La mise en oeuvre d'un modèle de contrôle d'accès adapté aux systèmes pervasifs. Application aux équipes mobiles gériatriques.

Dana Al Kukhun, Florence Sèdes

La mise en œuvre d'un modèle de contrôle d'accès adapté aux systèmes pervasifs

Application aux équipes mobiles gériatriques

Dana Al Kukhun — Florence Sèdes

IRIT, Université Paul Sabatier
118, Route de Narbonne
F-31062 Toulouse cedex 9
{kukhun, sedes}@irit.fr

RÉSUMÉ. *Les équipes mobiles gériatriques (EMG) se déplacent auprès du plus grand nombre de personnes âgées afin d'assurer des services dans le cadre d'une consultation globale. Les EMG ont besoin d'un système interopérable qui permet une facilité d'acquisition des données du patient qui sont distribuées et gérées par plusieurs autorités. Dans ce papier, nous montrons un système d'information pervasif dédié aux EMG. Un tel système permettra une évolution du domaine en termes de qualité et d'efficacité ; il garantira un accès transparent aux ressources médicales depuis n'importe où, n'importe comment et à n'importe quel moment. Nous mettons également en œuvre un contrôle d'accès basé sur XACML pour assurer la sécurité de tels systèmes détenant des informations privées et confidentielles.*

ABSTRACT. *Mobile Geriatric Teams (EMG) are evolving to meet the needs of the growing number of elder patients and to guarantee the delivery of better services through a comprehensive consultation. The EMG need an interoperable system that allows easy acquisition of patient data that are distributed and managed by several authorities. In this paper, we present a pervasive information system dedicated to serve the EMG. Such a system will strengthen the quality and increase the efficiency of medical decision-making, it will ensure seamless access to medical resources from anywhere, anyhow and anytime. We also implement access control based on XACML to ensure the security of systems holding such information that is highly private and confidential.*

MOTS-CLÉS : *systèmes de santé, systèmes pervasifs, contrôle d'accès, accessibilité, adaptation, RBAC, XACML.*

KEYWORDS: *healthcare systems, pervasive systems, access control, accessibility, adaptation, RBAC, XACML.*

DOI:10.3166/DN.12.3.59-78

1. Introduction

La notion d'ubiquité a été présentée par Weiser (1999) qui a prédit l'évolution des systèmes d'information au 21^{e} siècle en systèmes d'informations pervasifs, où les éléments de calcul vont « disparaître » en fonctionnant d'une manière homogène et en transparence totale. De tels systèmes ont pour objectif de permettre aux utilisateurs de communiquer entre eux à tout moment, depuis n'importe où et avec n'importe quel outil (Park *et al*., 2004).

De plus en plus, les systèmes de santé adoptent les nouvelles technologies pour la génération, le traitement, le stockage et la consultation de données médicales. Cette adoption vise à assurer une meilleure qualité de service et un fonctionnement plus efficace pour une meilleure consultation des données dans différents contextes. Prenant en compte la quantité d'informations distribuées dans différents référentiels physiques, l'accès aux ressources médicales en temps réel est devenu prioritaire.

En conséquence et grâce à l'évolution technologique des matériels, des dispositifs mobiles, des logiciels et de la connectivité, les systèmes de santé trouvent leur voie vers l'ubiquité qui leur permettra d'assurer aux utilisateurs une accessibilité transparente aux ressources médicales à tout moment, depuis n'importe où et avec n'importe quel dispositif.

Dans ce papier, nous présentons une étude analytique que nous avons menée sur l'accessibilité aux ressources de données médicales en nous appuyant sur un exemple réel : les équipes mobiles gériatriques (EMG) de la région Midi-Pyrénées. Notre travail est basé sur les résultats d'un projet réalisé par l'Université de Toulouse (Faculté de Médecine et Laboratoire de Gestion et Cognition) pour le ministère de Santé[1] dont l'objectif est d'évaluer la performance des services EMG de la région Midi Pyrénées et leur efficacité dans la prise en charge des personnes âgées fragiles, voir (Arthus *et al*., 2009).

Dans un premier temps, nous soulignons l'importance et le besoin du contrôle d'accès au dossier médical non seulement par rapport au rôle de l'utilisateur (RBAC) mais aussi par rapport à son contexte (localisation, temps, machine, connexion, etc.) et à la situation d'utilisation du système (urgence, accès depuis une base de donnée non familière, etc.). Pour répondre à ce besoin, nous proposons donc une extension du modèle RBAC qui s'appuie sur des règles d'accès *ad hoc* et adaptatives pour mieux répondre aux besoins de l'utilisateur.

Ces règles adaptatives sont utilisées dans un système de prise de décision adaptatif qui traduit la demande de l'utilisateur dans une requête XACML et qui, dans le cas d'un refus d'accès, cherche des ressources alternatives en appliquant un

1. Contrat HAS/CNSA, n°07/0008, INSERM U558 – Département de Santé publique faculté de médecine de Toulouse et Laboratoire Gestion et Cognition (EA 2048) - Université Paul Sabatier Toulouse 3.

mécanisme de réécriture de requête qui prend en compte le rôle de l'utilisateur, son contexte et sa situation.

Dans un deuxième temps, nous allons montrer les différents défis liés à l'acquisition et à la consultation d'information au sein des EMG. Ces problèmes émergent des membres de l'équipe dans les différentes phases d'interaction (avec le patient, entre les membres de l'équipe ou avec les différents composants du système de santé). A partir de cette étude et pour répondre à ces problèmes, nous proposons un prototype qui favorise l'interactivité et la mobilité des utilisateurs et qui améliore l'insertion, la consultation et le passage des flux de données entre différentes ressources distribuées dans le système d'information pervasif.

2. L'accès aux systèmes de santé pervasifs

2.1. *Les caractéristiques pervasives des systèmes de santé*

En analysant les caractéristiques des systèmes de santé, nous pouvons dire qu'ils sont de plus en plus centrés sur l'utilisateur (médecin, infirmière, patient, etc.) et qu'ils utilisent des technologies orientées service pour garantir une certaine qualité. Dans ces systèmes, la qualité de services est critique car elle touche la vie du patient.

La sensibilité et la confidentialité des données médicales justifient le fait qu'elles soient conservées dans leurs ressources d'origine et distribuées dans différents sous-systèmes (hôpitaux, laboratoires d'analyse, cabinets de médecin, etc.). Cette décentralisation influence la gestion d'accès aux ressources médicales qui passe par la distribution des privilèges d'accès selon le rôle de l'utilisateur dans la hiérarchie du système en utilisant le standard RBAC – *Role Based Access Control* – (Ferraiolo *et al*., 1992).

