT professionals, first real issue regarding integrity and security of electronic information came when the shift from mainframe to the client-server computing took place. In the mainframe model, no information was "leaking" to the outside world, the systems were single closed systems and only authorized persons were allowed to use the systems within the organization premises [3]. With the rise of the client-server architectures, heterogeneous computing environment and specially with that of distributed computing; information security and privacy concerns have become serious concern as usage of organizational resources is not limited to desktop PCs but also to distributed computing and

wireless technologies like mobiles, PDAs, laptops etc.

Distributed systems are characterized by many aspects, one of which is their potential size. In distributed computing systems (e.g. client-server systems or today's rising multi-tier systems) data stored, processed or accessed by many other computers across an enterprise and even outside of the enterprise. The results of data being stored in numerous places and transmitted here and there (e.g. laptop, PDA, mobile etc.) are massive and security officers recognized that data security would be an issue that had to be addressed with new solutions and new technologies [4].

In distributed systems, sharing and securing the communication and resources from users is necessary to prevent an unauthorized access. For example, an insurance company may be interested to get patient medical information for insurance purpose. Management of such large scale distributed systems is concerned with not only ensuring the availability but also tuning the services in order to achieve organizational goals. Moreover, an authorization request to use the resources and to utilize services can be made from any location, any time; but the need to know the purpose for which access request has been made is necessary in order to grant permissions.

Moreover, because of the distributed nature and wide spread of organizational structure, situations

exists in organizations in which it is normal to access different resources and services from different locations to complete a single task. Problem may arise when user A from domain X tries to access some resources that belong to domain Y . This problem has been addressed by current access control models, that is; *which* user can perform *what* operations on *which* object. We argue that *purpose* should be identified in order to grant user to access resources and services in multi-domain and multi-level domain environment.

In this paper, we present C-RBAC model that supports the enforcement of context oriented policies in distributed environment. Our work is an extension to C-RBAC architecture [5]. RBAC is used as a foundation to our architecture. Our model builds upon prior work on RBAC models, extending them to incorporate the spatial purpose and spatial domain roles. We choose modular representation of our approach that allows our model to incorporate current and future access control requirements. The modularity permits the future enhancements of our approach.

We provide our understanding of domain and introduced spatial domain roles. We emphasize that purpose should be attached to spatial roles that should be represented within organizational domains that may have multi-level and multi-domain relationships. We also show how our extended RBAC model can make use of the notion of spatial domain to allow administrator to flexibly partition the objects according to geographical boundaries.

Another contribution to this paper is the specification of access control policies that make use of the notion of spatial purpose roles to make access control decisions. We provide the definition of the purpose and the notion on which spatial purpose roles and spatial purposes can be created. By using a uniform notion of role to capture the purposes, we also give an idea that how spatial purpose role activation/deactivation and cardinality can also be defined through constraints.

A unique distinction we made in this paper is that, while some context like time and location may be the same for all users, the notion of purpose for which access request has been made to access an object may be different. For example, it may be possible that two users with same role, location and time context sends their request to access the resource/service, but because of the differences of their purposes, the access control service grants only one user to access resource/service. By using spatial domain, spatial purpose and spatial-purpose roles, our proposed model can easily tackle these types of scenarios.

The remainder of this paper is organized as follows: in section 2, we briefly discuss the related work. Section 3 reviews the traditional RBAC model. Our semantics of spatial domain, spatial purpose and

spatial-purpose-role concepts are briefly discussed in section 4 whereas extended C-RBAC model definition and function are given in section 5. Section 6 concludes the paper and future work.

2 RELATED WORK

In this section, we briefly highlight several existing access control architectures and models and compare them with our proposed model. We discuss traditional RBAC, time-based, load-based, content-based and purpose-based authorization models. Our proposed model allows the specification of policies that are supported by these models and also purpose specification.

