Ontology Based Hybrid Access Control for Automatic Interoperation

Yuqing Sun[1], Peng Pan[1], Ho-fung Leung[2], and Bin Shi[1]

[1] School of Computer Science and Technology, Shandong University, 250100 Jinan, China
{sun_yuqing, ppan}@sdu.edu.cn, meal@163.com
[2] Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong, China
lhf@cuhk.edu.hk

Abstract. Semantic interoperation and service sharing have been accepted as efficient means to facilitate collaboration among heterogonous system applications. However, extensibility and complexity are still crucial problems in supporting multi-level automatic collaborations across dynamically changed domains. In this paper, we propose the ontology based hybrid access control model. It introduces the concept of Industry Coalition, which defines the common ontology and servers as the portal of an application domain for public. By mapping local authorizations to the common ontology, an enterprise can efficiently tackle the problems of automatic interoperation across heterogonous systems in the Coalition, as well as of the general requests from dynamically changed exterior collaborators not belonging to the Coalition. Several algorithms are also proposed to generate authorization mappings and maintain security constraints consistent. To illustrate our model, an example of property right exchange is given and experiment results are discussed.

1 Introduction

With the development of distributed technologies, interoperation and services sharing are widely adopted to support collaboration across different enterprise systems [1,2]. Furthermore, the collaboration is becoming flexible and dynamic due to frequently changed market. Take the case of the supply chain management: an enterprise should consider its steady and reliable partners as well as new collaborators. This makes the enterprise system usually face wide range inquiries and should authorize different access rights for sensitive information to dynamic users according to security policies and relationships with them. It would be a time consuming and error prone process to manually manage the authorizations. Therefore, autonomic access control is urgently required to cope with the growing complexity.

Ontology has been accepted as an efficient mean to facilitate collaboration across different system applications [3,4,5]. Many researches are conducted on semantic interoperation between distributed heterogeneous database [6], like the method of automatically detecting and resolving semantic conflicts by common ontology [7] and

B. Xiao et al. (Eds.): ATC 2007, LNCS 4610, pp. 323–332, 2007.

the Access Control Toolkit (PACT) to enable privacy-preserving semantic access control without having to share metadata [8]. But these work focus on the structured data that may reside in structurally organized text files or database systems. Considering the vast amounts of resources instantly accessible to various users via web, which is semi constructed or unstructured, the semantic access control model (SAC) is proposed to support interoperability of authorization mechanism [9]. Propagation policies of authorization are proposed to prevent illegal inferences based on identification and categories of the domain-independent relationships among concepts [10]. Authors in [11] also develop a suite of tools to allow the use of semantic modeling features in XML documents. However, these work are mainly in the paradigm of communications between two ontology based systems and cannot process the plain requests without ontology. So, it is troublesome to support multi-level automatic collaborations across dynamically changed domains and enforce flexible policy.

In this paper, we propose a novel hybrid semantic access control model which introduces the concept of Industry Coalition to define the common domain ontology. On one side, by registering in the Coalition and mapping local authorizations to the common ontology, the registered member systems can automatically interoperate with each other. On another side, the Coalition servers as the portal of an application domain to help exterior collaborators query the registered members without any change of the requester's legacy systems. We also propose several algorithms of authorization mapping and security constraints verification. To illustrate our model, an example of property right exchange is given and experiment results are discussed.

The remainder of this paper is organized as follows. In section 2, preliminaries are given. In the following section we present the hybrid access control model. And then an illustrative example and experiments are discussed. At last, we draw some conclusions and future work.

2 Preliminaries

Ontology has been defined as a concept system, in which concepts are interpreted in a declarative way, as standing for the sets of their instances [12]. A common ontology-based manipulation of different resources is one of the most desirable solutions for achieving semantic interpretabilities. In work with a common ontology, four important issues should be considered: the construction of the common ontology using a comprehensive classification framework, maintenance of the ontology to allow its evolution, mapping from an information system to the common ontology, and solution of various context-dependent incompatibilities.