La nature évolutive de données médicales est très intéressante car elle reflète non seulement l'avancement d'une situation d'un patient en prenant en compte l'axe temporel mais aussi, les différentes interventions qui ont eu lieu par les membres de l'équipe médicale. Sachant qu'une grande partie des données médicales est générée et traitée en temps réel, l'administration des privilèges d'accès doit être centralisée pour assurer l'intégrité du système et une prise de décision fiable.

La gestion des droits d'accès est soigneusement appliquée aux ressources médicales qui sont souvent regroupées et classées par patient dans un dossier médical personnel. Ce dossier contient plusieurs types de données (texte, image, vidéo, etc.) qui décrivent l'évolution de la situation d'un patient.

Afin de faciliter le partage de données, elles sont souvent regroupées et sauvegardées dans des documents « semi-structurés » représentés en XML – eXtensible Markup Language – format qui décrit le contenu et la structure d'un document dans un format textuel. La simplicité, l'expressivité et l'interopérabilité de XML ont favorisé son déploiement dans l'échange des données médicales.

Le fait que XML devienne, de plus en plus, un standard d'échange d'information médicale (HL7, 1994) rend nécessaire l'utilisation d'un standard de contrôle d'accès pour gérer la prise de décision dans cet échange. XACML – *eXtensible Access Control Markup Language* – (OASIS, 2003) par exemple est un standard qui décrit les droits d'accès des utilisateurs sous forme des politiques XML et qui permettra d'appliquer les principes donnés par les législations médicales.

2.2. *L'importance de la sécurité dans les systèmes de santé*

Les données médicales étant considérées par la loi comme des données privées, sensibles et confidentielles, différentes législations internationales et nationales ont été proposées pour assurer la protection des données médicales, en particulier La déclaration de Helsinki (Helsinki, 1964), l'acte de confidentialité « Privacy Act » (Privacy Act, 1974), la loi HIPPA (HIPPA, 1996) et la loi des droits des malades et la qualité de systèmes de santé en France (Loi 2003-303, 2003).

Cette confidentialité justifie le stockage des données médicales dans leurs ressources d'origine et impose plus de contraintes d'accès, particulièrement dans le cas d'une consultation mobile.

En conséquence, l'accès aux données dans un système de santé doit respecter les principes de la protection des données personnelles du patient. Ces données ne sont pas accessibles de la même façon pour tous les membres de l'équipe médicale mais sont souvent restreintes aux besoins de la tâche à réaliser par l'utilisateur.

Dans les systèmes de santé pervasifs, l'accès aux données devient plus exigeant car il dépend non seulement du rôle de l'utilisateur ou de l'horaire de sa demande mais aussi de différentes contraintes contextuelles telle que sa localisation, le dispositif qu'il utilise et le réseau avec lequel il se connecte, etc.

La section suivante présente un état de l'art sur les principaux modèles utilisés pour la gestion des droits d'accès dans les systèmes d'information de santé en prenant en compte les caractéristiques pervasives du domaine.

3. Les modèles de sécurité utilisés dans le contexte médical

Un processus de gestion d'accès est souvent réalisé en trois étapes principales ; la première consiste en une modélisation des droits d'accès réalisée à travers un modèle générique tel que le modèle RBAC. La deuxième consiste à intégrer le contexte. Avec l'évolution des systèmes d'information pervasifs, ce modèle a été étendu pour gérer le contexte de l'utilisateur lors de l'attribution d'une permission. La troisième est chargée de gérer la distribution de ces privilèges d'accès tel que XACML qui est un standard d'échange orienté-service.

3.1. *Le Modèle RBAC*

La motivation principale autour de la proposition d'un modèle de contrôle d'accès à base de rôle (RBAC) était de faciliter l'administration des privilèges d'accès pour un grand nombre d'utilisateurs accédant à des ressources distribuées. La solution présentée par (Ferraiolo *et al*., 1992) était de regrouper les utilisateurs dans des rôles reflétant la structure organisationnelle de l'entreprise et puis, de distribuer les permissions à ces rôles au lieu de le répéter par individu.

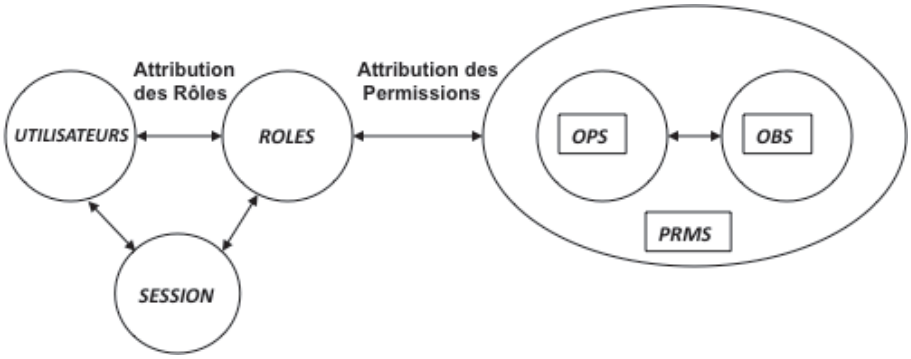

Figure 1. *Le Modèle RBAC*

Le ***rôle*** est le cœur du modèle RBAC et est vu comme une entité intermédiaire entre les utilisateurs et les permissions car il regroupe un ensemble de privilèges et les attribue, ensuite, aux utilisateurs en fonction de leur rôle.

Comme le montre la figure 1, l'attribution des rôles dans le modèle RBAC suit une relation mutuelle où un ***Utilisateur*** (personne, processus informatique, machine, etc.) peut jouer plusieurs rôles dans une seule session et un rôle peut être attribué à plusieurs utilisateurs.

$$\mathbf{AU} \subseteq \mathbf{Utilisateurs} \times \mathbf{Rôles}$$

L'attribution d'un rôle garantira plusieurs permissions ***PRMS*** à l'utilisateur et une permission peut être attribuée à plusieurs rôles.

$$\mathbf{AP} \subseteq \mathbf{Rôles} \times \mathbf{PRMS}$$

La nature d'une permission décrit le type d'opérations ***OPS*** (e.g. lire, écrire, mettre-à-jour, etc.) autorisé sur les objets ***OBS*** (ressources de données : documents, processus informatique, machines, etc.).

La relation entre ces objets et les opérations attribuées est aussi mutuelle ; une opération peut être autorisée sur plusieurs objets et à un objet peuvent être attribuées différentes permissions.

$$\mathbf{PRM} \subseteq \mathbf{OPS} \times \mathbf{OBS}$$

Afin de répondre aux besoins évolutifs de la gestion d'accès au sein de l'entreprise, le modèle RBAC a été étendu à différents profils afin de combler les lacunes et atteindre une meilleure performance à travers différents principes tels que la hiérarchie des rôles dans RBAC-1 (Sandhu, 1996) où un utilisateur peut hériter des droits d'accès d'un autre utilisateur, l'inclusion des contraintes lors de l'attribution d'un rôle dans RBAC-2 et la séparation des tâches distinctes entre les différents intervenants d'une mission dans RBAC-3 (Kuhn *et al*., 1997).