Several RBAC based models and architectures [6], [7], [8] have been proposed that attempt to capture the location based and/or time-based access control requirements in various applications for different sectors. However they have limited flexibility and granularity. Our contribution to this paper extends the traditional RBAC model in a way that traditional RBAC model can easily differentiate between users based on their various properties but it doesn't provide any support of the notion of purpose for which object properties can be used. Traditional RBAC does not provide timely and location-based access control, for example subject s can access object o from location l between 8:00 a.m and 5:00 p.m. Bertino et al. [9] have proposed time-based authorization model which was later generalized and extended to role hierarchies, separation of duty and cardinality constraints; GTRBAC [10], in which the notion of time has been considered only. Their access control model is discretionary whereas our model is mandatory. But in principle, their notion of temporal access control decisions is similar to time-purpose based access control decisions.

Woo and Lam [11] presented (GACL) Generalized Access Control Language in which the notion of system load has been considered. For example certain programs can only be executed or made available to users if there is enough capacity of the system to handle it. Our proposed model is also capable to capture state based authorization factors by using purpose roles that is based on the rationalization i.e. "why needed". Gopal and Manber [12] presented integration of content-based access mechanism with hierarchical files system. In their work, they have contributed towards the identification of issues evolved during efficiently integrating the hierarchical file systems with database and provide the solution to the identified problems.

In LOT-RBAC, Suroop et al. [13] have presented RBAC model by extending the traditional RBAC to the temporal and location constraints. GEO-RBAC Maria et al. [14] have presented a spatially aware RBAC which is probably the most

expressive location-role-based access control model in which users can use a role only when they are in the role-location context. But no architectural representation of the proposed extended model has been given. The model also lacks in addressing the access log constraints, log hierarchy mechanisms. The spatial RBAC model [15] allows the specification of Separation of Duty (SoD) but does not address the idea of location constraints that are not SoD.

In RB-GACA [16, 17], an architecture implementation based on RBAC has been given for multi-domain enterprises. Also the basic model definitions and administrative functions have been given, such as *AddUser*, *DeleteUser* etc.; but no policy syntax is provided with respect to the proposed architecture. Also the architecture does not address the issue that how obligations, duties and purpose oriented policies can be implemented and enforced within a single domain or in a multi-domain environment.

Micheal et al. [18] have presented Generalized RBAC in which the notion of object roles and environmental roles has been introduced for securing applications in the highly connected homes. In GRBAC the basic concept of object and environmental roles has been given but their semantics are missing. Authors haven't discussed how the proposed model can be modulated into an architectural representation. Also the notion of purpose roles which gives the justification of access control decision is not discussed. Ji-Won et al. [19] has proposed purpose oriented access control for privacy protection. Their model is based on the notion of purpose roles through which they proposed Intended purposes and Access purposes. Also a purposes hierarchy has been given along with the idea of role attributes and system attributes. However the access control model does not deal with other elements such as obligations and complex conditions which are essential part of privacy protection.

Our proposed model is capable to address all these issues and extend the traditional, location-based and temporal-based access control model with the notion of purpose roles. Another contribution that we have made is; we have provided the policy syntax on the basis of which purpose-oriented access control policies can be generated that will be used by the access control service of our architecture [5]. Besides normal access control policies, our architecture is capable to allow the security officer to specify obligation policies which are enforced by obligation enforcement service to deal with complex conditions.

3 TRADITIONAL RBAC

The request to access the object to perform some operations can be generated from anywhere and anytime by the users and applications. In majority of

cases, multiple objects within a single domain or from multiple domains communicate among each other to achieve some objectives. Sometimes it may happen that services may be requested by the applications or agents from different domains for different purposes. In such cases, the access control systems need to consider context information to enforce the normal access control policies as well as obligation policies that include for example time, location, load of the system, purpose etc. Therefore access control architectures should provide a support to enforce context oriented (location, time, purpose etc.) policies.

In RBAC, the user-role relationship is more dynamic than the role-permission relationship. As a result, context can be categorized into static constraints for e.g. user nationality, salary etc and dynamic constraints for e.g. time, location and purpose of the user for which access request has been made. One approach to enforce the dynamic context oriented policies is to rapidly change the permission assignment relations that depend on the dynamic contexts. Another approach is to define permissions that should consider the static and dynamic behavior of context constraints. Based on this, the adoption of existing well-known access control models and technologies is sensible as it provides a means to extend from traditional to context-dependant access control policies and facilitates obligation policies enforcement.

