UNE METHODE ADAPTATIVE POUR ASSURER L'ACCESSIBILITÉ AUX SYSTÈMES D'INFORMATIONS PERVASIFS DE L'ENTREPRISE

Dana Al KUKHUN , Florence SEDES
kukhun@irit.fr, sedes@irit.fr
IRIT, Université de Toulouse III, 118 Rout de Narbonne, 31062 Toulouse, France

Mots clefs :
Accessibilité, sécurité, contrôle d'accès, systèmes de gestion de données, Systèmes pervasifs, adaptation, XACML.
Keywords:
Accessibility, security, Access control, Management Information Systems, Pervasive systems, adaptation, XACML.
Palabras clave:
Accesibilidad, seguridad, control de acceso, Sistemas de Información de Gestión, omnipresentes sistemas, la adaptación, XACML.

Résumé

De plus en plus, la transparence devient un élément fortement requis pour assurer une meilleure accessibilité aux ressources de données au niveau de l'entreprise. Cette accessibilité est avantageuse pour les dirigeants puisqu'elle leur permet d'interroger différentes sources d'information et de prendre leurs décisions en se basant sur la situation réelle de l'entreprise. Grâce au développement technologique et l'intégration des nouvelles technologies au sein de l'entreprise, la connectivité a augmenté l'accessibilité aux ressources de données et a permis une grande liberté d'interaction depuis n'importe où, n'importe comment et à n'importe quel moment et c'est là que les systèmes deviennent pervasifs. Mais en étudiant cette connectivité, on constate qu'elle peut menacer la sécurité et la confidentialité des ressources de données et c'est là que le contrôle d'accès devient indispensable.
Dans cet article, nous analysons la gestion d'accès aux données distribuées dans une entreprise où le système d'information peut interroger des bases de données semi-structurées représentées en XML. Nous présentons le standard XACML qui est destiné à effectuer la gestion des droits d'accès en créant des politiques d'accès au format XML. Ensuite, nous montrons quelques challenges qui peuvent empêcher un décideur de prendre une décision dans un contexte critique à cause de la rigidité du système et la manque d'adaptation. Finalement, nous présentons une solution adaptative qui vise à trouver des ressources alternatives accessibles.

1 Introduction

La révolution des systèmes d'information pervasifs est liée au développement de la télécommunication, de la connectivité, des matériels et des logiciels. Ces systèmes visent à créer des environnements transparents et interopérables afin d'assurer un meilleur partage d'information entre différents systèmes d'informations et sous-composants hétérogènes contenant des données semi-structurées représentées en XML.

Les systèmes pervasifs doivent fournir une accessibilité transparente aux ressources de données, depuis n'importe où et n'importe comment et à n'importe quel moment. Mais la transparence de tels systèmes les rend vulnérables aux menaces et aux attaques de sécurité. Alors, on se trouve dans une challenge est de trouver un équilibre entre la discrétion de données et l'accessibilité transparente aux ressources pervasives existantes dans des environnements ouverts.

Avec l'expansion des capacités d'Internet et de télécommunications, XML (eXtensible Markup Language) est devenu une norme pour la représentation, le stockage et l'échange de données. XML a été choisi grâce à sa capacité à décrire la structure et le contenu des documents dans un format textuel simple. Cette expansion a ouvert les portes pour résoudre les problèmes d'intégration des données hétérogènes et a offert une représentation sémi-structurée pour différents types de données. XPath [17] et XQuery [18] sont des langues d'interrogation présentés pour accéder au contenu d'un document et l'interroger en prenant en compte sa structure.

Malgré tous ces pouvoirs, la sécurité de documents XML reste menacée : une attaque peut être menée sur un document, un sous-arbre d'un document ou le contenu d'un nœud simple. Différents standards ont été introduis pour appliquer des mesures de sécurité et de contrôle d'accès à différents niveaux d'un document XML (nœud, étiquette, données ou structure) afin de le protéger comme XML-Signature [19], XML Encryption [16] et XACML [11].