3.2. *L'évolution des modèles RBAC sensibles au contexte*

Avec l'évolution des systèmes d'information pervasifs, l'attribution d'une permission à un utilisateur est devenue plus complexe et dépendante du contexte. C'est la raison pour laquelle plusieurs nouveaux modèles d'accès ont été proposés pour prendre en compte l'évolution de la définition du contexte (temps, localisation, caractéristique du système, connexion de réseaux, dispositif de l'utilisateur, etc.).

L'axe temporel est le premier élément contextuel qui a été inclus dans le modèle RBAC : les travaux de (Bertino *et al*., 2001) ont étendu le modèle RBAC vers un modèle TRBAC (Temporal RBAC) qui considère le temps comme une contrainte qui peut déterminer l'activation et la désactivation d'un rôle. L'intégration de l'aspect temporel a donné plus de flexibilité pour créer des exceptions pour les individus et pour spécifier des dépendances temporelles entre les actions réalisées par un utilisateur.

Ensuite, avec l'évolution des dispositifs mobiles, l'intégration de la localisation de l'utilisateur a fait l'objectif de plusieurs travaux de recherche comme ceux de (Hansen *et al*., 2003) qui ont proposé un modèle RBAC Spatial ou l'attribution d'un rôle dépend à la position spatiale de l'utilisateur.

Les travaux de (Bertino *et al*., 2005) proposaient un modèle Géo-RBAC (Geographical RBAC) qui déterminent la localisation d'un utilisateur soit par son *positionnement physique exact* (à l'aid d'un GPS) ou à travers son *positionnement logique* calculé implicitement (à travers la région dans laquelle il se déplace, cette région peut être définie à différentes granularités).

Avec l'évolution de l'ubiquité, différents modèles sensibles au contexte ont été proposés tels que le modèle uT-RBAC (Chae *et al*., 2006) qui considère le temps et la localisation de l'utilisateur comme des éléments importants pour l'activation et désactivation d'un rôle.

D'autres travaux ont présenté un modèle RBAC sensible au contexte pour les systèmes pervasifs (Emami *et al*., 2007) et ont souligné le fait que les attributs contextuels sont très dynamiques ce qui peut risquer de déstabiliser les autorisations. En conséquence, les auteurs ont distingué 2 types d'éléments contextuels : (i) *des éléments de durée longue* – chargés de l'attribution des rôles et (ii) *des éléments de*

durée courte – chargés de l'attribution des permissions. Ces éléments peuvent être reliés soit à l'utilisateur soit à l'environnement.

Une autre extension a été proposée pour fournir un modèle RBAC adapté aux besoins des systèmes pervasifs par (Kulkarni *et al*., 2008). Ce modèle a séparé la gestion du contexte du contrôle d'accès pour faciliter la prise de décision dans le cas où une autorisation est liée à plusieurs contraintes contextuelles. Les auteurs fournissent un service dédié à la gestion des ressources pervasives. A partir de l'ensemble des contraintes contextuelles, une décision d'accès à une ressource est prise.

Après avoir réalisé cette étude sur les différentes extensions qui visent à rendre le modèle RBAC plus adapté aux contraintes du temps réel des systèmes pervasifs, nous constatons qu'elles ne prennent pas en compte la situation dans laquelle se trouve l'utilisateur lors de la consultation du système (cas d'urgence, incendie, etc.).

3.3. *Le Standard XACML*

Le modèle RBAC a résolu le problème d'administration des ressources de données distribuées en les gérant d'une manière centralisée. Mais avec l'évolution des architectures orientées-service et les services web, le problème de la gestion d'accès devient plus compliqué car les politiques de contrôle d'accès sont devenues également distribuées et parfois gérées par différents administrateurs. Pour résoudre ce problème, le standard XACML a été introduit par (OASIS, 2003).

XACML (*eXtensible Access Control Markup Language*) est un standard basé sur XML qui décrit des politiques de contrôle d'accès permettant de définir les privilèges des utilisateurs sur les ressources informatiques d'un système. Ce standard permet d'authentifier et de sécuriser les systèmes en prenant en compte différents éléments reliés au contexte de l'utilisateur.

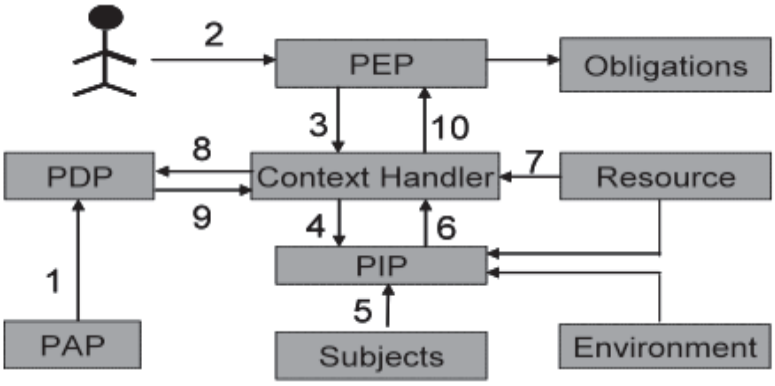

Figure 2. *Modèle simplifié de la gestion d'accès à un flot de données en XACML*

La spécification XACML fournit une architecture qui décrit le processus de gestion d'accès lors d'une demande d'accès (cf. figure 2). Quand un utilisateur demande d'accéder une ressource, un Point d'imposition de politique de sécurité PEP (*Policy Enforcement Point*) interfère pour vérifier si l'accès est autorisé ou non. Afin de vérifier la validité d'une demande d'accès, le système doit vérifier s'il existe une politique de sécurité qui correspond à cette demande. Cette vérification est réalisé par le PEP qui crée une requête contenant les attributs de l'utilisateur et les envoie au Point de décision de politique de sécurité PDP (*Policy Decision Point*) qui prend la décision en consultant la liste des politiques d'accès qui sont localisées dans les Magasins de politiques d'accès PAPs (*Policy Administration Points*). En utilisant la politique de sécurité pertinente (choisi par le PDP), le PEP retourne la réponse appropriée au client et assure que cette décision est respectée et que le client ne peut accéder qu'aux ressources autorisées.

XACML est considéré comme un standard efficace de part sa capacité à gérer les droits d'accès d'une manière distribuée en prenant en compte le contexte de l'utilisateur ou le service. Un profil XACML RBAC a été introduit par (OASIS, 2004), en favorisant ainsi la portabilité du standard vers des services à grande échelle.

