Separation of Duty and Context Constraints For Contextual Role-Based Access Control (C-RBAC)

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

Abstract

This paper presents the separation of duty and context constraints of recently proposed Contextual Role-Based Access Control Model C-RBAC. Constraints in C-RBAC enabled the specification of a rich set of Separation of Duty (SoD) constraints over spatial purpose roles. In healthcare environment in which user roles are position and are purpose dependant, the notion of SoD is still meaningful and relevant to the concept of conflict of interest. SoD may be defined as Static Separation of Duty (SSoD) and Dynamic Separation of Duty (DSoD) depending on whether exclusive role constraints are evaluated against the user-role assignment set or against the set of roles activated in user's session. In particular, the model is capable of expressing a wider range of constraints on spatial domains, location hierarchy schemas, location hierarchy instances, spatial purposes and spatial purpose roles.
.

Keywords: Separation of duty, Constraints, C-RBAC, Location Hierarchy Schemas.

1. INTRODUCTION

Today, organizations have assumed their global presence because of advancement in intranet and internet technologies due of which organizations, today, are able to provide location based services to its customers and users anywhere, anytime. On the other hand, rapid growth in mobile technology has made it possible for the users to access organization resources, no matter, they are in static or in motion state. Because of the global presence of organizations and its widely dispersed resources and services, security of resources is the biggest threat to organization in terms of its business and even reputation. Similarly, to user and customer, the threat is the unauthorized usage of their personal and confidential information no matter by any outside intruder or employee of any company for example data entry operators, clerks, doctors, bankers etc.

In order to promise the security and correct usage of information, many countries have ratified legislation to protect privacy for individuals [1]. For example, Gramm-Leach-Bliley Act (GLB Act) [2] for financial sector, Health Insurance Portability and Accountability Act (HIPAA) [3] for medical sector in United States, Personal Information Protection and Electronic Documents Act (PIPEDA) [4, 5] 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.

In order to cope with these legislations, many access control and privacy based access control models have been proposed that have tried to ensure the security of organization resources. Some examples are time based [9, 10, 11, 12], location based [13, 14, 15, 18], Spatio temporal [16, 17] and purpose based [6, 7, 8]. However they lack in addressing an issue that how organizations can be partitioned in terms of departmental domains? Another issue that we noted is location hierarchy ambiguity.

Context Constraints

Constraints are a mechanism that help an organization lay out a higher level policy that has to be honored before every access. Constraints can apply to user-role, role-permission assignments and other factors such as time criteria to be followed before every access. An important constraint used to prevent abuse of authority is the constraint on roles to be mutually exclusive. This is related to the principle of separation of duties [18]. A similar constraint on mutually exclusive permissions also supports this principle of separation of duties for permissions. Constraints act as prerequisites on roles and permissions that any subject has to pass in order to be granted the requested role / permission. Basic event expressions used by C-RBAC constraint specification language are presented in table 1. These event expressions were used to enable/disable purposes, locations at different granularities and to define spatial purpose relationship between purpose and locations at lloc/ploc, lhs/lhi and sdom level. Through these expressions, a location can be enabled or disabled. This helps to restrict the access control decisions for a specific location or a complete set of hierarchically organized locations at location hierarchy schema/instance or domain level. These expressions also allow the administrator to enable or disable purposes or spatial purposes that are defined at a particular location or a group of locations.

Simple Event (p ∈ PURPOSE, ploc ∈ PLOC, lloc ∈ LLOC, LHS ∈ LHSS, LHI ∈ LHIS whereas ploc, lloc, LHS and LHI ∈ loc_type	
enable p or disable p	*To enable or disable purpose*
$enable_p$ *p* at *loc_type* or $disable_p$ *p* at *loc_type*	*To enable or disable purpose at different location granularities*
$assign_p$ *p* to *loc_type* or $de\text{-}assign_p$ *p* to *loc_type*	*To assign or de-assign purpose at different location granularities*
$assign_p$ *p* to *s* or $de\text{-}assign_p$ *p* to *s*	*To assign and de-assign purpose to a users' session*
enable loc_type or disable loc_type	*To enable or disable locations with different granularities like lloc, ploc, lhs, lhi or sdom*

Table 1: Events defined for purpose and location context

Table 2 shows status predicates used by C-RBAC model to check enabling/disabling, active and assignment status of purpose and location alone and also purpose with different location granularities.