Since the role based access control model (RBAC) is considered as the most appropriate paradigm for access control in complex scenarios [13], our proposed model focuses on RBAC system. In RBAC, role is an abstract description of behavior and collaborative relation with others in an organization. Permission is an access authorization to object, which is assigned to role instead of to individual user so as to simplify security administration. The motivation of role hierarchy is to efficiently manage common permissions by defining multiple reusable subordinate roles in formulating other roles. Constraints are principles used to express security policy.

3 The Ontology Based Hybrid Access Control Model

The proposed ontology based hybrid access control model, called *OHAC*, is depicted in Fig.1. Different with other semantic models, it introduces the concept of Industry Coalition, which represents as an association or guild of representative enterprises in a specific application domain. By defining common ontology of the domain, the Coalition provides a platform for members to share, federate and collaborate with each other, as well as serves as a portal to provide common services for the public.

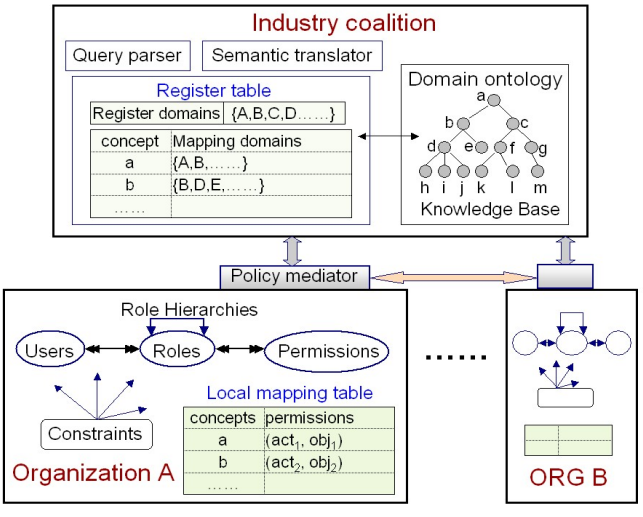

Fig. 1. The ontology based hybrid access control model (*OHAC*)

Participant members of the Coalition are distributed and autonomous in the sense that they keep control on their own resources and the rights to change the meaning and implementation of authorizations, in which role hierarchies, security policies etc. may be heterogeneous. They register in the Coalition and establish the mappings of local authorizations to the common ontology so as to support the collaboration with other registered members and respond requests coming from public users. The proposed *OHAC* model is formally defined in the following subsections.

3.1 Modeling Industry Coalition

The Industry Coalition of *OHAC* is responsible for constructing the common ontology and maintaining the register information about member enterprises. The Query Parser model is used to analyze and process users' request. If a request comes from exterior of the coalition and is not in the ontology language, the Query Parser will pass it to the Semantic Translator for translating into ontology-based query according to the common ontology. Then the Query Parser transfers it to the correlative members. Here is the formal definition of Industry Coalition.

Definition 1: A *Concept Cpt* is a generalized abstract term that may have several concrete instances, which is in form of triple *Cpt* =<*Name, Des, MpI* > where *Name* is the identifier of *Cpt*, *Des* is the description of *Cpt* in plain text, and *MpI* is the distinct set of mapping instances and stores the registered enterprise information that have mapped their authorizations to *Cpt*. It may have several properties that expressed as <*org, portal*>, where *org* is the identifier of the mapped enterprise and *portal* is the mapping information.

Definition 2: *Ontology OT* is a distinct set of concepts and their relations, which is defined as 2-tuple *OT* =< *CONCEPT, CR* >, where *CONCEPT* is a set of concepts and *CR* is a relationship on *CONCEPT*. *CR* has the form of <c_1,c_2,*relation*>, where $c_1,c_2 \in$ *CONCEPT*, and *relation* is a member of set {*sub-class, part-of, disjoint, property*}, which refers to the relationship between concepts c_1 and c_2.