Dans la section suivante, nous allons expliquer le fonctionnement de prise de décision dans XACML. Nous montrerons qu'après avoir effectué une analyse d'efficacité, nous avons trouvé que ce standard n'adapte pas ses réponses par rapport aux besoins des utilisateurs qui se trouvent par fois dans des scénarios critiques. Pour répondre à ce manque, nous proposons dans la suite un modèle adaptatif qui offre des solutions alternatives permettant de répondre aux demandes d'accès non autorisées en proposant des éléments similaires.

4. Problématique

Comme nous l'avons cité, le standard XACML vise à faciliter la prise de décision d'accès dans un environnement distribué. En analysant cette prise de décision d'un point de vue de système, nous pouvons constater que XACML est dédié pour assurer un accès strictement sécurisé aux ressources d'information. Par contre, si l'on se place du point de vue de l'utilisateur, XACML ne fournit pas un service adapté et produit des réponses plutôt rigides (Al Kukhun *et al*., 2007).

En figure 3, nous présentons une version simplifiée de la traduction d'une demande d'accès sous forme d'une requête XACML où un sujet (ici une infirmière à l'EMG de l'hôpital de Toulouse) demande d'accéder une ressource (le dossier médical d'un patient) dans un certain contexte (à une certaine heure : 15h28, à partir d'une localisation précise : la maison du patient).

Suivant le fonctionnement du standard (illustré en figure 2), cette requête sera traitée par le système qui la comparera avec les politiques d'accès qu'il possède et lui fournira plusieurs choix des réponses: (i) il lui permet d'accéder au dossier en

question (ii) il rejette sa demande d'accès ou (iii) il renvoie un message d'erreur syntaxique qui signale le manque d'opérateur, de condition, etc.

Ce mécanisme de prise de décision assure l'intégrité du système mais en analysant le cas où le système renvoie une réponse négative, nous constatons qu'il ne peut pas répondre aux besoins des utilisateurs qui se trouvent parfois dans des situations critiques et qui ont besoin de savoir s'il existe d'autres ressources similaires ou alternatives auxquelles ils peuvent accéder.

Dans notre exemple, la loi médicale précise les conditions d'accès à un dossier médical qui est, en principe, seulement accessible dans l'enceinte de l'hôpital et pendant les horaires du travail. Cette loi est traduite sous forme d'une politique XACML (cf. figure 7) qui sera conservée dans le PAP de l'hôpital.

```
<Request>
  <Subject>
        <Attribute
        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
                    <AttributeValue> Sonia Laure </AttributeValue>
        </Attribute>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-Role"
        DataType="http://www.w3.org/2001/XMLSchema#string">
                    <AttributeValue> Nurse </AttributeValue>
        <Attribute
        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-loc"
        DataType="http://www.w3.org/2001/XMLSchema#string">
                   <AttributeValue> Patient House </AttributeValue>
        </Attribute>
        <Attribute
        AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-time"
        DataType="http://www.w3.org/2001/XMLSchema#time">
        <AttributeValue> 15.28.49.495000000+02:00 </AttributeValue>
        </Attribute>
  </Subject>
  <Resource>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            DataType="http://www.w3.org/2001/XMLSchema#string">
                    <AttributeValue> Medical Report </AttributeValue>
        </Attribute>
  </Resource>
  <Action>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
                    <AttributeValue> read </AttributeValue>
         </Attribute>
  </Action>
  <Environment/>
</Request>
```

Figure 3. *Une version simplifiée d'une requête XACML*

Dans cette situation, la demande de consultation sera rejetée à cause du contexte courant de l'utilisateur (maison du patient) qui est considéré comme une menace de sécurité du système. Dans de tels contextes, il serait intéressant que le système puisse autoriser à cet utilisateur l'accès à d'autres ressources moins sensibles et qui contiennent des informations pertinentes pour la consultation telles que les fichiers contenant les analyses et les radiologies du patient.

Dans ce papier, nous présentons ce point de vue adaptatif en montrant qu'une consultation dans le cadre d'une visite d'une EMG exige un accès « intelligent et proactif» où le système cherchera (dans le cas d'une demande rejetée) s'il existe des ressources autorisées qui sont pertinentes et alternatives dans ce contexte. Pour réaliser une telle recherche, nous présentons une extension du modèle RBAC qui s'adapte aux besoins des utilisateurs et à la nature du service attendu par le système.

5. Contribution

5.1. *PS-RBAC : un modèle RBAC pervasif et sensible à la situation*

Le modèle PS-RBAC[2] « Pervasive Situation-aware RBAC » que nous proposons est une extension du modèle RBAC. L'objectif derrière ce modèle est de permettre la construction d'autorisations flexibles qui s'adaptent au changement de droits d'accès causé par la mobilité de l'utilisateur. Notre modèle prend en compte les attributs contextuels de l'utilisateur et la situation dans laquelle il consulte le système afin de lui fournir des propositions d'accès à des ressources alternatives.

Comme nous le montrons en figure 4, nous adoptons le principe d'attribution des rôles du modèle RBAC. Puis, nous étendons les permissions attribuées à ces rôles pour acquérir deux types des permissions : (i) des permissions prédéfinies par les politiques existantes dans le système, (ii) des permissions adaptatives définies en temps réel par le processus adaptatif que nous avons défini.

Afin de réaliser cette adaptation et de construire ces nouvelles permissions, le mécanisme d'attribution des permissions dans le modèle PS-RBAC proposé s'appuie sur un composant qui étudie le contexte de l'utilisateur puis la sensibilité de sa situation qui, en fonction du résultat, réalisera un processus de recherche vers des ressources similaires autorisées et les proposeront comme des solutions alternatives.

Dans ce qui suit, nous présentons le processus adaptatif que nous proposons en intégrant des composants supplémentaires dans le modèle RBAC. Nous allons définissons formellement ce nouveau modèle afin d'expliquer les relations entre les objets.

2. Travail réalisé lors d'un stage de collaboration avec Pr. Elisa Bertino et Pr Yuqing Sun, Purdue University.

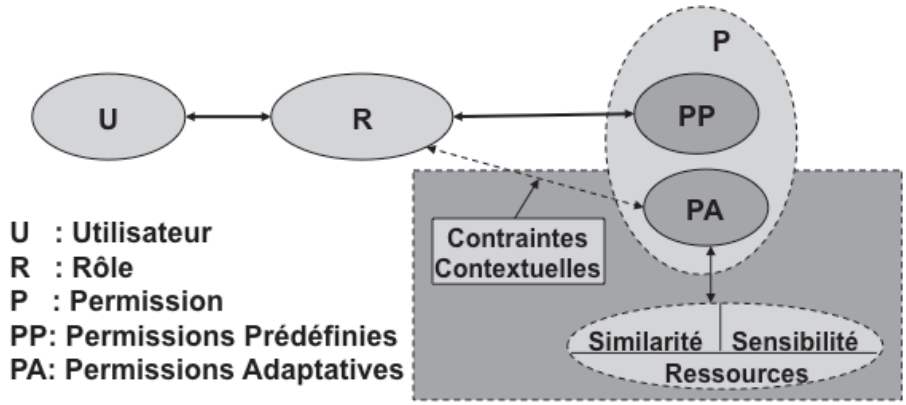

Figure 4. *Le Modèle PS-RBAC « Pervasive Situation-Aware RBAC »*

L'Utilisateur U dans notre modèle est une entité qui interagit pour accéder aux ressources d'un système. Un utilisateur peut être une personne, un processus informatique, un service web, une machine, etc.