Status Predicate	*Status Predicate with location and time*	*Semantics for*
enabled (p)	*enabled(p, loc_type, t)*	*p is enabled at [location loc_type] and [time t]*
enabled (p, loc_type)	*enabled (p, loc_type, t)*	*p is enabled at [location loc_type] and [time t]*
assigned (p, loc_type)	*assigned (p, loc_type, t)*	*p is assigned to [location loc_type] at [time t]*
assigned (p, s)	*assigned (p, s, loc_type, t)*	*p is assigned to users' session s at [location loc_type] and [time t]*
active (p)	*active (p, loc_type, t)*	*p is active at [location loc_type] and [time t]*
enabled (loc_type)	*enabled(loc_type, t)*	*Loc_type is enabled at [time t]*

Table 2: Status predicates for purpose and location context

Table 3 summarizes the constraint types and expressions that are applicable on purpose and location context used by C-RBAC model. For all C-RBAC constraints, time_epr define the time and loc_type define a location with different granularity:

Constraint Categories	*Constraints*	*Expression*
Purpose with location and time constraints	*Purpose enabling*	*([time_epr],[loc_type],$enable_p$ / $disable_p$ p)*
	Purpose assignment	*([time_epr],[loc_type],$assign_p$ / $de\text{-}assign_p$ p)*
Purpose with location and duration constraints	*Purpose enabling*	*([$time\_epr_1$, $time\_epr_2$],[loc_type],$enable_p$/ $disable_p$ p)*
	Purpose assignment	*([$time\_epr_1$, $time\_epr_2$],[loc_type],$assign_p$/ $de\text{-}assign_p$ p)*
location with time constraints	*Location enabling*	*([time_epr], $enable_t$ / $disable_t$ loc_type)*

Table 3: C-RBAC Constraints types

Purpose with location and time constraints These constraints were used to specify the exact time interval during which the purpose can be enabled or disabled at some location, and during which purpose over location (spatial purpose) assignment is valid. For example if the requirement is to not to authorize any surgeon in surgical ward to write patient's PHI for routine checkup between 8pm to 8am then purpose enabling constraint can be defined to disable purpose at surgical ward location with the specified time interval. Similarly if the requirement is to allow surgeon to access PHI from MinorOPT for emergency purpose then purpose assignment constraint can be defined to assign emergency purpose at MinorOPT.

Purpose with location and duration constraints These constraints are used to specify the time duration for which an enabled purpose or purpose assigned at some location is valid. These types of constraints are useful in enforcing obligation or retention policies for example if the obligation or retention policy states that no access to PHI should be granted for more than 2 hour from surgical ward for routine operation purpose then these constraints can be helpful to enforce such privacy rules to disable or de-assign routine operation purpose at surgical ward after the

specified time duration is over. Similarly if the privacy rules states that no access to PHI is granted from research department between 5pm to 8am then duration constraints with purpose assignment can be defined on research department to de-assign research purpose at the specified time.

Location with time constraints These constraints are used to specify the time duration for which a location is enabled and access decisions should be evaluated for the user requesting from that location during the specified time. These types of constraints are useful in enforcing obligation or retention policies for example if the obligation policy states that access to PHI should be granted from emergency ward between 7pm to 8am then these constraints can be helpful to enforce such privacy rules to enable emergency ward spatial domain during the specified time.

Privacy constraints on SPR enabling, activation, user-role, role-permission assignments

Table 4 shows basic event expressions used by C-RBAC constraint specification language. These event expressions are used to enable/disable spatial purposes role and to assign and de-assign spatial purpose role to users; and permissions to spatial purpose roles.