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

La réécriture de requêtes XML est aussi considérée comme un élément clé pour sécuriser l'accès aux documents semi-structurés où elle intervient dans la modification de la visualisation de la structure arborescente d'un document selon les privilèges d'accès accordés à un utilisateur.

Dans cet article, nous proposons d'utiliser la réécriture de requêtes XACML afin d'adapter la sécurisation d'accès aux ressources d'informations pervasives en répondant aux besoins des utilisateurs.

Nous allons premièrement introduire un état de l'art sur l'accessibilité de ressources d'information réécriture de requêtes XML comme un moyen pour sécuriser le requêtage d'une base de donnée XML. Ensuite, nous allons exposer les caractéristiques de systèmes d'information pervasifs en soulignant l'importance de la sécurité et l'accessibilité aux ressources de données dans ces environnements interopérables en utilisant des standards de sécurité comme XACML. Finalement, nous proposons de réécrire les requêtes XACML pour assurer une sécurité adaptable et flexible au sein des systèmes de gestion de données pervasifs.

2 Les Challenges d'Accès aux Systèmes d'Information Pervasifs

La notion d'ubiquité a été présentée par Weiser [15] qui a prévu le futur des systèmes d'information dans le 21ème siècle, où les éléments de calcul vont disparaître en fonctionnant d'une manière homogène et en transparence totale. Dans les systèmes pervasifs, les utilisateurs communiquent entre eux à n'importe quel moment, n'importe où et avec n'importe quel outil [13].

L'évolution des systèmes d'information pervasifs a introduit les challenges de sécurisation et la gestion des données pervasifs. Ces systèmes doivent, à la fois, permettre aux utilisateurs d'obtenir une grande accessibilité et protéger le système en appliquant des politiques de sécurité invulnérables contre les attaques d'intrus.

2.1 Les challenges de la gestion de données pervasifs

Les Systèmes de Gestion de Données deviennent de plus en plus des Systèmes de Gestion de Données Pervasifs afin d'affronter et de résoudre différents problèmes principaux : le premier concerne l'intégration de volumes importants de documents hétérogènes, et leur représentation dans une norme générique (XML par exemple), dans le but d'assurer une interaction homogène entre leurs différents sous-composants dispersés à différents endroits et qui ont des configurations qui changent progressivement et dynamiquement.
Le deuxième problème concerne le cas où un utilisateur veut accéder et échanger des données existant sur un dispositif d'une autre personne soit dans son système ou dans un système externe. Ce problème est composé de deux challenges ; l'un de la certification d'un utilisateur pour qu'il puisse accéder et avoir différents privilèges d'accès au système selon son rôle et son contexte et l'autre de la compatibilité de systèmes et de composants logiciels qui permettent l'affichage des données multimédia.
Le troisième problème concerne les moyens pour équilibrer les besoins de fournir un accès transparent aux données et la gestion des droits d'accès au système. Tandis que ces systèmes fournissent des services aux différents utilisateurs, ils doivent leur permettre d'accéder directement aux sources de données pour réaliser leurs missions en efficacité totale. Au même temps, différents niveaux d'accès devraient être accordés aux utilisateurs selon leurs rôles en utilisant les politiques de RBAC, où le système sera capable de s'adapter aux besoins de l'utilisateur selon son rôle, chaque rôle ayant ses propres politiques de sécurité qui décrivent ses droits d'accès.