Therefore, we have selected Role-Based Access Control model [20]. Throughout the design of the model, RBAC is used as a foundation. In this section, we define the traditional RBAC and highlight its potential benefits.

3.1 Basic RBAC Definitions

RBAC uses the notion of role that categorizes the subjects based on various properties. Individual users are called subjects which are associated with one or more roles. Another important concept in RBAC is object which is defined as resource of the system that is manipulated only through operations supported by that object. In order to perform some operation on an object, subject must possess a role that must be associated with the respective operation. Fig. 1 shows the core model of RBAC.

3.2 Role Hierarchy

Role hierarchy is the structural representation of roles that reflects the organizational work break down structure. Role hierarchy also classifies some roles as super role and sub role. Super role represents the hierarchical relation among sub roles. In other words, super role is a specialization of generalization of sub roles. For example cardiologists, neurologists, medical specialist, all of them are sub roles of the **doctor** role. The benefit of role hierarchy is to allow administrator to define

general purpose access control policies and to assign them to the super roles. The hierarchical relationship between roles allows the policy to be inherited by sub roles. This approach eases the policy management and allows the administrator to define a single policy for once and assign it to the super role which then can be accessed by sub roles through role inheritance.

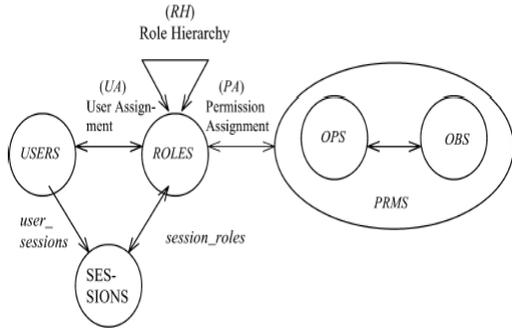


Figure 1: Core role-based access control model

3.3 Separation of Duty (SoD)

Separation of duty, SoD plays an important role in an access control policy specification. Role hierarchy allows permission inheritance that sometimes allows subjects to acquire conflicting permissions at a same time. SoD is a way to resolve these conflicting issues so that a subject s should not acquire conflicting permissions p because of role hierarchy. For example, a doctor cannot be his own patient.

3.4 Benefits of RBAC

Use of RBAC provides many advantages to the organizations. Hierarchical support among roles easily reflects the organization structure. RBAC supports the access permission delegation through roles. Separation of duty avoids role conflict among subjects and restricts the subjects in acquiring conflicting roles at the same time. For example a teacher assistant cannot acquire the permission to mark his/her own paper. Another example could be, a doctor can either acquire *daydoctor* or *nightdoctor* role but not both at a same time.

4. DOMAIN AND PURPOSE

4.1 Domain

Distributed systems are characterized by many aspects, one of which is their potential size. Due to the strewn nature, these systems contain unlimited number of geographically dispersed objects within multiple hosts, sites or even countries. Several definitions of the concept domain have been given in literature. Twidle et al. [21] proposed that domains are flexible means of partitioning objects based on geographical boundaries, object type, management

functionality, responsibility and authority or for the convenience of human managers. Like directories in a file system, domain holds local names of objects that are its members. In [22], Emil proposed that domain is an object that maintains a list of references to objects that have been grouped together for the purpose of management. Through object list, domains differentiate the direct or indirect objects (members of domain).

Definition 1 (Domain): *domain is a logical bound defined over some space that contains at least one object whereas space and object are identifiable by the system.*

Object can be applications or even another fully or partially ordered domain. We argue that spatial roles should be organized within the domain for several reasons. Firstly, role is a grouping mechanism that is used to categorize subjects based on job title, user functions or responsibilities. Secondly, roles are defined based on the job functions performed by the organization’s employees. However, a domain is a flexible means of partitioning objects based on geographical boundaries, object type, management functionality, responsibility and authority or for the convenience of human managers [21]. Furthermore, role represents organizational structure and can be designed based on different types of structures e.g. flat, traditional and project organizational structures. Domain represents departmental structure of an organization along with multi-level and multi-domains relationships whereas role represents the participants in domains. Moreover, purposes can be attached with domains in order to establish relationships among/between domains.

