A Survey in Using Ontologies and Rules Reasoning in Access Control System

Pierre-Yves Gicquel[0000−0002−3639−6137], Jeremy Bouche-Pillon[0000−0001−6923−9915], Pascale Zarate[0000−0002−5188−1616], Nathalie Aussenac-Gilles[0000−0003−3653−3223], and Yannick Chevalier[0000−0002−8617−4209]

Institut de Recherche en Informatique de Toulouse (IRIT), Université de Toulouse, CNRS, Toulouse INP, UT3, UT1, UT2, F-31062 Toulouse, France

Abstract. In today's heavily cloud distributed-service period, access control systems are primary components to guarantee security and con- fidentiality of resource repositories. However, access control systems most widely used were deigned before this period of generalized service based infrastructure. This creates important difficulties in the maintenance of such systems. New approach in access control system, based on a formal and logical approach of security rules have been proposed that makes use of the semantic web technologies. In this paper we propose a survey of these semantic approaches together with a comparison of their respective strength depending on the considered use case.

Keywords. Ontology, Semantic-web, Access control, Rule based system.

1 Introduction

Access control refers to the regulation of access to shared resources depending on the entity requesting access, the characteristic of the resource and the privacy preferences of the resource/data owners [7]. Although access control has been an early topic of interest, starting with file permission systems, the generalization of cloud services and IoT raised several new challenges [8]. Most access-control systems that are *de facto* standards were designed before this generalization and are technically costly to maintain and scale on their current form. One fruitful approach for overtaking these issues is the use of semantic-web technologies to both formally describe and enforce access-control policies [17].

Although ontology-based access control policies are a subject of interest in many works, few systematic surveys were proposed on this topic. To the authors' best knowledge, the most recent one dates back to 2014 [14]. In this paper, we aim at giving a more recent overview taking into account emerging trends in ontology-based access control. We propose an original set of feature-oriented comparison criteria between different methods, which is designed to assist researchers in the choice of a particular method over another. Finally, we identified several

limitations that are consubstantial to all ontology-based control access systems and we discuss an extension of such systems using concepts from Multi-criteria Decision Analysis.
In the remainder of this paper, we first specify the used criteria for analysing the selected papers and we provide an overview of the system presented in these papers. In the second section, we compare these systems based on the proposed criteria. The third section examines limitations shared by all these approaches and discusses an architecture aiming at overcoming these limitations.

2 Surveyed Systems

To conduct this survey, approaches of the access control problem were selected based on their use of languages and formalism from semantic web to either implement or to design access control models. The approaches presented in these papers can be divided into two categories.
On the one hand, there are approaches that use an already existing access control models and try to implement them using semantic web methods and languages. On the other hand, there are approaches that searched to develop new access control models using semantic web techniques and languages.

2.1Approaches Using Already Existing Access Control Models

ROWLBAC. "ROWLBAC" is an implementation of the "Role-Based Access Control" (RBAC) model that uses OWL. The 4 key notions of RBAC are "roles", "actions", "subjects" and "objects". The RBAC policies give rights to certain "subjects" to do certain "actions" to certain "objects" depending on their "roles", like illustrated in the figure 1. The authorizations defined in RBAC are only binary, an action is either authorized or prohibited.