2.2 Les besoins de transparence et l'accessibilité dans l'entreprise

Nous illustrons, en figure 1, l'importance d'avoir une interaction transparente au sein des systèmes d'informations pervasifs qui doivent permettre aux différents utilisateurs d'accéder directement aux ressources d'informations internes, d'accéder indirectement aux ressources d'information externes et finalement de consulter les ressources d'informations stockées dans des dispositifs mobiles en construisant des connexions ad hoc. L'ensemble de ces services doit prendre en compte le rôle de l'utilisateur et ces droits d'accès et éventuellement, va garantir aux utilisateurs une accessibilité transparente aux différentes ressources d'information (le triangle en figure 1).
La sécurité est, comme nous l'avons déjà indiqué, cruciale dans les Systèmes d'Information Pervasifs : grâce à ces systèmes, l'utilisateur pourrait accéder au système depuis n'importe où en utilisant des connexions de fiabilité limitée (ad hoc). Afin d'assurer un système interopérable, les Systèmes de Gestion de Données Pervasifs doivent équilibrer entre l'accessibilité libre aux ressources pour les utilisateurs internes (locaux) et la sécurité - où l'accès est restreint - pour les utilisateurs externes. Un aspect important dans le contrôle d'accès est celui du contexte de l'utilisateur (localisation, connectivité, machine, ambiance entourant), les éléments du contexte peuvent influencer la décision d'accès au système.
Nous envisageons d'effectuer cet équilibre entre le contexte de l'utilisateur, son besoin d'accès au système et son adhésion comme membre direct ou indirect dans l'entreprise. Nous allons utiliser l'adaptation dans les différents axes d'interaction au sein des systèmes pervasifs ; une adaptation automatique effectuée selon le contexte (préférences, rôle, matériel, logiciels, mode de connectivité, etc.) de l'utilisateur peut améliorer la performance et l'efficacité du système.
Nous soulignons l'importance d'utiliser des normes basées sur XML pour assurer l'intégrité du système et une meilleure représentation des données. La naissance de XACML se situe dans cette perspective et vise à assurer un accès sécurisé aux ressources de données hétérogènes et dynamiques.