En principe, au moment de l'accès au système, l'utilisateur s'identifie pour ouvrir une session dans laquelle il lui sera attribué un ou plusieurs rôles qui reflètent les différentes tâches et missions qu'ils effectuent dans l'entreprise. Cette attribution prend en compte les attributs de l'utilisateur tels que son identité, profil, etc.

Etant un modèle qui reflète la mobilité et la variété du contexte, l'utilisateur sera aussi caractérisé par des attributs contextuels dynamiques (localisation, réseaux, heure, etc.). Ce dynamisme influence les permissions qui lui seront données.

Un Rôle R reflète le positionnement d'un utilisateur dans la hiérarchie organisationnelle de l'entreprise. Le regroupement de plusieurs personnes (effectuant une tâche similaire) dans un rôle a pour objectif de faciliter la distribution et la mise-à-jour des droits d'accès aux ressources de données.

Le rôle dans notre modèle est placé au cœur du système : il fait la liaison entre les utilisateurs et les permissions et assure une gestion décentralisée des droits d'accès (qui est souvent réalisée par une troisième partie (e.g. un administrateur).

L'attribution des rôles aux utilisateurs UA est représentée par une relation « many-to-many » où un utilisateur peut se voir attribuer plusieurs rôles et un rôle peut être relié à plusieurs utilisateurs en même temps.

$$\mathbf{AU} \subseteq \mathbf{Utilisateurs} \times \mathbf{Rôles}$$

Par exemple, dans le cas d'un système de santé, un utilisateur peut occuper plusieurs rôles en même temps : il peut être un patient (sous traitement) et un médecin traitant en même temps ou un médecin et un chef de service, etc.

Une Permission P est une autorisation qui donne à l'utilisateur le droit d'accéder aux ressources du système, cette autorisation passe à travers le rôle. Notre modèle génère deux sortes de permission selon la situation et le contexte de consultation : des permissions prédéfinies et des permissions adaptatives.

$$\mathbf{P = \{PP \cup PA\}.}$$

Les Permissions Prédéfinies PP sont des autorisations définies explicitement et en avance par les gestionnaires du système. Dans le cas d'un système distribué qui utilise XACML pour la gestion des droits d'accès, ces permissions sont sauvegardées dans des politiques et distribuées dans plusieurs PAPs.

L'attribution des Permissions Prédéfinies APP est représentée par une relation « many-to-many » où un rôle peut être attribué à plusieurs permissions et une permission peut être associée à plusieurs rôles.

$$\mathbf{APP \subseteq Roles \times PP}$$

Les Permissions Adaptatives PA sont des autorisations alternatives proposées d'une manière *ad hoc* par notre modèle. La génération de telles permissions a lieu dans le cas d'un rejet d'une demande d'accès établie dans une ***situation*** importante (consultation extra hospitalière, urgence, etc.).

Ces autorisations sont liées au contexte courant de l'utilisateur présenté par un ensemble de ***Contraintes Contextuelles CC*** qui ont une nature dynamique dans les environnements pervasifs. Dans le modèle proposé, il y a détection de ces contraintes, identification de l'ensemble des ressources accessibles dans ce contexte et recherche de ressources similaires qui peuvent répondre à la demande de l'utilisateur.

Pour obtenir ces ressources similaires, un ***gestionnaire de similarité*** est chargé de mesurer la similarité entre les ressources non autorisées et l'ensemble des ressources afin de proposer une ressource pertinente. Cette similarité peut être liée au contenu d'un document (contenu textuel), à sa structure (document XML) ou à différentes relations spatio-temporelles (dans le cas d'une recherche vers un objet localisé à proximité).

L'attribution des Permissions Adaptatives APA forme une relation « many-to-many » entre les rôles et les permissions qui sont fortement influencés par le contexte courant présenté par les contraintes contextuelles.

$$\mathbf{APA \subseteq Rôles \times PA \cup CC}$$

Dans ce qui suit, nous allons montrer l'architecture de notre système et comment nous allons appliquer ce modèle et l'intégrer dans l'architecture de XACML pour assurer une prise de décision adaptative.

5.2. *Un système adaptatif basé sur la réécriture des requêtes XACML*

Nos travaux appliquent une procédure adaptative qui prend en compte le rôle de l'utilisateur, son contexte et sa situation afin de lui fournir des moyens alternatifs d'accéder au système dans le cas où il effectue une demande non autorisée (due au changement du contexte de l'utilisateur ou à la variété de contenu des systèmes interrogés). Pour réaliser cet objectif, nous appliquons un mécanisme de réécriture des requêtes de l'utilisateur (Al Kukhun *et al.*, 2007) en utilisant la recherche de degré de similarité entre un élément non autorisé (demandé par l'utilisateur) et des documents ou des services existants dans le système et autorisés à l'utilisateur.

Comme présenté en figure 2, l'architecture que nous proposons vise à étendre le modèle de prise de décision dans XACML en ajoutant une couche adaptative réalisée par un mécanisme de réécriture de la requête de l'utilisateur dans le cas où elle est refusée par le PDP (Al Kukhun *et al.*, 2008a et b).