Definition 2 (Spatial Domain): *Spatial domain describes a logical bound that surrounds at least one or a list of object(s) and contains spatial purpose roles identified by the system.*

$$\text{Spatial domain } SDOM \langle SDOM, SD_BOUND \rangle$$

where $SDOM$ is spatial domain name and SD_BOUND is a set of logical locations specifying area covered by $SDOM$ such that;

$$SD_BOUND: occurrences_{LSDOM}(SDOM) \rightarrow lloc \in LLOC$$

Given a spatial domain, we call *domain-location mapping function* for $SDOM$ defined as $occurrences_{LSDOM}(SDOM)$ and $occurrences_{PSDOM}(SDOM)$ that generates a set of logical and physical locations respectively covered within the given domain such that $occurrences_{LSDOM}(SDOM) \rightarrow lloc \in LLOC$ and $occurrences_{PSDOM}(SDOM) \rightarrow ploc \in PLOC$

PLOC.

Definition 3 (Multi-Level Domain Relationship): Without losing generality we say that two domains $SDOM_1$ and $SDOM_2$ may have a multi-level relationship such that;

$$multiLvlDom(SDOM_1, SDOM_2) \text{Æ} (\forall lloc_2, lloc_2 \in occurrence(SDOM_2) \text{Æ} (\exists lloc_1, lloc_1 \in occurrence(SDOM_1) \wedge contains(lloc_1, lloc_2)))$$

$\implies contains(lloc_1, lloc_2) \text{Æ}$ Logical semantics of the relationship “contains” [5].

Definition 4 (Multi-Domain Relationship): Let $lloc_1$ and $lloc_2$ be the locations such that $lloc_1 \in SDOM_1$ and $lloc_2 \in SDOM_2$.

We define multi-domain relationship as;

(4.1)

$$multiDom_{ovrlp}(SDOM_1, SDOM_2, sps) \text{Æ} (\forall lloc_2, lloc_2 \in occurrence(SDOM_2) \text{Æ} (\exists lloc_1, lloc_1 \in occurrence(SDOM_1) \wedge overlaps(lloc_1, lloc_2))) \wedge (\forall lloc_1, lloc_1 \in occurrence(SDOM_1) \text{Æ} (\exists lloc_2, lloc_2 \in occurrence(SDOM_2) \wedge overlaps(lloc_1, lloc_2)))$$

$\implies overlaps(lloc_1, lloc_2) \text{Æ}$ Logical semantics of the relationship “overlaps” [5].

(4.2)

$$multiDom_{disj}(SDOM_1, SDOM_2, sps) \text{Æ} (\forall lloc_1, lloc_2 \in occurrence(SDOM_1) \text{Æ} (\exists lloc_2, lloc_2 \in occurrence(SDOM_2) \wedge disjoint(lloc_1, lloc_2)))$$

$\implies disjoint(lloc_1, lloc_2) \text{Æ}$ Logical semantics of the relationship “disjoint” [5].

where sps is spatial purpose set defining the spatial purposes for which $SDOM_1$ access resources for $SDOM_2$ and vice versa (definition 6).

As shows in Fig. 2, fully or partially ordered overlap allows us to establish inheritance relationship between domains so that users of one domain can access resources of another domain. For example, domain “Surgical Ward” is partially included in the domain “emergency Ward”. Domain “Minor OPT” is fully included in two domains i.e. “Emergency Ward” and “Surgical Ward”.