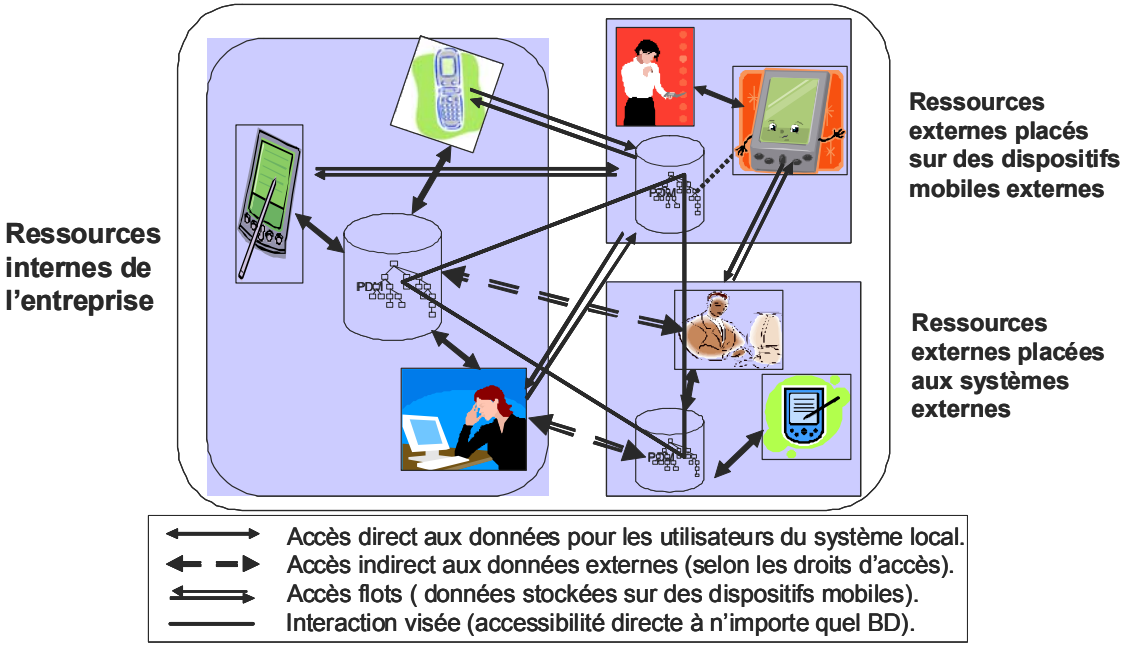

Figure 1 : L'importance d'avoir une accessibilité transparente aux données

3 Comment exprimer le contrôle d'accès en utilisant XACML?

XACML a été proposé par l'OASIS [11] afin d'assurer des transactions sécurisées au sein des Systèmes d'Information Pervasifs. Puisque les Systèmes Pervasifs fournissent des environnements dynamiques qui permettent un échange simple et flexible des données, XACML fournit une politique de sécurité stricte exigée par l'application de différentes politiques de contrôle d'accès pour l'échange des données.

Dans XACML, un utilisateur demande au serveur d'accéder une ressource; un Point d'Imposition de Politique de Sécurité PEP (Policy Enforcement Point) interfère pour vérifier si l'accès est autorisé et sécurisé. Afin d'appliquer une politique de sécurité, le PEP crée des attributs décrivant l'utilisateur (son profil) 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 localisée indépendamment dans un Magasin de Politiques. En utilisant la politique de sécurité choisi par le PDP, le PEP retournera la réponse appropriée au client et assure qu'il n'accèdera qu'aux ressources autorisées (cf figure 2).

En analysant le processus de prise de décision dans XACML, on trouve que le système est bien protégé et répond à la demande (requête) de l'utilisateur dans un manière binaire : soit il lui permet d'accéder une ressource, soit il ne le permet pas. Ce mécanisme assure l'intégrité du système mais ne répond pas aux besoins d'utilisateurs qui aimeront savoir quelles sont les autres ressources qu'ils peuvent accéder et utiliser et pouvoir accéder directement aux autres services disponibles.