Simple Event (spr ∈ SPR, u ∈ USERS, and prms∈ PRMS	
enable spr or disable spr	*To enable or disable spatial purpose role*
$assign_u$ *spr* to *u* or $de\text{-}assign_u$ *spr* to *u*	*To assign or de-assign spatial purpose role to user*
$assign_p$ *prms* to *spr* or $de\text{-}assign_p$ *prms* to *spr*	*To assign and de-assign permissions to spatial purpose role*

Table 4: Events defined for spatial purpose role

Table 5 shows status predicates used by C-RBAC model to check enabling/disabling, active and assignment status of spatial purpose role to users; and permissions to spatial purpose role. Given a time duration and location granularity, these predicates check the status of spatial purpose role enabling and activation.

Status Predicate	***Status Predicate with location and time***	***Semantics for***
enabled (spr)	*enabled(spr, loc_type, p, t)*	*spr is enabled at loc_type at t with for p*
$assigned_u$ *(u, r)*	*assigned (u, spr, loc_type, p,t)*	*u at loc_type is assigned to spr for p at time t*
$assigned_p$ *(prms, r)*	*assigned (prms, spr, loc_type, p,t)*	*prms is assigned to spr at loc_type for p at time t*
$active_{spr}$ *(spr)*	*active (spr, loc_type, p, t)*	*spr is active at loc_type with p at t*
Can_activate(u,spr)	*Can_activate(u, spr, loc_type, p, t)*	*u at loc_type can activate spr for p at time t*
Can_acquire(u,prms)	*Can_acquire(u, prms, loc_type, p, t)*	*u at loc_type can acquire prms for p at time t*

Table 5: Status predicates for spatial purpose role

Based on the simple events and status predicates defined for spatial purpose role in table 4 and 5 respectively; table 6 summarizes the constraint types and expressions that are applicable on spatial purpose role in C-RBAC model. For all C-RBAC constraints, time_epr defines the time and loc_type defines a location with different granularity such that:

Constraint Categories	***Constraints***	***Expression***	
p ∈ PURPOSE, loc_type ∈ PLOC, LLOC, LHSS, LHIS, SDOM, u ∈ USERS, prms ∈ PRMS			
Privacy constraints on spr enabling, user-role and role-permission assignments	*SPR enabling*	*(time_epr, loc_type, p, $enable_{spr}$ / $disable_{spr}$ spr)*	
		([$time\_epr_1$, $time\_epr_2$], loc_type, p, $enable_{spr}$/ $disable_{spr}$ spr)	
	User-role assignment	*(time_epr, loc_type, p, $assign_u$ / $de\text{-}assign_u$ spr to u)*	
		([$time\_epr_1$, $time\_epr_2$], loc_type, p, $assign_u$/ $de\text{-}assign_u$ spr to u)	
	Role-permission assignment	*(time_epr, loc_type, p, $assign_p$ / $de\text{-}assign_p$ prms to spr)*	
		([$time\_epr_1$, $time\_epr_2$], loc_type, p, $assign_p$/ $de\text{-}assign_p$ prms to spr)	
Privacy Constraints on SPR Activation			
Duration Constraints	*Total active role duration*	*Per-role*	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, D_{active}, $active_{spr}$ spr)*
		Per-user-role	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, u, $D_{uactive}$, $active_{spr}$ spr)*
	Max. role duration per activation	*Per-role*	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, D_{max}, $active_{spr}$ spr)*
		Per-user-role	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, u, D_{umax}, $active_{spr}$ spr)*
Cardinality Constraints	*Total no. of activations*	*Per-role*	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, N_{active}, $active_{spr}$ spr)*
		Per-user-role	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, u, $N_{uactive}$, $active_{spr}$ spr)*
	Max. no of concurrent activations	*Per-role*	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, N_{max}, $active_{spr}$ spr)*
		Per-user-role	*([$time\_epr_1$, $time\_epr_2$], loc_type, p, u, N_{umax}, $active_{spr}$ spr)*

Table 6: Privacy constraints on spatial purpose role for C-RBAC model

As explained earlier that a spatial purpose role can have disabled, enabled and active states. These different states lead us to define different privacy constraints of C-RBAC model shown in table 6. Specifically, these constraints can be applied to roles as well as to user-role and role-

permission assignments. Depending on the healthcare requirements, spr enabling and activation can be restricted to particular time, location and purpose.