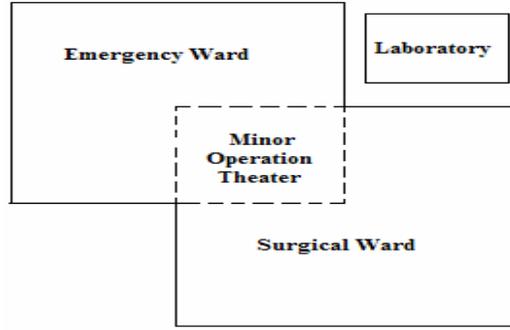


Figure 2: Graphical representation of domain

4.2 Purpose

Purpose describes the reason for which organizational resources are used [19]. In [23] P3P defines the purpose as “the reason(s) for data collection and use” and specifies a set of purposes, including current, admin, develop, contact and telemarketing [23]. A security privacy policy normally states that the particular resource can be accessed only for the specific purpose(s) under specific condition. For this purpose, Intended purpose and Access purpose have been proposed by Ji-Won et al. [19] whereas intended purposes regulate the usage of data/resource and access purposes are the purposes for accessing a particular data/resource. Intended purposes are further extended to Allows Intended Purposes (AIP) and Prohibited Intended Purposes (PIP). They have shown diagrammatical representation of purpose by introducing purpose tree in which purposes are organized in a hierarchical way to establish relationship between them for management simplicity.

Definition 5 (Purpose): Purpose is the intention of the user that is computed based on the contextual values that are assigned to the environment in which the user is requesting access to use resources. Such that;

$$Purpose P \text{Æ} U \times R \times T \times LOC_ATR$$

where $U \in Users$, $R \in Roles$, T is time interval and $LOCATION_ATTRIBUTES$ 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 .

Definition 6 (Spatial Purpose): spatial purpose is defined as the set of purposes for which one domain

interacts with another domain such that;

Spatial Purpose $SP \langle spr, spl \rangle$

where sp is spatial purpose name and spl is spatial purpose location, a set of logical locations defining the boundaries for spr such that;

$SPL = \{lloc_1, lloc_2, \dots, lloc_n\}$, where $lloc \in LLOC$

By providing our understanding of purpose, domain and introducing spatial purposes, a domain can also establish a relationship between other domains by using purpose concept as show in Fig. 3.

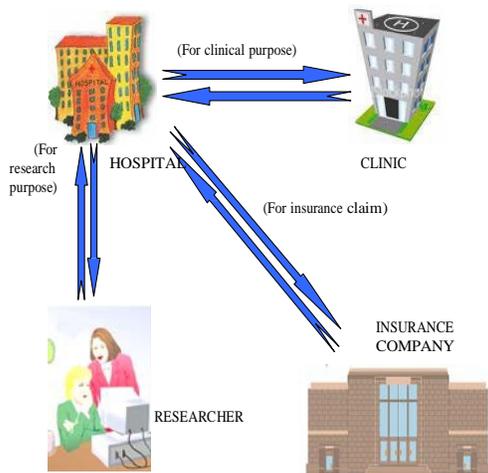


Figure 3: Domain registration through multi-domain relationship and spatial purpose

By definition 4.1, 4.2 and 6, we can define spatial purpose between hospital and insurance company as $\langle Insurance, Hospital, Insurance Company, \{Insurance Claim, Insurance Marketing\} \rangle$, between hospital and research department of any university as $\langle Research, Hospital, University, \{Laboratory Data Analysis\} \rangle$.

5. CONTEXTUAL ROLE-BASED ACCESS CONTROL MODEL

5.1 Core C-RBAC

RBAC is a very useful access control model but due to the distributed and heterogeneous nature of organizations, subject centric (traditional RBAC) is not sufficient. With the rapid advancement in technologies today, organizational resources are widely distributed. Also users can send request to access the resources at any time from any location. Under these circumstances, an extension of RBAC model is necessary in order to properly manage the

organizational resources in multi domain environment keeping in mind the confidentiality, integrity and availability.

We proposed this as C-RBAC, an extension of traditional role-based access control model that allows security administrators to define context oriented access control policies enriched with the notion of purposes. By adding purpose roles, we extend traditional access control model that helps organizations to know *which* user can perform *what* operation on *which* object with *what* purpose. We have provided the basics of our model. The extended C-RBAC model is shown in Fig. 4.