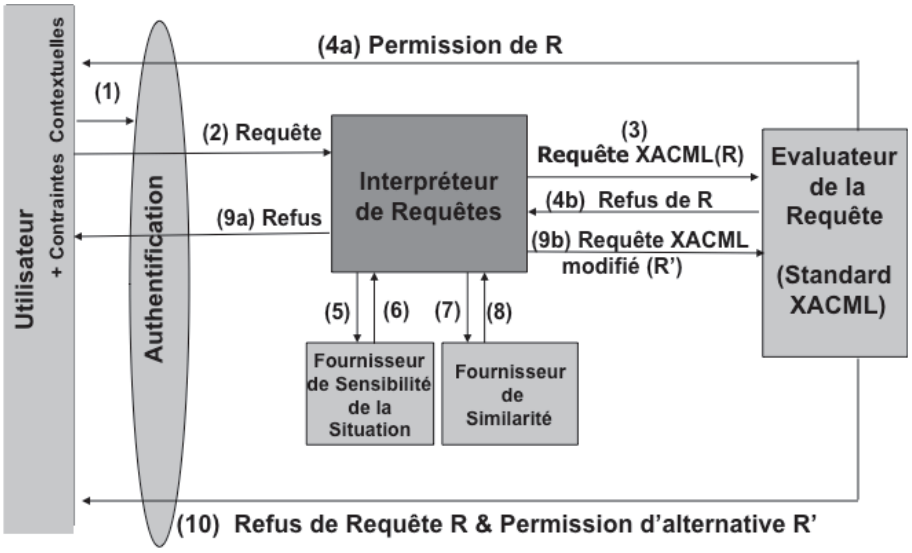

Figure 5. *Le modèle adaptatif de réécriture des requêtes XACML*

Le système récupère les contraintes contextuelles de l'utilisateur et les reçoit avec une étape d'authentification **(1)**. Puis, quand l'utilisateur lance sa requête, le système la communiquera au générateur de requête **(2)** qui la traduira vers une requête de format XACML **R.** Celui-ci prend en compte cette demande et la combine avec les contraintes contextuelles puis l'envoie vers l'Evaluateur de requêtes **(3)** qui joue le rôle d'un PDP et suit le processus normal de XACML.

Selon les droits d'accès de l'utilisateur (précisés par les politiques d'accès sauvegardées dans les PAPs – voir le schéma XACML en section 3.3), le système

répond à cette demande soit en permettant l'utilisateur d'accéder à la ressource demandée **(4a)**, ou en lui répondant avec un refus d'accès **(4b)**. C'est dans ce dernier cas que notre mécanisme adaptatif intervient pour étudier la situation dans laquelle l'utilisateur a consulté le système. Cette situation est définie par le Fournisseur de Sensibilité de la Situation **(5 et 6)** qui autorise la régénération de la requête **R'** dans le cas d'une situation d'urgence par exemple.

Cette régénération ou réécriture de requêtes est réalisée grâce au Fournisseur de similarité **(7 et 8)** qui prend les contraintes contextuelles de l'utilisateur comme un point de départ pour la recherche des documents ou des services autorisés et qui ont des similarités de contenu ou de fonctionnement avec la ressource initialement demandée par l'utilisateur et qui été jugé comme non autorisée.

Cette étape est destinée à restituer à l'interpréteur de requêtes des ressources alternatives similaires. Dans le cas où le système n'aura pas des propositions, l'interpréteur des requêtes va envoyer à l'utilisateur un refus d'accès **(9a)** – cas classique. En revanche, dans le cas où le système trouve des ressources similaires, le Générateur de la Requête réécrit la requête initiale en remplaçant la ressource demandée par la nouvelle ressource jugée similaire (par notre Fournisseur de Similarité) puis l'envoie vers l'Evaluateur de Requêtes qui réévalue la nouvelle requête **R' (9b*)** et répond l'utilisateur avec un refus d'accès pour sa demande initiale et une permission pour accéder aux ressources alternatives **(10)**.

6. Application au service des équipes mobiles gériatriques (EMG)

Dans cette section, nous soulignons l'importance de l'accessibilité au sein de systèmes de santé particulièrement dans les cas d'urgences et dans des scénarii critiques temps réel. Dès lors, un modèle adaptatif nous apparaît incontournable.

6.1. *La Mission des EMG*

Les difficultés de prise en charge des personnes âgées au sein de l'hôpital, aussi bien dans les services d'accueil des urgences (SAU) que dans les services de spécialités, ont conduit les gériatres à proposer des structures mobiles d'évaluation, de conseils et de soins.

En réponse à la circulaire ministérielle du 18 mars 2002, les équipes mobiles de gériatrie (EMG) se sont mises en place, tout en s'appuyant sur des unités gériatriques complètes et structurées (médecin spécialiste, infirmière, aide-soignante et secrétaire). Leurs missions s'articulent autour de l'évaluation médico-psycho-sociale globale. Elles s'attachent à proposer des recommandations et à anticiper l'orientation du patient dans son parcours de soin. Les EMG s'adressent en priorité à la personne âgée fragile pour laquelle le bénéfice attendu est le plus sensible.

A partir de différentes visites et rencontres avec les membres des EMG dans la région Midi-Pyrénées, nous avons trouvé différentes pistes de recherche autour d'un système d'information de santé qui a un rôle très important dans la réussite de la mission de l'équipe.

6.2. *Scénario actuel d'une intervention d'une EMG*

Une intervention d'une EMG prend lieu après la réception d'un fax d'un « bon de demande » adressé par un service. En analysant les types de demande d'une mission, nous distinguons 2 modes d'activité :

1. une activité *intra-hospitalière*, où l'EMG se mobilise pour effectuer une intervention dans un autre service dans le même hôpital ;

2. une activité *extra-hospitalière* où l'EMG se déplace vers un service hors l'hôpital tel que le centre de soins de suite et de réadaptation SSR, l'établissement d'hébergement pour les personnes âgées dépendantes EHPAD, le centre local d'information et de coordination CLICS, etc.).

L'activité demandée vise normalement à traiter un patient et pour cela, l'équipe – composée d'une secrétaire, d'une infirmière, d'une aide-soignante et d'un médecin spécialiste – aura besoin d'accéder aux différentes ressources médicales puis, de construire un dossier d'événement gériatrique.

En considérant la caractéristiques mobile de l'équipe, nous soulignons l'importance de pouvoir réaliser ces missions en accédant aux ressources d'information depuis n'importe quel service/localisation, à n'importe quel moment et en utilisant n'importe quelle machine et système d'information.

6.3. *Les challenges d'accès et de sécurité dans le processus de recueil et de passage d'information au sein de l'équipe*

Dans cette section, nous soulignons l'importance de fournir un système d'information efficace au service de l'EMG lors d'une consultation.

La nature d'une consultation exige la création du dossier patient d'une manière évolutive où chaque membre de l'équipe peut récupérer et consulter les données du patient à partir du système d'information (selon ses droits d'accès) et ensuite, peut insérer ses remarques et d'autres données au fur et à mesure.

Dans les systèmes actuels, le passage d'information lors de la fin d'une tâche est réalisé directement par chaque membre soit en utilisant des formulaires à moitié remplis à la main (dans le cas d'une intervention *extra-hospitalière*) ou avec des formulaires imprimés à partir du système informatique (dans le cas d'une intervention *intra-hospitalière*).

Pour réaliser une meilleure consultation et un passage d'information, le dossier d'événement gériatrique doit être rempli de manière coopérative et interactive. Le spécialiste devra pouvoir consulter la situation du patient et la mettre à jour selon plusieurs techniques, en accédant aux flux des données générés en temps réel et extraits à partir des machines dédiées pour la surveillance du patient.

C'est pour cette raison, que nous soulignons l'importance de fournir un système pervasif qui améliorera la consultation des données du patient pour une EGM et assurera le passage d'information de manière collaborative et interactive.