Definition 3: *Industry Coalition IC* is a 4-tuple *IC*=<*Name, Des, OT, RT*>, where *Name* is a String that identifies the industry coalition, *Des* is the textural description that outline the purpose of the industry coalition, *OT* is the common ontology definition of a specific domain, and *RT* is the register table of member enterprises.

3.2 Leveraging the Legacy System of Coalition Member

Within a coalition, member enterprises may have different local meanings of system authorization and their resources may be stored in the structured data like database, semi-structured XML data or unstructured files like audio, video and pictures etc. To support automatic semantic interoperation, they should leverage their legacy systems by adding web-based interface to map local supplied authorization to the common ontology. Generally, RBAC model is adopted to enforce security policies in an enterprise legacy system, in which permissions are assigned to roles and users are assigned to concrete roles so as to acquire the permissions. So system will grant appropriate roles for authorization requests.

Definition 4: *Local Mapping Table LMT* is a triple *LMT* =<*cpt, loc_cpt, ptr*>, where *cpt* is the identifier of a concept in the common ontology, *loc_cpt* is the identifier of a locally defined concept that is corresponding to *cpt*, *ptr* gives the link of the authorized permission in local system that is relative to *cpt*.

Definition 5: *TYPE = {normal, forbidden}* is an enumerable type set of authorization or role, in which *normal* and *forbidden* respectively denote whether an authorization or role is permitted or forbidden for a request coming from exterior users.

Definition 6: A *Permission per* is defined as a 4-tuple *per*=<*id, des, type, impt*>, where *id* is the identifier of *per, des* is its description, *type*$\in$*TYPE* is the type of *per*, and *impt* is the implementation of *per* which is generally in form of (*act,obj*) to give the concrete operation.

Definition 7: A *Role r* is defined as a 4-tuple *r*=<*id, des, type, p_set*>, where *id* is its identifier, *des* is its description, *type* $\in$ *TYPE* is the role type that denotes open or not for public, and *p_set* is the set of authorization that are assigned to *r*.

Definition 8: An *Inheritance Relation IR* refers to the relationship between two roles with the properties of antisymmetric and transmissible. If role r_1 inherits all the per-

missions owned by role r_2, we denote it as $IR = (r_1, r_2)$ or $r_1 \geq r_2$ and all users of r_1 are the users of r_2.

Also we give the predicates of $AuthorizedP(r)$ to calculate the permissions owned by the given role r, which are used in the following algorithms. R and P denote the set of roles and permissions respectively.

$AuthorizedP(r \in R) = \{p \mid p \in P \wedge p \in r.p\_set\}$

3.3 Hybrid Semantic Authorization Query

After Industry Coalition establish the common ontology and member enterprises map their local authorizations to the ontology, the proposed *OHAC* model can support the hybrid automatic interoperations: *inter-access* that is across the registered member enterprises in the Coalition, and *exterior access* that is with the dynamically changed exterior enterprises not belonging to the Coalition. Details are given below.

Inter-access: When an enterprise wants to communicate with other member in the same coalition, it firstly queries the Coalition server whether the requested enterprise has registered. The Coalition server will check the *register table* and return the result. If both sides have registered on the same coalition, which means they have mapped local authorizations to the common ontology, they can communicate directly. In this case, the applicant translates its queries from local concepts into common concepts, which are inter-coalition understandable. The provider receives and translates the query from the common concept into its local means of authorization according to *local mapping table*. And then it judges whether the request is permitted or denied complying with its security policies. This process of *inter access* is illustrated in Fig.2 and the authorization management algorithm of *Authorization_Query* is given in the following subsection.