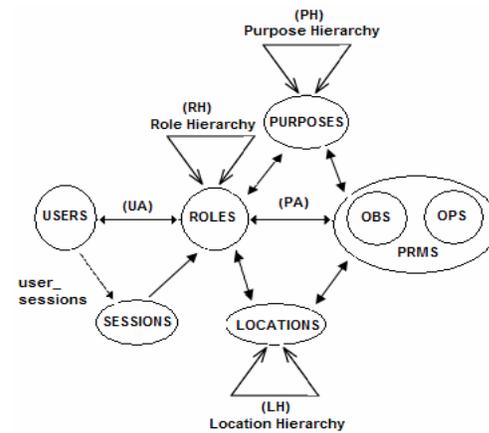


Figure 4: Contextual Role-Based Access Control Model (C-RBAC)

Definition 7 (Spatial Purpose Role): spatial purpose role defined as $\langle spr, spl_ext, sps \rangle$, where spr is the role name, spl is spatial purpose location, a set of logical locations defines the boundaries of the space and sps is a spatial purpose set of purposes by which role can be assumed by the user.

Spatial Purpose Role $SPR \langle spr, spl_ext, sps \rangle$

where spr is the spatial purpose role name, l_ext is set a set of logical location such that $spl_ext = \{lloc_1, lloc_2, \dots, lloc_n\}$, where $lloc \in LLOC$ and $sps = \{sp_1, sp_2, \dots, sp_n\}$, such that $sp \in SP$.

Furthermore, the function $Occurrence_{lloc}$ maps the logical location into sub-locations such that, $Occurrence_{lloc}(lloc) \rightarrow 2^{lloc}$.

Basics definitions and functions of extended RBAC model are given below.

- $SUBJECTS = \{s_1, s_2, \dots, s_n\}$ is a set of n subjects in the system.
- $USERS = \{u_1, u_2, \dots, u_n\}$ is a set of n users in the system.

- $OBJ = \{o_1, o_2, \dots, o_n\}$ is a set of n objects in the system.
- $OPS = \{op_1, op_2, \dots, op_n\}$ is a set of n operations in the system.
- $PRMS = \{prms_1, prms_2, \dots, prms_n\}$ is a set of n permissions in the system such that $PRMS = 2^{(OPS \times OBJ)}$.
- $PLOC = \{ploc_1, ploc_2, \dots, ploc_n\}$ is a set of n physical locations in the system.
- $LLOC = \{lloc_1, lloc_2, \dots, lloc_n\}$ is a set of n logical locations in the system.
- $SPR = \{spr_1, spr_2, \dots, spr_n\}$ is a set of n spatial purpose roles that describes the authority and responsibility on a member of a role with respect to location and purpose.
- $SP = \{sp_1, sp_2, \dots, sp_n\}$ is a set of n spatial purpose that describes the space covered by the purpose.

We also include some administrative operations for the proposed model to add/delete user, add/delete role, assign/de-assign user-to-role assignment and permission-to-role assignment.

- *User-Role Assignment Relation:* $UA \subseteq USERS \times SPR$.
- *Role-Permission Assignment Relation:* $PA \subseteq PRMS \times SPR$.
- *Purpose-Location Assignment:* $SA \subseteq P \times LLOC$.
- *Spatial Purpose Role-Spatial Purpose Assignment:* $SPA \subseteq SPR \times SP$.
- *Spatial Domain-Spatial Purpose Assignment:* $SDOM_SP \subseteq SDOM_i \times SDOM_j \times SP$.
- *Spatial Purpose-Location Assignment:* $SA \subseteq SP \times LLOC$.
- *subject_user* ($s:SUBJECT$) $\rightarrow (u:USERS)$, one-to-one mapping of a subject s onto the subject's associated user u .
- *subject_roles* ($s:SUBJECT$) $\rightarrow 2^{SPR}$, one-to many mapping of a subject onto a set of spatial roles. Formally: $subject_roles \subseteq \{spr \in SPR \mid (subject_user(s), spr) \in UA\}$.
- *assigned_users* (SPR) $\rightarrow 2^{USERS}$, one-to many mapping of a role onto a set of users. Formally: $assigned_users(SPR) \subseteq \{u \in USERS \mid (u, spr) \in UA\}$.
- *assigned_prms* ($spr:SPR$) $\rightarrow 2^{PRMS}$, one-to-many mapping of a spatial role onto a set of permissions. Formally: $assigned_prms(spr) \subseteq \{prms \in PRMS \mid (prms, spr) \in PA\}$.
- *prms_roles* ($prms:PRMS$) $\rightarrow 2^{SPR}$, one-to-many mapping of permission onto a set of spatial roles.