Grâce à cette évolution des systèmes d'information de santé vers des systèmes pervasifs, la qualité de service sera assurée par une EMG qui pourra traiter le patient depuis n'importe où, n'importe comment et à n'importe quel moment.

Le fait d'avoir un système pervasif résoudra la complexité d'accès au dossier du patient et le traitement de données dans un cas de consultation mobile. L'interaction au sein de l'EMG sera plus efficace et fournira un échange transparent avec les ressources de données.

6.4. *L'implantation d'un système de contrôle d'accès adaptatif pour les EMG*

Dans cette section, nous soulignons l'importance de fournir un système d'information efficace au service de l'EMG lors d'un processus de consultation.

Afin de faciliter l'adoption du standard XACML, nous avons fourni un prototype dédié aux administrateurs chargés de la gestion de contrôle d'accès au sein des EMG, cette gestion passe par la création des politiques de contrôle d'accès en forme des politiques XACML, cf. figure 6.

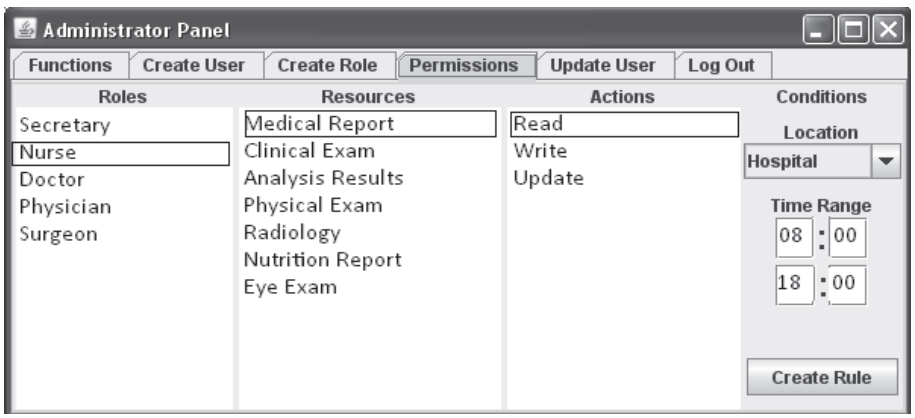

Figure 6. *Prototype chargé de la création des politiques d'accès XACML*

Comme nous le montrons, un utilisateur est représenté par un rôle auquel on peut attribuer différentes permissions pour accéder à différentes ressources selon certaines contraintes contextuelles (ici : localisation et durée). Le résultat d'une telle opération sera la génération d'un fichier XML contenant la politique d'accès, voir figure 7.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy PolicyId="GeneratedPolicy" RuleCombiningAlgId="urn:oasis:
names:tc:xacml:1.0:rule-combining-algorithm:ordered-permit-overrides">
 <Target>
  <Subjects>    <AnySubject/>    </Subjects>
  <Resources>  <AnyResource/>  </Resources>
  <Actions>      <AnyAction/>    </Actions>
 </Target>
 <Rule RuleId="urn:oasis:names:tc:xacml:1.0:hospital-system:rule" Effect="Permit">
  <Target>
   <Subjects>
    <Subject>
          <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-
          Role" DataType="http://www.w3.org/2001/XMLSchema#string">
          <AttributeValue> Nurse </AttributeValue></Attribute>
    </Subject>
   </Subjects>
   <Resources>      <Resource>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
          DataType="http://www.w3.org/2001/XMLSchema#string">
              <AttributeValue>Medical_Report.xml</AttributeValue> </Attribute>
    </Resource>    </Resources>
   <Actions>      <Action>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
      DataType="http://www.w3.org/2001/XMLSchema#string">
            <AttributeValue>Read</AttributeValue> </Attribute>
    </Action>    </Actions>
  </Target>
  <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-
equal">
    <Attribute> <AttributeValue>08.00.00.495000000+02:00 </AttributeValue>
   </Attribute></Apply>
 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal">
    <Attribute><AttributeValue>18.00.00.495000000+02:00 </AttributeValue>
    </Attribute>    </Apply>
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Attribute  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-loc"
      DataType="http://www.w3.org/2001/XMLSchema#string">
          <AttributeValue>Hospital</AttributeValue> </Attribute>
   </Apply>
  </Condition>
 </Rule>
 <Rule RuleId="FinalRule" Effect="Deny"/>
</Policy>
```

Figure 7. *Exemple d'une politique XACML réalisée avec notre prototype*

Le prototype est dédié également aux utilisateurs de système (médecins, infirmières, etc.) qui lancent des requêtes à partir de différentes contextes. Un exemple d'une requête XACML a été présenté en figure 3, cette requête sera réalisée par une interface spécialisée, voir figure 8. Cette interface interrogera la base de données des politiques XACML et dans le cas d'un refus d'accès dans le cas d'une situation critique, le Fournisseur de Similarité cherchera s'il y en a des ressources similaires à proposer à l'utilisateur et lui permettre d'y accéder. Le fait que notre système fonctionnera dans un environnement pervasif pourra enrichir le processus de détection des contraintes contextuelles de l'utilisateur qui sera réalisé implicitement par notre système (qui pourra extraire le numéro du patient à partir de la puce RFID de sa carte d'assurance ou préciser sa localisation en faisant la liaison entre l'adresse actuelle détectée par un GPS intégré dans la machine de l'utilisateur et l'adresse mentionné dans le dossier du patient ou l'adresse de l'hôpital, etc.). Toutefois, en cas du manque des informations, ces contraintes peuvent être aussi précisés explicitement par l'utilisateur lors d'une interrogation.

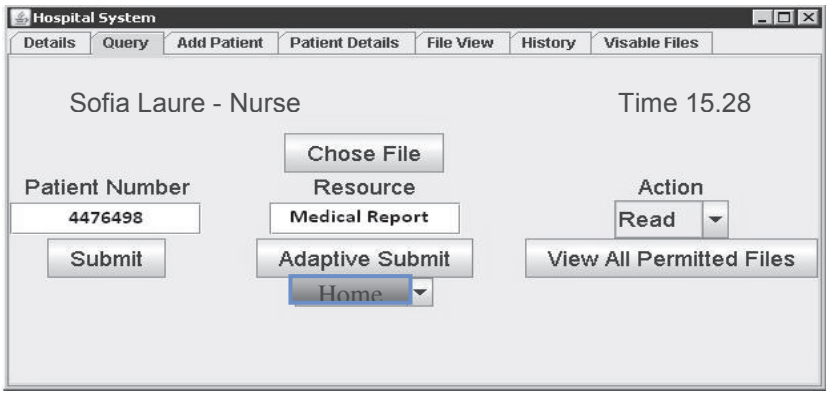

Figure 8. *Exemple de prototype dédié au lancement des requêtes d'accès*

7. Conclusion

L'accessibilité aux ressources d'information dans les systèmes de santé est un aspect très important en particulier dans une consultation en temps réel ou dans des situations critiques. De plus, le contrôle de cet accès forme une brique de base essentielle pour gérer cette accessibilité. Dans cet article, nous avons présenté un modèle adaptatif qui vise à trouver des solutions alternatives pour les utilisateurs qui demandent d'accéder à des ressources non autorisées pendant leur déplacement dans un environnement pervasif. C'est le cas d'une l'équipe gériatrique mobile. Pour réaliser cette flexibilité, nous avons utilisé la réécriture des requêtes XACML avec une mesure de sensibilité de la situation de requêtage et de la similarité entre les ressources de données. Notre objectif est de fournir une meilleure qualité de service et une transparence d'accès sans menacer la sécurité ou l'intégrité du système.