Privacy constraints on SPR enabling This category of constraints were defined to specify the time interval, location and purpose during which spr can be enabled or disabled, and during which user-role and role-permission assignments are valid. For example, spr enabling constraints can be defined to restrict researchers to not to access medical information from laboratory for research purpose during a specific time interval. Constraints on user-role assignments can be defined to restrict users of a particular category to not to access PHI for a specific purpose, from specific location at specific time. Similarly role-permission assignment constraints restrict permission assignment to spatial purpose role during a specific time interval, from specific location for specific purposes.

Privacy constraints on SPR activation These constraints restrict users to activate spatial purpose role from the location, purpose and time duration specified in the constraint. For example total activation duration constraint on spr restricts the span of the role's activation duration in a given period to a specified value from specific location for specific purpose. After the users have utilized the specified total active duration for spr from the specified location with specified purpose, spr cannot be activated again, even though it may still be enabled. The total active duration constraint may be specified on per-role and per-user-role basis. Per-role constraint restricts the total active duration for spr. Once the sum of all the activation durations of spr reaches the maximum allowed value from the specified location and purpose, no further activation of the role is allowed and the current activations are terminated. Per-user-role constraint restricts the total active duration for spr by a particular user. Once a user utilizes the total active duration of his spr, he is not allowed to further activate spr, whereas other users may still activate it.

The maximum duration constraint per activation constraint restricts the maximum allowable duration for each activation of a spr from a specific location with specific purpose. Once such time duration expires for a user, spr activation for that user becomes invalid. However, there may still be other activations of the same spr in the system, including one by the same user in some other session from different location or with different purpose. This constraint can also be specified on per-role or per-user-role basis. A per-role constraint restricts the maximum active duration for each spr activation for any user, unless there is a per-user-role constraint specified for that user. A per-user-role constraint restricts the maximum active duration allowed for each activation of a spr by a particular user. Activation duration can be limited within a pre-specified interval.

Healthcare applications may also imply restrictions on concurrent activation of spr for controlling access to sensitive information. In order to impose such restrictions cardinality constraints on spr activations was introduced. This constraint was categorized into two types: total number of activations and maximum number of concurrent activations. With total number of activations, spr activations can be limited to N activations. This constraint can be specified as per-role and per-user-role. Per-role constraint allows at most Nactive activations of spr in a given time interval from a specific location and purpose whether these activations occur simultaneously in different sessions or at different times. Once the total number of activations equals to Nactive, users will not be able to activate spr from the specified location with the same purpose. For example, a per-role constraint can be defined on researcher role to ensure that users from research department do not access all the resources while others are denied access. Similarly, in order to restrict the number of activations for a specified user, per-user-role constraint can also be defined.

Through maximum number of concurrent activations constraint, spr is restricted to N concurrent activations in a specified time, location and purpose. This constraint on per-role based can be specified to restrict the number of concurrent activation of spr to a maximum value. For example, if only 3 doctors are on duty in emergency ward then it is easy to assume that emergency doctor role can have utmost 3 activations from emergency ward. No more than 3 activations will be allowed to perform operations. Similarly, per-user-role constraints restrict the total number of activations of spr by a particular user to a given value.