Formally: $prms_roles(prms) \subseteq \{spr \in SPR \mid (prms, spr) \in PA\}$.

- *assignedSPR_sp* ($spr:SPR$) $\rightarrow 2^{SP}$, one-to-many mapping of spatial purpose role onto a set of spatial purposes. Formally: $assignedSPR_sp(spr) \subseteq \{sp \in SP \mid (spr, sp) \in SPA\}$.
- *assignedSDOM_sp* ($sdom_i, sdom_j$) $\rightarrow 2^{SP}$, mapping of spatial domain multi-level and multi-domain relationship into set of spatial purposes. Formally: $assignedSDOM_sp(sdom_i, sdom_j) \subseteq \{sp \in SP \mid (sdom_i, sdom_j, sp) \in SDOM_SP\}$.
- *assignedSDOM* ($sdom, sp$) $\rightarrow 2^{SDOM}$, mapping of spatial domain relationship onto other spatial domain with respect to spatial purposes. Formally: $assignedSDOM(sdom, sp) \subseteq \{sdom_i \in SDOM \mid (sdom, sp) \in SDOM_SP\}$.
- *assignedLOC_sp* (sp) $\rightarrow 2^{LLOC}$, one-to-many mapping of spatial purposes onto the set of logical locations. Formally: $assignedLOC_sp(sp) \subseteq \{lloc \in LLOC \mid (sp, lloc) \in SA\}$.
- *assignedSP_loc* $\rightarrow 2^{SP}$, one-to-many mapping of a spatial purpose onto the set of logical locations. Formally $assignedSP_loc(lloc) \subseteq \{sp \in SP \mid (sp, lloc) \in SA\}$.

Our proposed policy is a tuple in the form $\langle s, r, op, o, ftime, etime, l \rangle$ which semantically denotes a request by a user in a subject role s with a role r to perform an operation op on a resource in object role o under the temporal condition $ftime$ and $etime$, location condition l .

6. CONCLUSION AND FUTURE WORK

In this paper, we have proposed an extension of RBAC by introducing the notion of purpose-roles. We argue that notion of purposes must be defined in access control policies as it helps the organizations to know *which* user can perform *what* operations on *which* object for *what* purpose. A purpose tree has been given for purpose role management. We have presented the proposed policy syntax that can be used to define purpose-oriented access control policies. We also explained our understanding of the concept domain and presented the extended RBAC architecture for multi-domain environment.

The basics of extended RBAC function and administrative operations have been given. Our future work makes use of the extended functions and allows administrator to define purpose-oriented roles to secure organizational resources that can be accessed from anywhere, anytime in a distributed multi-domain environment.

As for the role management, we do not consider hierarchical relationship among roles and policies. Also separation of duty including both static and dynamic and special constraints like cardinality

constraints implementation needs to be discussed. We leave these issues for our future work.