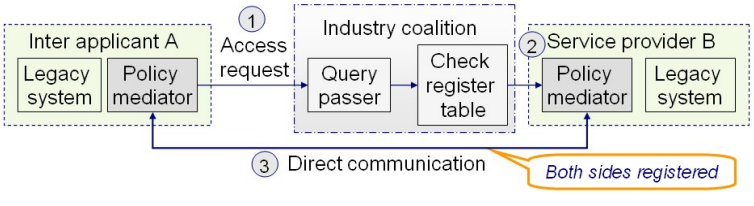

Fig. 2. *Inter-access* process across enterprises in same industry coalition

Exterior access: Member enterprises of a Coalition often have the requirements to collaborate with new appropriate partners not belonging to the Coalition so as to find new business opportunities. Vice versa, the public want to have knowledge of the industry and representative enterprises for business. In this case, the Coalition serves as a portal of all the registered enterprises to provide open services for the public. When an exterior access is requested, the Coalition server translates it into inter-coalition understandable text according to the common ontology. Then it checks the *register table* and parses the query to the correlative servers of registered enterprises that have supplied services. When these members receive the request, they activate (or deny) different roles for the applicant according to their security policies, which is

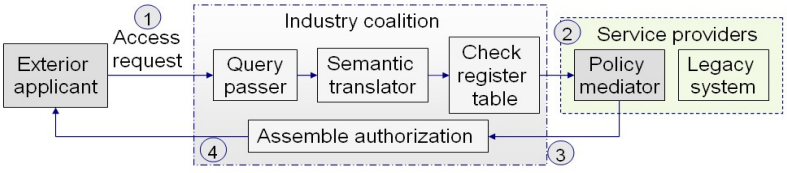

Fig. 3. Exterior access request process

depicted in the below algorithm of *Authorization_Query*, and return the results to the Coalition. The Coalition collects the results and transfers them to the applicant. This process is illustrated in Fig.3.

3.4 Role Mapping and Generation

This subsection describes the process how an enterprise responds requests. Since local systems mainly adopt RBAC to manage access rights, authorizations are embodied in roles. So it is crucial to determine which roles are granted to the applicant. We propose the algorithm to map or generate roles for a set of requests as below.

Algorithm: *Authorization_Query*(*RQ, RS*)
Input: a set of requested authorizations $RQ = \{a_1, a_2, \ldots, a_k\}$
Output: a set of permitted roles $RS = \{r_1, r_2, \ldots, r_n\}$
1. for each $a_i \in \{a_1, a_2, \ldots, a_k\}$ do step 2
2. if $a_i.type = forbidden$ then mark a_i with *DENY*; $RQ = RQ - \{a_i\}$;
3. Verify all authorizations in *RQ* to satisfy all security constraints;
4. If not consistent then remove the conflict authorizations from *RQ*;
5. For each $r \in R$ do step 6 to step 7
6. if $AuthorizedP(r) \subseteq RQ$
7. then $RS = RS \cup \{r\}$; $RQ = RQ - AuthorizedP(r)$;
8. If $RQ \neq \varnothing$ then generate a new role *r'* where $r'.p\_set = RQ$; $RS = RS \cup \{r'\}$;
9. Return *RS*.

The system firstly verifies the requests satisfying all security constraints and wipes off the forbidden authorizations. Then it searches exist roles and select the roles whose assigned permissions is a subset of the requests as candidates for the applicant. For those requests not belonging to a single role, the system will generate a new role to cover them and consider the role as a candidate too. By granted the above roles, the applicant can activate the correlative authorizations. For the complexity of above algorithm, suppose n_s and n_r be the number of security constrains and roles respectively, k is the number of requests, it is in $O(n_r + k*n_s)$.

3.5 Security Analyses

A critical issue of automatic interoperation is to ensure security constraints consistent. We focus on the constraint of conflict of interests (*CoI*) here, while others can be discussed similarly. *CoI* restrict access rights to sensitive information about enterprises with interest conflicts to different users. In an open environment, we specially

should consider the case that users acquire conflict permissions via multi domain role inheritances [14].