Separation of Duty (SoD) Constraints

Constraints in C-RBAC enable the specification of a rich set of Separation of Duty (SoD)constraints over roles. SoD is widely recognized to be a fundamental principle in computer security [Li et al. 2004]. These constraints are introduced to prevent conflicts of interest arising when a single individual can simultaneously perform sensitive tasks requiring the use of mutually exclusive duties. The general form of a role exclusive constraint is: ({r1, ..., rm}, n) where each r1 is a role and n and m are integers with $n \leq m$. This constraint forbids a user to be a member of n or more roles in {r1, ..., rm} [Li et al. 2004]. In a the presence of context in which the user's roles are dependent on the position and purposes, the notion of SoD is still meaningful and thus the contextual dimension is relevant for the concept of conflict of interest. This pragmatic observation has led us to define exclusive role constraints for spatial purpose roles. The work defines two types of constraints Static Separation of Duty Constraints (SSoD) and Dynamic separation of Duty Constraints (DSoD). These constraints states that a user cannot play two conflicting spatial purpose roles at enabling or activation time at given location and purposes. For example, a separation of duty constraint preventing the same user to enable the role of practitioner nurse from entering the patient PHI and head nurse for approving a patient PHI. Similarly, one should not be authorized to play the role of practitioner nurse and head nurse. On the other hand, there are also cases in which conflict arises because of spatial or purpose context. For example, an individual should not be allowed to activate the role of emergency doctor and cardiologist in emergency ward and cardiac care ward simultaneously.

A SoD relation in C-RBAC consists of a triplet: (SSoD_Name, SP_RS, n). The SoD_Name indicates the transaction or business process in which common user membership must be restricted in order to enforce a conflict of interest policy. The SP_RS is a set containing the constituent spatial purpose roles for the named SoD relation. The n designates the cardinality of the subset within the SP_RS to which common user memberships must be restricted. Cardinality greater than one indicating a combination of spatial purpose roles that would constitute a violation of the SoD policy. For example, an organization may require that no one user may be assigned to three of the four roles that represent the medical treatment function.

Static Separation of Duty (SSoD)

Preventing a user from gaining authorization for permissions associated with conflicting roles can be achieved through SSoD. SSoD allows the enforcement of constraints on the assignment of users to roles. These constraints can take on a wide variety of forms like user-based, role-based, permission-based (Jaeger, T., and Tidswell,2001). Static constraints have also been shown to be a powerful means of implementing a number of other important separation of duty policies for example Gligor et al. [1998] formally defined four other types of static separation of duty policies. The static constraints defined in this section are those that place restrictions on sets of spatial purpose roles and in particular on their ability to form UA relations. This means that if a user is assigned to one spatial purpose role, the user is prohibited from being a member of a second

spatial purpose role. For example, a static constraint preventing the same user to enable the role of Surgeon for reading the patient's PHI in surgical ward and Surgeon_MinotOPT for reading the patient's PHI from MinorOPT. Similarly the static constraint restricts the user that one should not be authorized to play the role of practitioner nurse and head nurse simultaneously at the same location for the purpose of PHI entry and PHI entry approval respectively. The formal definition of static separation of duty is given below.

Definition 1 ***(SSoD)*****:** Static separation of duty is defined as a triplet (SSoD_Name, SP_RS, n) where SSoD_Name indicates the transaction or business process in which common user membership must be restricted in order to enforce a conflict of interest policy, each SP_RS is a spatial purpose role set, and n is cardinality such that;

$$SSoD \subseteq (2SPRloc\_type\ ,\ p \times N)$$

If q a subset of roles in SP_RS, and n is a natural number ≥ 2, with the property that no user is assigned to n or more roles from the set SP_RS in each (SSoD_Name, SP_RS, n) ∈ SSoD. Formally:

$$\forall (SP\_RS,\ n) \in SSoD, \forall q \subseteq SP\_RS:\ |q| \geq n) \Rightarrow \bigcap\nolimits_{r \in t}\ AssignedUser(spr_{loc\_type,p}) = \emptyset$$

Since the SSoD property relates to membership of users in conflicting roles, the AssignedUser function shall incorporate functionality to verify and ensure that a given user assignment does not violate the constraints associated with any instance of an SSoD relation.