8. Bibliographie

Al Kukhun D., Sèdes F., « La Réécriture de Requêtes XACML : Un mécanisme pour assurer une sécurité adaptable pour les systèmes de gestion de données pervasifs », *Atelier GEDSIP (INFORSID07)*, juillet 2007, France, p. 42-61.

Al Kukhun D., Sèdes F., "Adaptive Solutions for Access Control within Pervasive Healthcare Systems", *ICOST 2008*, Ames, IA, USA, p. 42-53.

Arthus I., Montalan M.A., Vincent B., « Quels outils pour piloter la performance d'une Equipe Mobile de Gériatrie », *Journal d'Economie Médicale*, vol. 27. n° 1-2. 2009, p. 43-59.

Bertino E., Bonatti P., Ferrari E., "TRBAC: A temporal role-based access control model", *ACM Trans. Inf. Syst. Secur*, vol. 4, n° 3, 2001, p. 191-233.

Bertino E., Catania B., Damiani M.L., Perlasca P., "GEO-RBAC: a spatially aware RBAC", *Proc. of the Tenth ACM Symposium on Access Control Models and Technologies (SACMAT 2005)*, Stockholm, Sweden, p. 29-37.

Chae S.H., Kim W., Kim D.K., "uT-RBAC : Ubiquitous role-based access control model", *IEICE transactions*, 2006, vol. 89, n° 1, p. 238-239.

Déclaration d'Helsinki de l'association médicale en 1964. http://www.genethique. org/ carrefour_infos/textes_officiels/titres_textes/declaration_helsinki_2000.htm.

Dey A.K., "Understanding and Using Context", *Personal and Ubiquitous Computing Journal*, vol. 5, n° 1, 2001, p. 4-7.

Duan Y. and Canny J., "Protecting User Data in UbiComp: Towards trustworthy environments", *Privacy Enhancing Technologies (PET 2004)*, Selected Papers, p. 167.

Emami S. S., Amini M., and Zokaei S., "A Context-Aware Access Control Model for Pervasive Computing Environments", *Proceedings of the the 2007 international Conference on intelligent Pervasive Computing* (October 11-13, 2007), IPC. IEEE Computer Society, Washington, DC, 51-56.

Ferraiolo D. and Kuhn D., "Role Based Access Control", *15th National Computer Security* Conf. Oct 13-16, 1992, p. 554-563.

Hansen F., Oleshchuk V., "SRBAC: A Spatial Role-Based Access Control model for mobile systems", *Proceedings of the 7th Nordic Workshop on Secure IT Systems*, 2003, Gjvik, Norway.

Health Insurance Portability and accountability act of 1996, http://aspe. hhs. Gov / admnsimp /pl104191.htm#261

HL7, Health Level Seven, accredited by ANSI in 1994. http://www.hl7.org/

Hong J., Suh E., Kim J., and Kim S., "Context-aware system for proactive personalized service based on context history", *Expert Syst. Appl,* vol. 36, n° 4, May 2009, p. 7448-7457.

Kim Y., Moon C., Jeong, D., Lee J., Song C., Baik D., "Context-Aware Access Control Mechanism for Ubiquitous Applications", *AWIC* 2005, p. 236-242.

Kuhn D., “Mutual Exclusion of Roles as a Means of Implementing Separation of Duty in Role-Based Access Control Systems”, *2nd ACM Workshop Role-Based Access Control*, 1997, p. 23-30.

Kulkarni D., Tripathi A., “Context-aware role-based access control in pervasive computing systems”, *SACMAT* 2008, p. 113-122.

Lim T., Shin S., “Intelligent Access Control Mechanism for Ubiquitous Applications”, *ICIS* 2007, 11-13 July 2007, p. 955-960.

Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=MESX0100092L

OASIS, *A brief Introduction to XACML*, 14 mars 2003, http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html

OASIS, XACML Profile for Role Based Access Control (RBAC) Committee Draft 01, 13 February 2004 http://docs.oasis-open.org/xacml/cd-xacml-rbac-profile-01.pdf

Park I., Kim W. and Park Y., “A Ubiquitous Streaming Framework for Multimedia Broadcasting Service with QoS based mobility Support”, *LNCS 3090* in Springer-Verlag (SCI-E), June 2004, p. 65-74.

Paterno F., “Model-based tools for pervasive usability”, *Interacting with Computers*, vol. 17, n° 3, 2005, p. 291-315.

Pirzada A. A. and McDonald C., “Secure Pervasive Computing without a Trusted Third Party”, *Proceedings of the the IEEE/ACS international Conference on Pervasive Services* (July 19 - 23, 2004). ICPS. IEEE Computer Society, Washington, DC, 240-240.

Privacy Act of 1974. http://www.house.gov/matheson/the_privacy_act_of_1974.html

Sandhu R., “Role Hierarchies and Constraints for Lattice-Based Access Controls”, *ESORICS* 1996, p. 65-79.

Turunen M., Hurtig T., Hakulinen J., Virtanen A., and Koskinen S., “Mobile Speech-based and Multimodal Public Transport Information Services”, *Proceedings of MobileHCI 2006 Workshop on Speech in Mobile and Pervasive Environments*, http://www.igd.fhg.de/igd-a1/RSPSI/papers/RSPSI-Turunen.pdf

Tripathi A., Ahmed T., Kulkarni D., Kumar R., Kashiramka K., “Context-Based Secure Resource Access in Pervasive Computing Environments”, *PerCom Workshops* 2004, p. 159-163.

Want R., Borriello G., Pering T., and Farkas K.I., “Disappearing Hardware”, *IEEE Pervasive Computing*, 1, 1, Jan. 2002, p. 36-47.

Weiser M., “The computer for the 21st century”, *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 3, n° 3, July 1999, p. 3 - 11.Kolski C., *Interfaces homme-machine*, Paris, Editions Hermès, 1997.

Yau S., Karim F., “Context-Sensitive Middleware for Real-Time Software in Ubiquitous Computing Environments”, *ISORC*, 2001, p. 163-170.