Here are two examples to illustrate the conflicts, which is depicted in Fig.4. In (a), roles b_2 and b_3 have the *COI* constraint in enterprise B, while in (b), roles b_2 and b_4 are with *COI*. Suppose user Alice is assigned to the role a_2, Bob is assigned to the role a_3 and John is assigned to the role a_1 in enterprise A. In example of (a), Alice and Bob separately request the authorizations of B and acquire the roles of b_2 and b_3. So John can acquire b_2 and b_3 simultaneously by inheritance. In (b), Bob acquires the new role that is generated for his requests. Although the new role and b_2 are without *COI*, John still acquires the conflict authorizations of p_1 and p_4 by inheritance. So above two cases all violate the security constraints of *COI*. Following property and correlative verification algorithm are given to verify and keep the security constraints consistent.

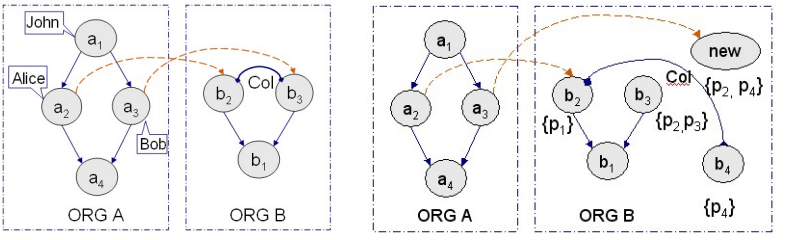

Fig. 4. Two examples of *CoI* conflicts arising from multi-domain interoperation

Property: Let *CS* be the set of *COI constraints.* Each constraint is in form of $rs=(n, p_1, p_2, \ldots, p_n) \in CS$. If *rs* is required for a set of permissions $p_1, p_2, \ldots$and p_n, then $p_1, p_2, \ldots$and p_n should not be assigned to the same role and furthermore not assigned to the same user via different roles.

Algorithm: *Verify_COI*(*CS, RS*)
Input: *COI* constraint set *CS* and the mapped role set *RS* to the same enterprise
Output: *True* if roles in *RS* satisfy constraints in *CS*; *False*, otherwise.

1. for all $r_i \in RS=\{r_1, r_2, \ldots, r_n\}$ do step 2
2. $congregation\_permissions = \bigcup_{i=1,2\ldots n} AuthorizedP(r_i)$
3. For each $rs \in CS$, do step 4 to step 5
4. $overlap\_perms = congregation\_permission \cap rs$
5. if $|overlap\_perms| > 1$ then return *Flase*
6. Return *True*

Let $|RH|$ denotes the number of role hierarchies. The complexity of predicate *AuthorizedP* is $O(|RH|)$ because it should calculate all the permissions that are authorized to its junior roles. Suppose n_s be the number of *COI* constrains. The complexity of algorithm *Verify_COI* is in polynomial time of $O(|RH|*n+n_s)$.

4 Illustrative Example and Experiments

In this section, we adopt an example of the property rights exchange to illustrate how to apply the proposed *OHAC* model in supporting automatic interoperation. Property rights exchange in China includes enterprise assets exchange, intangible assets exchange etc [15]. Property Rights Exchange Centers (*PREC*) are the concessionary enterprises that are responsible for organizing the exchange, of which systems are heterogeneous in security policies and resource structures. The relationships among them are different and they cooperate with each other at different aspects with different depth, which may be changed dynamically. Some of them associate together to exert their strong points, like the North-Association of Property Rights Exchange (*NAPRE*). There are different kinds of interoperation requirements across centers, association, participants and government etc. Accompanying with the development of property rights trade, automatic interoperation is needed to improve the efficiency while satisfying the overwhelming objective of system security.