7. REFERENCES

- [1] Open Clinic, Decision Support Systems, <http://www.openclinical.org/dss.html>. Last accessed on: January 22, 2007.
- [2] P. Wohlmacher, P. Pharow: Applications in health care using public-key certificates and attribute certificates, Annual computer security applications conference, pp. 128, ISBN: 0-7695-0859-6, (2000).
- [3] M.N. Tahir: A secure online medical information system in distributed and heterogeneous computing environment, *Information & Security: An International Journal*, vol. 15, No.2, pp. 211-215, (2004).
- [4] A. Hess and K.E. Seamons: Access control model for dynamic client-side content, Proceedings of the eighth ACM symposium on Access control models and technologies, Como, Italy, pp. 207 – 216. ISBN: 1-58113-681-1, (2003).
- [5] M.N. Tahir: Architectural representation of c-rbac, contextual role-based access control, *Journal of Privacy Technologies*, (paper under review).
- [6] D. Ferraiolo and R. Kuhn: Role-based access control, Proceedings of 15th National Computer Security Conference, USA, (1992).
- [7] R. Sandhu, R. Coyne, H. Feinstein and C. Youman: Role-based access control models. *IEEE Computer* vol. 29, issue 2, pp 38-47, (1996).
- [8] R. Sandhu, D. Ferraiolo, and R. Kuhn: The NIST model for role-based access control: Towards a unified approach, Proceedings of ACM Workshop on Role-Based Access Control, Berlin, Germany, ISBN: 1-58113-259-X, pp. 47-63, (2000).
- [9] E. Bertino, C. Bettini, E. Ferrari, and P. Samarati: An access control model supporting periodicity constraints and temporal reasoning, *ACM Transactions on Database System*, vol. 23, issue 3, pp. 231–285, (1998).
- [10] J.B.D. Joshi, E. Bertino, U. Latif and A. Ghafoor: A generalized temporal role-based access control model, *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, issue 1, pp. 4-23, (2005).
- [11] T.Y.C. Woo and S.S. Lam: Designing a distributed authorization service, Proceedings of IEEE INFOCOM, vol. 2, pp. 419-429, (1998).
- [12] B. Gopal and U. Manber: Integrating content-based access mechanisms with hierarchical file systems, Proceedings of the third symposium on Operating systems design and implementation, pp. 265-278, (1999).
- [13] S. Chandaran and J.B.D Joshi: LoT-RBAC: A location and time-based RBAC model, Proceedings of the 6th International Conference on Web Information Systems Engineering (WISE'05), pp. 361-375, New York, USA, (2005).
- [14] E. Bertino, B. Catania, M.L. Damiani and P. Persasca: GEO-RBAC: A Spatially AwareRBAC, 10th Symposium on Access Control Models and Technologies (SACMAT'05), Stockholm, Sweden, pp. 29-37, (2005).
- [15] F. Hansen and V. Oleshchuk: Spatial role-based access control model for wireless networks, 58th IEEE Vehicular Technology Conference (VTC'03), vol. 3, pp. 2093 – 2097, (2003).
- [16] W. Qiang, H. Jin, X. Shi, D. Zou, and H. Zhang: RB-GACA: A rbac based grid access control architecture, GCC 2003, LNCS 3032, pp. 487–494, (2004).
- [17] H. Jin, W. Qiang, X. Shi and D. Zou: RB-GACA: A rbac based grid access control architecture, *International Journal of Grid and Utility Computing*, vol. 1, no. 1, pp. 61-70, (2005).
- [18] M. Covington, M. Moyer and M. Ahmad: Generalized role-based access control for securing future applications, Proceedings of the 23rd National Information Systems Security Conference, Baltimore, MD, (2000).
- [19] J.W. Byun, N. Li: Purpose based access control for privacy protection in relational database systems, *The VLDB Journal: The international journal on very large databases*, (2004).
- [20] D. Ferraiolo, R. Sandhu, S. Gavrila, R. Kuhn and R. Chandramouli: Proposed NIST standard for role-based access control, *ACM Transactions on Information System Security*, vol. 4, issue 3, pp. 224-274, (2001).
- [21] M.S. Sloman and K.P. Twidle: Domains: A Framework for Structuring Management Policy, *Network and Distributed Systems Management*, Addison-Wesley, pp.433-453, issue 16, (1994).
- [22] E. Constantine: A role-based framework for distributed systems management, PhD Thesis, (1998).
- [23] World Wide Web Consortium (W3C), Platform for Privacy Preferences (P3P), www.w3.org/P3P. Last accessed on: January 10, 2007.