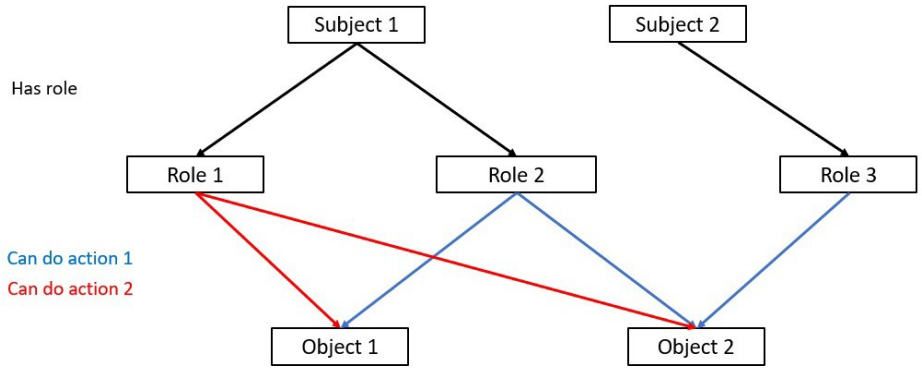

Fig. 1. Example of RBAC control

A reference in the definition of the RBAC model is the standardization works

carried out by the NIST [15, 7]. Different levels of variations of the initial RBAC model are described in [15], each one adding new constraints and capabilities to the previous one:
−*Flat RBAC*: The most basic version of RBAC, there are no relations between roles.
−*Hierarchical RBAC*: The roles are organised into a hierarchy, with a inheritance mechanism for the authorizations given to roles.
−*Constrained RBAC*: This variation introduces "Separation of Duty" (SoD) constraints. These constraints are used to specify if an action needs an authorization from more than one person to be permitted.
−*Symmetric RBAC*: Finally, this variation allows for regular revocations or reassignments of permissions in order to avoid role inflation.
The model used in [16] makes a different distinction between "possible roles" and "active roles" than in the NIST standardization [7]. Indeed, contrary to the NIST model in which a subject could only have one active role at a time, ROWLBAC allows a subject to have several active roles at a time. This modification also has a consequence on the "Separation of Duty" constraints. In ROWLBAC, there are "static SoDs" that specify the "possible roles" that a single subject can not have at the same time, and "dynamic SoDs" that indicate the roles that a single subject can not have "active" at the same time.
ROWLBAC suggests two ways of implementing RBAC principles in OWL. In the first one, each role is modeled by a class, subclass of the general class "Role" and in the second one each role is an instance of this general class [16].
Finally, the access rights are written directly in the ontology, as shown in listing 1.1. Some properties of RBAC that could not be expressed in OWL are enforced using description logic. For example, the ROWLBAC implementation uses the N3Logic language [16].
Listing 1.1: Access rule example with ROWLBAC (from [16]) Permitted Vote Action a r d f s : Class ; r d f s : sub Class Of rbac : Permitted Action ; owl : e q u i v a l e n t C l as s [a owl : Class ; owl : i n te r s e c t i o n O f (Vote [a owl : R e s t r i c t i o n ; owl : all Values From ex : A c t i v e Ci t i z e n ; owl : on Property rbac : s u b j e c t])].

ABAC. The "Attribute-Based Access Control" (ABAC) model is similar to RBAC. But instead of just the notion of "roles", any kind of attribute that allows to describe the access context can be modeled. It may be identities /roles, devices, actions, types of data, location, time, ... For instance, ABAC allows to model the whole context of data access in a smart home environment [6] (cf. figure 2).

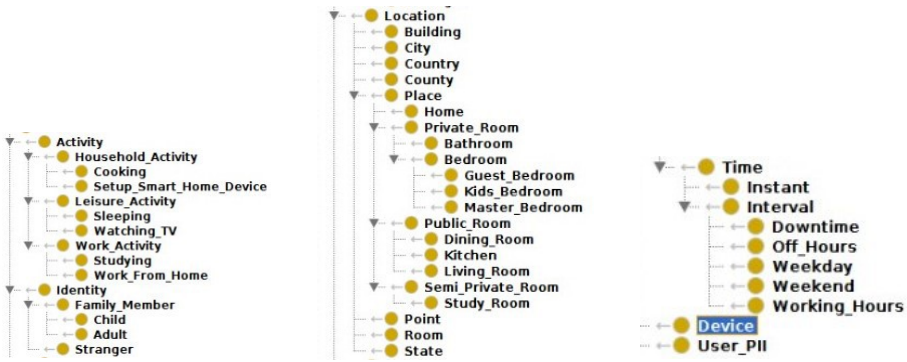

Fig. 2. Example of ABAC attributes (from [6])

One implementation of ABAC using OWL was mentioned at the end of [16], still using N3Logic to define rules. An other implementation proposed in [6] uses SWRL to write the access rules. The listing 1.2 gives an example of a rule for ABAC.

Listing 1.2: Access rule example in SWRL for ABAC model (from [6])

```
sme : CrashReports ( ?requestedData )                    ∧sme :
familyMemberInRoom ( ?aMember )                          ∧sme :
ageOf ( ?aMember , ?someAge )                          ∧swrlb : less
Than ( ?someAge , "18")                                  ∧
=> accessDenied ( ?requestedData )
```

OrBAC. "OrBAC" stands for "Organization-Based Access Control" model. It can be seen as a deepening of RBAC concepts which allows to abstract more than just the "subject" of a permission. Thus, the OrBAC model allows to describe the structure of an organization through three abstract concepts: "roles", "views" and "activities", abstracting respectively "subjects", "objects" and "actions" [9]. Here the idea of "roles" is the same as in RBAC, "views" regroup objects having a common property and "activities" model actions on "views". These abstractions are illustrated in figure 3.