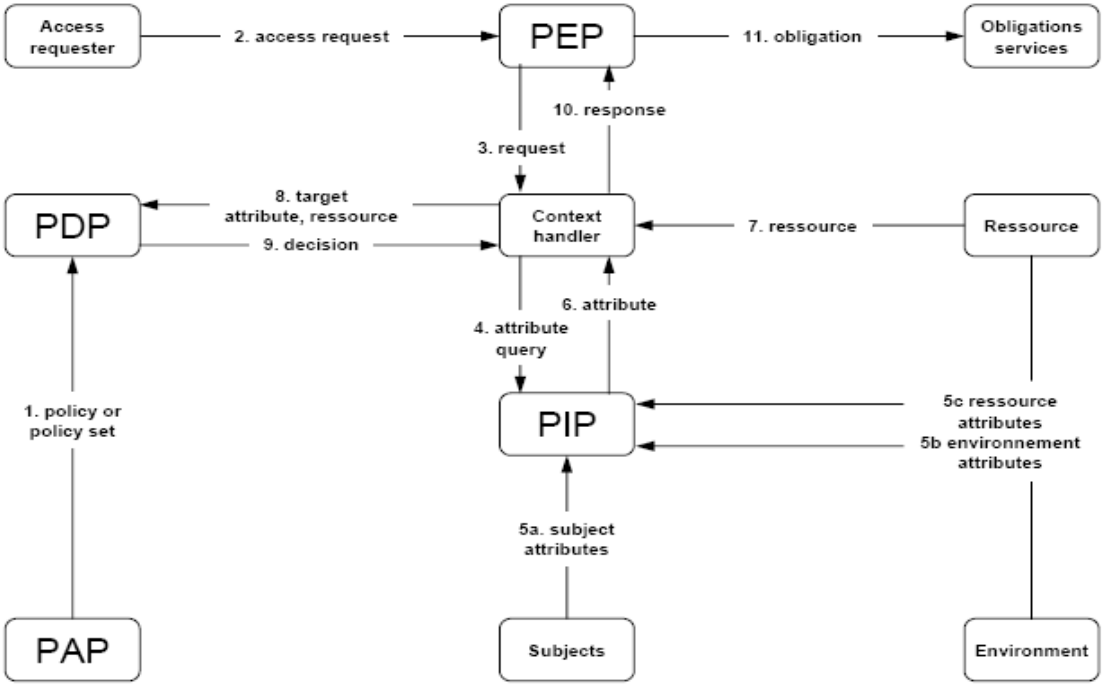

Figure 2 : L'importance d'avoir une accessibilité transparente aux données

En analysant le processus de prise de décision dans XACML, on trouve que le système est bien protégé et répond à la demande (requête) de l'utilisateur dans un manière binaire : soit il lui permet d'accéder une ressource, soit il ne le permet pas. Ce mécanisme assure l'intégrité du système mais ne répond pas aux besoins d'utilisateurs qui aimeront savoir quelles sont les autres ressources qu'ils peuvent accéder et utiliser et pouvoir accéder directement aux autres services disponibles.

4 L'adaptation en utilisant la réécriture des requêtes XACML

XACML assure un accès sécurisé aux ressources d'information d'un point de vue du système [12]. Mais dans une perspective de l'utilisateur, XACML ne fournit pas un service adaptif. Par exemple, si un utilisateur exige l'accès à un document XML qui contient un sous-arbre non autorisé, le système rejettera sa demande au lieu d'afficher une sous partie autorisée de l'arbre. Donc la réponse du système est binaire et ne propose pas à l'utilisateur une liste des chemins accessibles ou potentiels.
Nous proposons d'appliquer la réécriture de requêtes XACML afin de modifier et réécrire la requête de l'utilisateur pour récupérer la plus grande quantité d'information disponible en utilisant des vues virtuelles d'un document. Ce qui permet au système de prendre en compte le rôle de l'utilisateur et de répondre à ses besoins sans menacer la sécurité du système ou son intégrité.
Notre proposition vise à offrir un accès adaptable et sécurisé aux Systèmes d'Information Pervasifs et à augmenter leur efficacité et expressivité en accédant à différentes ressources d'information et dans la recherche d'information.

Cette réécriture va permettre une autorisation d'accès aux ressources dans une granularité plus fine en fonction du rôle de l'utilisateur et de son contexte. En conséquence, la réécriture de requêtes XACML peut fonctionner pour imposer les politiques d'accès aux documents.

5 L'intégration de la réécriture adaptative dans la prise de décision d'accès à l'entreprise

Nous allons prendre l'exemple d'un utilisateur demandant d'accéder à certaines ressources d'information qu'il considère importantes pour la prise d'une décision. Pour accéder au système, l'utilisateur présente ses éléments d'authentification (identifiant, mot de passe / signature électronique / empreinte digitale, etc.), voir le figure 3 (étape 1). Puis, grâce à ces éléments, le système va détecter le rôle de cet utilisateur (en fonction de la hiérarchie de l'entreprise). Selon le rôle attribué, le système va identifier ses droits d'accès aux ressources demandés.

Dans un environnement pervasif, l'attribution d'un droit d'accès peut être affectée par le contexte actuel de l'utilisateur (sa localisation, le type de machine, sa connectivité, etc.). Alors le système va récupérer les attributs contextuels de l'utilisateur et va les passer à l'interpréteur de requêtes pour construire une requête XACML. Nous montrons dans (l'étape 3) que le système transmet cette requête pour qu'elle soit traitée par les composants de prise de décision du standard XACML (PEP, PDP et PIP). Selon les politiques d'accès existantes dans le système, une permission d'accès peut être attribuée à l'utilisateur (voir l'étape 4a) ou un refus d'accès est retourné au système (étape 4b).