Consider the set SP_RoleSet = {Surgeonloc_type,p , Surgeon_MinorOPTloc_type,p}. According to SSoD definition, the constraint (SP_RS, 2) ∈ SSoD; means that an individual cannot be Surgeon and Surgeon_MinorOPT at the same time, at same location with the same purpose.

Similarly a constraint can be defined to prevent the user from playing n distinct spatial purpose roles from the same location and purposes. For example, consider a spatial purpose role <Surgeon, Loc_TypeSurgeon, PSETSurgeon>, a SSoD constraint can be defined as (SurgeonConstraint, Surgeonloc_type,p, 2) ∈ SSoD means that an individual can be a surgical doctor in at most one location depending on the loc_type and p defined for Surgeonloc_type,p.

Definition 2 (*Static Separation of Duty in the Presence of a Hierarchy*): In the presence of a spatial purpose role hierarchy, static separation of duty is redefined based on authorized users rather than assigned users as follows.

$$\forall (SP\_RS,\ n) \in SSoD, \forall q \subseteq SP\_RS:\ |q| \geq n) \Rightarrow \bigcap\nolimits_{r \in t}\ authorized\_users(spr_{loc\_type,p}) = \emptyset$$

Dynamic Separation of Duty (DSoD)

Like SSoD, dynamic separation of duty is also intended to limit the permissions that are available to the user. However DSoD relations differ from SSoD relations by the context in which these limitations are imposed. SSoD relations define and place constraints on a user's total permission space whereas DSoD constraints limits the availability of the permissions over a user's permission space by placing constraints on the spatial purpose roles that can be activated within or across a user's sessions. DSoD allow a user to be authorized for two or more spatial purpose roles that do not create a conflict of interest when acted on independently, but produce conflict of interest concerns when activated simultaneously. For example, a user may be authorized for both the roles of nurse and headnurse, where the nurse is allowed to enter patient's PHI and headnurse is allowed to acknowledge corrections in the patient's PHI. If the individual acting in the role nurse attempts to switch the role to headnurse, DSoD would require the user to drop the role nurse before assuming the role of headnurse. As long as the same user is not allowed to assume both of these roles at the same time, a conflict of interest situation will not arise.

Definition 3 (*DSoD*): Dynamic separation of duty is defined as a triplet (DSoD_Name, SP_RS, n) where DSoD_Name indicates the transaction or business process in which common user membership must be restricted in order to enforce a conflict of interest policy, each SP_RS is a spatial purpose role set, and n is cardinality such that;

$$DSoD \subseteq (2^{SPR}{}_{loc\_type\,,\,p} \times N)$$

If q a subset of roles in SP_RS, and n is a natural number ≥ 2, with the property that no user may activate n or more roles from the set SP_RS in each (DSoD_Name, SP_RS, n) ∈ DSoD. Formally:

$$\forall SP\_RS \in 2^{SPR}{}_{loc\_type\,,\,p},\ n \in N,\ (SP\_RS,\ n) \in DSoD \Rightarrow n \geq 2 \wedge |SP\_RS| \geq n,\ and$$
$$\forall s \in SESSIONS,\ \forall SP\_RS \in 2^{SPR}{}_{loc\_type\,,\,p},\ \forall role\_subset \in 2^{SPR}{}_{loc\_type\,,\,p},\ \forall n \in N,\ (SP\_RS,\ n)$$
$$\in DSoD,\ role\_subset \subseteq SP\_RS,\ role\_subset \subseteq session\ roles(s)\ ) \Rightarrow |role\_subset| < n.$$

Consider a SP_RS = $\{Surgeon_{loc\_type,p}\,,\ Surgeon\_MinorOPT_{loc\_type,p}\}$. The DSoD constraint (SP_RS, 2) means that an individual cannot activate both spatial purpose roles in the same session. In other words, a surgical doctor cannot activate the role of Surgeon in Surgical and MinorOPT wards.