Multi-OrBAC. "Multi-OrBAC" is an extension of OrBAC that allows to consider a complex network composed of many organizations. For example, a context it can be applied to would be to ensure the security of medical data processing in

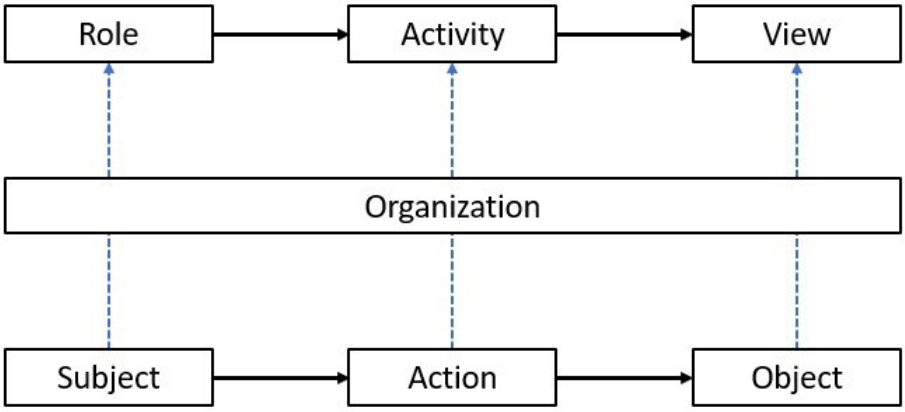

Fig. 3. OrBAC abstraction

the hospital environment [10]. Compared to the original OrBAC, Multi-OrBAC adds a level of abstraction thanks to the notion of "organization", and with it, the necessity to link the notions of "roles", "views", "actions" and "context" to the organisation they are related to. It also allows to define a hierarchy in the considered organizations as well as to describe inheritance for permissions depending on this hierarchy. Finally, the rules in Multi-OrBAC follow a similar principle than in ABAC. An example is given in listing 1.3.

Listing 1.3: Access rule example for Multi-OrBAC model (from [1])

```
Permission(Physician-in-\Org_A, Reading-in-Org_B, MedicalRecord,dis
aster) ∧ Play(Bob, Physician-in-Org_A) ∧
Correspond_to(f1.xml, MedicalRecord-in-Org_B) ∧
Belong_to(Read-xml(), Reading-in-Org_B) ∧
Is-true(disaster-in-Org_B)
-> Is_permitted(Bob, Read-Xml-File(), f1.xml)
```

2.2 Approaches Defining New Access Control Models

OBAC. The "Ontology-Based Access Control" (OBAC) model aims at providing access control mechanisms for FAIR datasets. Although FAIR principles do not necessarily require semantic web technologies to describe metadata, the use of RDF and SPARQL endpoints has become standard *de facto*. Access-control policies can be required to manage FAIR data in sensitive context, such as criminal case reports, as mentioned in [4]. These authors propose to tackle this problem by making use of existing metadata linked to the dataset under consideration. OBAC also uses the notion of roles but, unlike ROWLBAC, roles do not directly appear in rules. Instead, each role is associated to a graph projection (with SPARQL Construct, see example in listing 1.4) in order to restrain access to a subset of the original graph depending on each user's credential.

Listing 1.4: Example of SPARQL Construct query used in OBAC (from [4])

```
?item dwo:hasTitle ?object .IF
?item rdf:type dwo:Item .
?item dwo:hasDestination dwd:USA .
?item dwo:hasOrigin dwd:USA .
?item dwo:hasTopic ?topic .
?topic rdf:type ?topicType .
?topicType rdfs:subClassOf+ dwo:Drugs .
```

KAoS. Although KAos is not *stricto sensu* an access control system, we decided to include it in this paper given its major influence. KAos was initially aiming at providing an agent-based framework making use of semantics in service description to support collaboration between different systems. Multi-agent systems providing an agnostic for message transmission before the generalization of REST protocol. Although authors present KAos, in its first version, [3] as an agent-based framework, following works on KAos have left this option behind. One aspect worth noticing about KAos first version is that it was not semantically grounded despite the authors' claims. The semantics was limited to sets of action-verbs that agents were able to execute.
Nevertheless, through multiple and regular iterations (see for example [18] and [19]), KAos has become agnostic with respect to message brokers and has focused on defining an OWL representation of policies. These policies go beyond access control, for example they can be used to describe mandatory actions applying whenever a given policy fails to apply. KAos is still able to express access-control policies but its scope is larger (cf. figure 4).

3 Feature Based Comparison of Selected Systems

3.1Comparison Criteria

We have selected comparison criteria aiming to choose one of the approaches to implement an ontology-based access control using adapted to the specific needs of end users. These criteria are therefore not orthogonal but express some trade-off between different requirements.
The first criterion is the **expressiveness** of the access control rules defined by an approach. This expressiveness correlates with the granularity and the specificity of the allowed access control rules. Granularity refers to the maximum precision in selecting resources which are under control and specificity refers to the precision in selecting types of users for which the rules will apply.
The second criterion is the **ability to generalize** the approaches to different application domains. The application domain indeed strongly impacts the semantic representation of resources and users. Therefore it is crucial for a fruitful implementation to consider whether and how easily an approach can be applied to a new application domain.