We consider it as an appropriate example to apply the *OHAC* model, in which *NAPRE* is regarded as the Industry Coalition and is responsible for defining the common ontology of property rights exchange domain, illustrated as Fig.5. The sketch map of the register table in *NAPRE* is given in Tab.1 that records the information

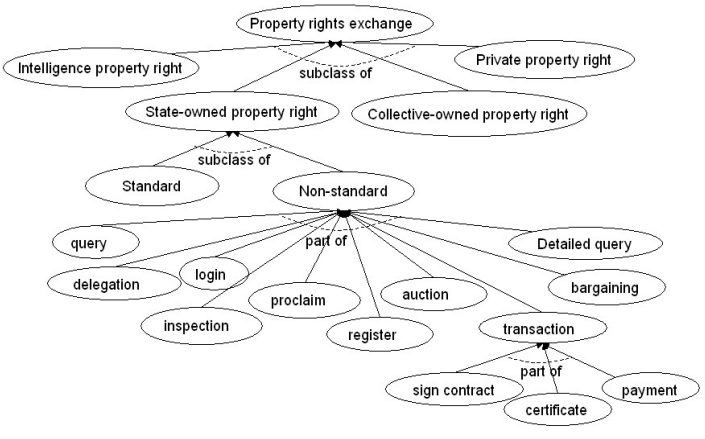

Fig. 5. The common ontology of property rights exchange domain

Table 1. The register table of the *NAPRE*

Concept	Mapping Domains
delegation	*QD,JN*
inspection	*QD,JN*
query	*SD,ZJ,TJ, BJ*
detailed query	*QD,JN*
proclaim	*QD, JN*
sign contract	*QD, JN, WF, SD, ZJ, TJ, BJ*
certificate	*QD, JN*
bargaining	*QD, JN, WF, SD, ZJ, TJ, BJ*

Table 2. The local mapping table of *PREC QD*

Concepts	Local Concepts	symbol	Authorizations	Description
delegation	entrust	*en*	*http://www.qd_pr.com/entrust.jsp*	*delegatedproject*
inspection	monitor	*mnt*	*http://www.qd_pr.com/servlet/monitorServlet*	*delegatedproject*
detailed_query	query_in_detail	*que*	*http://www.qd_pr.com/detailquery.jsp*	*projectinprocess*
proclaim	bulletin	*blt*	*http://www.qd_pr.com/bulletin.html*	*vendedproject*
sign_contract	contract	*con*	*http://www.qd_pr.com/servlet/contractServlet*	*vendedproject*
certificate	witness_trades	*wit*	*http://www.qd_pr.com/witnesstrades.htm,*	*vendedproject*
bargaining	trade-off	*trd*	*http://www.qd_pr.com/trade-off.jsp*	*vendedproject*

Table 3. System response time

Access Type		Response Time(ms)
Inter-access	1. A→B	1170
	2. A→IC→B	2052
Exterior access	3. Extra→IC→A	2484
	4. Extra→IC→A & B	4536

Table 4. System specifications

Tier	IC	Member A	Member B	Exterior applicant
CPU	Pentium 4 2.66GHz	Pentium 4 2.4GHz	Pentium 4 2.4GHz	Athlon XP 2000+
RAM	1GB	512MB	512MB	512MB
OS	Winxp sp2	Winxp sp2	Winxp sp2	Winxp sp2

about the member exchange centers in *NAPRE*. Tab.2 describes the local mapping table of the *PREC QD*.

We investigate four aspects of the proposed *OHAC* model, which are the direct interoperation between two registered members, two members interoperation via the Industry Coalition (*IC*), an exterior applicant interoperating with one member A via *IC*, and the exterior applicant interoperating with two members of A and B via *IC*. We program the prototype in Java with Sun Java j2sdk-1.4.2.04 and Apache Tomcat 5.0.28 Web Container. The network is established on the China Education and Research Network (CERNET). Each node is distributed in a different net segment that is connected by 100 Mbps LAN. The experiment results are given in Tab.3 and the system specifications are described in Tab.4. On condition of auto-interoperation, we can see from Tab.3 that the response time of type 1 is the lowest since it saves much network time. Type 2 and type 3 are similar with a little more time in type 3 for ontology translation. The time impact of type 4 is the highest, which explains that distribution of query consumes much time.