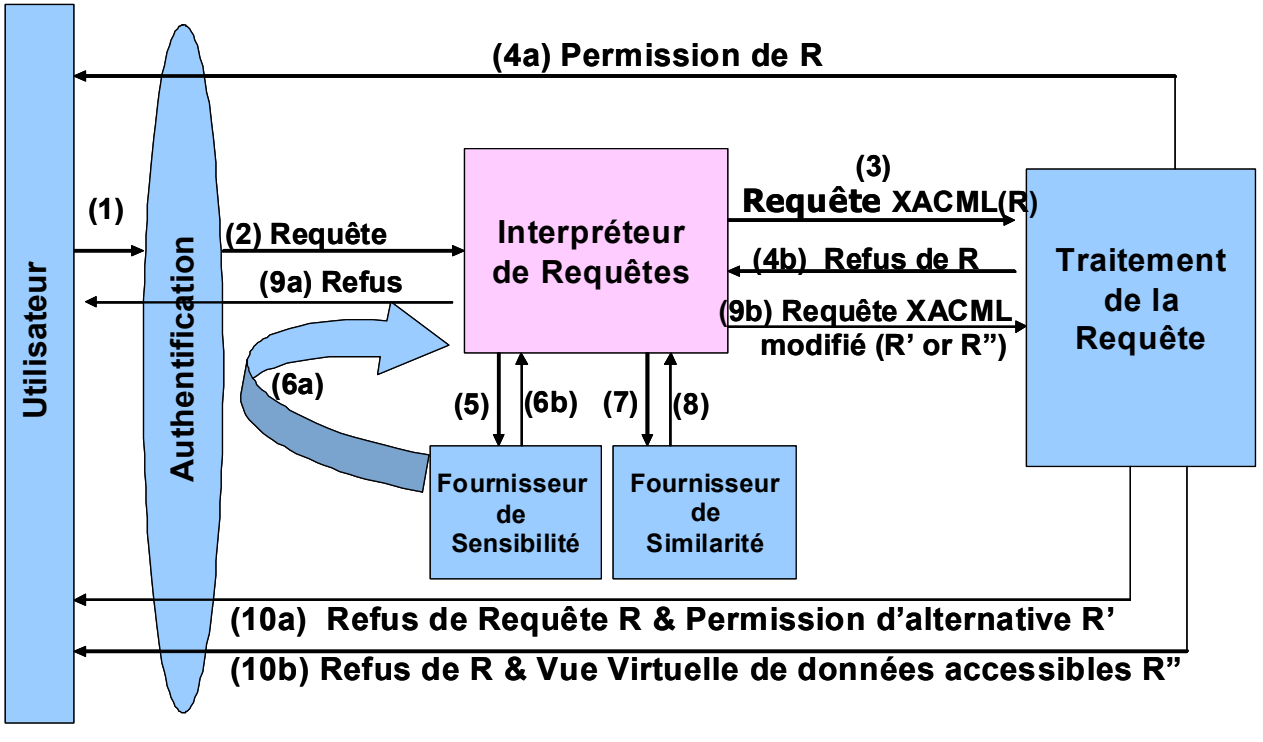

Figure 3 : Les composants de prototype qui réalise la réécriture adaptative des demandes d'accès

C'est dans ce cas que notre système va appliquer l'adaptation en examinant l'importance de la situation courante de l'utilisateur (si c'est un cas urgent ou si c'est requis pour la prise d'une décision importante). En vérifiant de la sensibilité de la demande de l'utilisateur (étape 6), le système va chercher des ressources similaires qui peuvent être utiles pour la prise de telle décision (étape 8). Ensuite, le système va réécrire la requête de l'utilisateur et la transmettre (dans l'étape 9b) pour être jugée par les composants de XACML. Finalement, si ces ressources similaires sont autorisées, notre système va présenter à l'utilisateur une de ces ressources comme alternative (étape 10a) ou une vue qui contient une liste des ressources/ services autorisés (étape 10b).