Similarly the constraint $\{EmergencyDoctor_{loc\_type,p},\ 2\}$ means that the role $EmergencyDoctor$ can be active in more than one ward and thus play different roles with different permissions, however if an individual be located there and the wards share a common space, then only one of such spatial purpose roles can be enabled depending on the purpose of the user.

2. CONSLUSION & FUTURE WORK

In this paper, constraints for C-RBAC were presented that enable the specification of a rich set of Separation of Duty (SoD) constraints over spatial purpose roles. Precisely, this chapter provides the specification of the context constraints based on the privacy requirements and different states of roles as explained in the previous chapter. Then privacy constraints on SPR enabling, activation, user-role, role-permission assignments were presented. Making the constraints as a

base, the study then discussed the separation of duty including static (SSoD) and dynamic (DSoD) used by the proposed C-RBAC model.

3. REFERENCES

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

[2]. U.S. Senate Committee on Banking, Housing, and Urban Affairs (1999). Information Regarding the Gramm-Leach-Bliley Act of 1999 [GLB Act]. [Online]. Available: http://banking.senate.gov/conf [2007, October 15].

[3]. Health Insurance Portability & Accountability Act [HIPAA] (1996). [Online]. Available: http://www.hipaa.org [2007, October 15].

[4]. Personal Information Protection and Electronic Documents Act [PIPEDA] (2000). [Online]. Available: http://www.nymity.com/pipeda/ [2007, October 15].

[5]. PIPEDA: Personal Information Protection and Electronic Documents Act (2004), Department of Justice of Canada [Online]. Available: laws.justice.gc.ca/en/P-8.6/text.html [2006, December 13]

[6]. Ying, C. S. (2006). Health Insurance Portability and Accountability Act (HIPAA)-compliant Privacy Access Control Model for Web Services. Master's thesis, The Hong Kong University of Science and Technology, Hong Kong.

[7]. Sidiroglou, S., Ioannidis, S., and Keromytis, A. D. (2006). Privacy as an operating system service. In Proceedings of the Workshop on Hot Topics in Security (HOTSEC), Vancouver, CA.

[8]. Protecting the Privacy of Patients' Health Information, Available: http://www.hhs.gov/news/facts/privacy.html [2007, June 28]

[9]. Bertino, E., Bonatti, P. A. and Ferrari, E. (2001). TRBAC: A temporal role-based access control model. ACM Transactions on Information and System Security, 4(3), 191–233.

[10]. 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.

[11]. Joshi, J. B. D., Shafiq, B., Ghafoor, A. and Bertino, E. (2003). Dependencies and separation of duty constraints in GTRBAC. In Proceedings, ACM Symposium on Access Control Models and Technologies, 51–64.

[12]. Joshi, J.B.D., Bertino, E. and Ghafoor, A. (2002). Temporal Hierarchies and Inheritance Semantics for GTRBAC. In Seventh ACM Symposium on Access Control Models and Technologies (SACMAT02), Monterey, California, USA.

[13]. Mantoro, T. and Johnson, C. W. (2003). Location History in a Low-cost Context Awareness Environment. Workshop on 'Wearable, Invisible, Context-Aware, Ambient, Pervasive and Ubiquitous Computing', Australian Computer Science Communications, 21(6), Adelaide, Australia.

[14]. Ray, I. and Kumar, M. (2006). Towards a location-based mandatory access control model. Computers & Security, 25(1), 36-44.

[15]. Bertino, E., Catania, B., Damiani, M.L. and Persasca, P. (2005). GEO-RBAC: A Spatially AwareRBAC, 10th Symposium on Access Control Models and Technologies (SACMAT'05), Stockholm, Sweden, 29-37.

[16]. Suroop, C. and Joshi, J.B.D. (2005). LoT-RBAC: A Location and Time-Based RBAC Model. In Proceedings of 6th International Conference on Web Information Systems Engineering, LNCS 3806, 361-375, New York, USA.

[17]. Fu, S., Xu, C. (2005). 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.

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