5 Conclusions and Future Work

This paper discusses the crucial problem of multi-level automatic collaborations across dynamically changed and heterogonous domains. It proposes a hybrid access control model, which introduces the concept of Industry Coalition to define the common ontology and server as the portal of a specific application domain. By mapping local

authorizations to the common ontology, enterprises can efficiently support automatic interoperations across heterogonous member systems in the Coalition, as well as the general requests from dynamically changed exterior collaborators not belonging to the Coalition. Several algorithms are also proposed to generate authorization mappings and maintain security constraints consistent. At last, an illustrative example and experiments show its effect and efficiency. Further works include improving the role generation algorithm and applying this model to new application domains.

Acknowledgements

This work was partially supported by the National Nature Science Foundation of China (90612021), the National High Technology Research and Development Program of China (863 Program) (2006AA01A113), Science Development Plan Program of Shandong province of China (2004GG2201131) and the Natural Science Foundation of Shandong Province of China (Y2004G08).

References

1. Ferraiolo, D., Barkley, J., Kuhn, R.: A Role-Based Access Control and Reference Implementation within a Corporate Intranet. ACM TISSEC 2, 34–64 (1999)
2. Park, J., Sandhu, R., Ahn, G.: Role-based Access Control on the Web. ACM TISSEC 4, 37–71 (2001)
3. Tekeda, H., Iwata, K., Takaai, M., Sawada, A., Nishida, T.: An ontology-Based Cooperative Environment for Real World Agents. Int. Conf. of Multi-agent Systems, pp. 353–360 (1996)
4. Park, J.S.: Towards Secure Collaboration on the Semantic Web. ACM SIGCAS Computers and Society 33, 1–10 (2003)
5. Bertino, E., Fan, J.P., Ferrari, E., Hacid, M.S., Elmagarmid, A.K., Zhu, X.Q.: A hierarchical access control model for video database systems. ACM TOIS 21, 155–191 (2003)
6. Pan, C.C., Mitra, P., Liu, P.: Semantic Access Control for Information Interoperation. In: Proc. of SACMAT'06, Lake Tahoe, California, USA, pp. 237–246 (2006)
7. Ram, S., et al.: Semantic Conflict Resolution Ontology: An Ontology for Detecting and Resolving Data and Schema-level Semantic Conflicts. IEEE TKDE 16, 189–202 (2004)
8. Mitra, P., Pan, C.C., Liu, P., Vijayalakshmi, A.: Privacy-preserving semantic interoperation and access control of heterogeneous databases. In: Proc. of ASIACCS, pp. 66–77 (2006)
9. Yague, M.I., Gallardo, M., Mana, A.: Semantic Access Control Model: A Formal Specification. In: di Vimercati, S.d.C., Syverson, P.F., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 24–43. Springer, Heidelberg (2005)
10. Li, Q., Vijayalakshmi, A.: Concept-level access control for the Semantic Web. In: Proc. of the ACM workshop on XML security, Fairfax, Virginia, pp. 94–103 (2003)
11. Trastour, D., Preist, C., Coleman, D.: Using Semantic Web technology to Enhance Current Business-to-Business Integration Approaches. In: Proc of EDOC, pp. 222–231 (2003)
12. van der Vet, P.E., Mars, N.J.I.: Bottom-Up Construction of Ontologies. IEEE TKDE 10, 513–526 (1998)
13. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Rose-Based Access Control Model. IEEE Computer 29, 38–47 (1996)
14. Shafiq, B., Joshi, J.B.D., Bertino, E., Ghafoor, A.: Secure Interoperation in a Multidomain Environment Employing RBAC Policies. IEEE TKDE 17, 1557–1577 (2005)
15. Sun, Y.Q., Pan, P.: PRES—A Practical Flexible RBAC Workflow System. In: Proc. of 7th International Conference on Electronic Commerce, pp. 653–658 (2005)