6 Conclusion

L'accès aux sources d'information est très important pour la prise de décision dans l'entreprise. La rigidité des politiques d'accès peut empêcher un décideur de consulter des données importantes pour la prise d'une certaine décision. Pour éviter le refus d'accès dans telle situation, nous avons présenté dans ce papier une solution adaptative qui vise à réécrire les demandes des utilisateurs afin de leur fournir des ressources alternatives accessibles.
Notre solution prend en compte le contexte de l'utilisateur qui peut consulter le système depuis n'importe où, n'importe comment et à n'importe quel moment. Nous appliquons notre solution au standard XACML qui décrit les politiques de contrôle d'accès en format XML et peut répondre aux besoins des environnements pervasifs.

7 Bibliographie

[1] **BARU C., GUPTA A., LUDÄSCHER B., MARCIANO R., PAPAKONSTANTINOU Y, VELIKHOV P., CHU V**.: "XML-Based Information Mediation with MIX". SIGMOD Conference 1999: 597-599

[2] **BERTINO E., CASTANO S., FERRARI E., MESITI M.:** "Specifying and Enforcing Access Control Policies for XML Document Sources", World Wide Web Toutorial 3(3), 2000.

[3] **DAMIANI, E., DE CAPITANI DI VIMERCATI S., PARABOSCHI, S., SAMARATI, P**: "Fine grained access control for soap e-services". In Proceedings of the 10th International World Wide Web Conference (May 2001), ACM, pp. 504—513

[4] **DAMIANI E, VIMERCATI S., PARABOSCHI S., SAMARATI P.:** "Securing XML Documents" In EDBT 2000 Proceedings, Konstaz, Germany, 27-31 March 2000.

[5] **FAN W., CHAN C.Y., GAROFALAKIS M.:** "Secure XML Querying with Security Views". SIGMOD Conference 2004: 587-598

[6] **GABILLON A., BRUNO E.:** "Regulating Access to XML documents", Proceedings of the fifteenth annual working conference on Database and application security 2002, Niagara, Ontario, Canada, 15-18 July 2001, pp: 299 – 314.

[7] **KUDO M., HADA S.:** "XML document security based on provisional authorization", ACM CCS 2000, Athens, Greece, pp: 87 - 96

[8] **LUO B., LEE D., LEE W., LIU P.,** "QFilter: fine-grained run-time XML access control via NFA-based query rewriting", CIKM'04, November 8–13, 2004, Washington, DC, USA. ACM, pp: 543 - 552

[9] **MANOLESCU I., BENZAKEN V., ARION A., PAPAKONSTANTINOU Y**.: Structured Materialized Views for XML Queries. BDA 2006

[10] **MOHAN S., SENGUPTA A., WU Y., KLINGINSMITH J.,** "Access Control for XML - A Dynamic Query Rewriting Approach", Conference on Information and Knowledge Management, Proceedings of the 31st VLDB Conference, ACM, Trondheim, Norway, 2005, pp : 251 - 252

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

[12] **OASIS**, "XACML Version 2.0", OASIS Standard, 1 Feb 2005, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[13] **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, pp.65-74.

[14] **RIZVI S., MENDELZON A., SUDARSHAN S., ROY P**.: “Extending Query Rewriting Techniques for Fine-Grained Access Control”, SIGMOD’04 Conference: 551-562.

[15] **WEISER M**., “The computer for the 21st century”, ACM SIGMOBILE Mobile Computing and Communications Review, Volume 3, Issue 3, July 1999, pp: 3 - 11.

[16] **W3C**, XML Encryption Syntax and Processing. W3C Candidate Recommendation 04 March 2002, http://www.w3.org/TR/2002/CR-xmlenc-core-20020304/

[17] **W3C**, XML Path Language XPath Version 1.0, W3C Recommendation 16 November 1999, http://www.w3.org/TR/xpath.

[18] **W3C**, XQuery 1.0: An XML Query Language, W3C Recommendation 23 January 2007, http://www.w3.org/TR/xquery/

[19] **W3C**, XML-Signature Syntax and Processing. W3C Recommendation 12 February 2002, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/