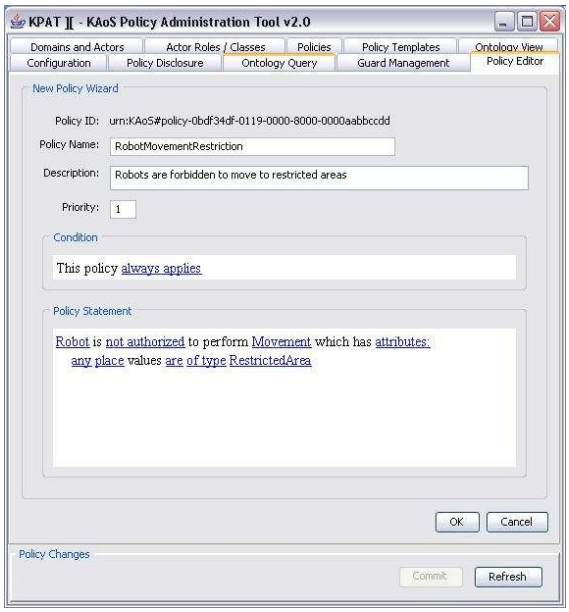

Fig. 4. Example of KAoS policy (from [19])

The third and last criterion is the **intelligibility** of the access control rule formalism. In order to maintain the system and to facilitate user acceptance, it is desirable that the formalism be understandable even with little or no prior knowledge of the semantic web. The conceptual choices have a direct impact on this possibility. Such a criterion also provides information on the auditability of the system, i.e. the possibility to check more or less automatically if the system meets certain requirements.

3.2 Comparison of approaches

Expressiveness of the rules The ROWLBAC approach, based on RBAC is expressive in terms of specificity, allowing to define arbitrary complex roles hierarchy. These roles are then associated to actions that can be either permitted or prohibited. The approach, however, provides very few ways to model actions in an expressive way, for example to organize actions hierarchically. Moreover, the approach does not allow to represent obligation, which is an important concept distinct from authorization and interdiction.

The OWL implementation of ABAC in [6] reflects the greater expressiveness of the ABAC access-control protocol over RBAC [5]. In ABAC, the authorization policies are defined by rules which depend on the attributes of the users performing the request, the considered resource and the environment in which the request is made. The notion of context of a request is introduced by taking the environment into account. [6] propose an elegant and expressive model of

physical contexts by using a transitive object property which allows to represent the physical context with different degrees of granularity. For instance, a user located in the bathroom can be considered as being either in the house or in a private room : house $\overset{\text{partOf}}{\leftarrow}$ private room $\overset{\text{partOf}}{\leftarrow}$ bathroom.
It is difficult to characterize the expressiveness of OBAC since it relies exclusively on the expressiveness of the considered FAIR dataset. Nevertheless it should be noted that the use of SPARQL Construct offers an innovative and potentially powerful way to address the issue of access control.
Multi-OrBAC is an extension of the OrBAC approach that also corrects some modeling errors that went unnoticed in OrBAC [2]. Multi-OrBAC aims at providing a well-founded semantic framework for access control across several organizations. It is together with KAOS [19] the most expressive approach of all. Not only are the concepts of roles and roles hierarchy in organization defined (as in ROWLBAC), but Multi-OrBAC also provides ways to represent resources and activities at an organization level. This does not preclude several organizations to share similar resources and activities. On the contrary, it allows to establish a correspondence between these similar activities. Furthermore, Multi-OrBAC offers the three classic deontic modalities: prohibition, obligation and permission together with a fourth (non deontic) modality: recommendation. It is thus possible to design very expressive rule sets fitting the complexity of multi-organizational access management.
Finally, KAos [**?**] is undoubtedly the most expressive approach, mainly because the scope of this approach goes beyond access-control. KAoS reaches the multi-OrBAC level of expressiveness and extends it in several ways. The most innovative advances are first the ability to define priority in rule application whenever several rules are triggered simultaneously. This allows to precisely control in which order the rules will be applied in complex situations. Second, KAoS provides the ability to take historical context of rule execution to define meta-rules that will use that context to modify the rule set and the rule execution priority.

Generalisability to other application areas The RBAC model implemented in ROWLBAC has been recognized by a NIST study as being adapted to the majority of business needs [7]. Besides, because of its simplicity, it can easily be generalized to other contexts. For example, in [16], it is used to specify authorized actions of people in a society according to their status.
In the ABAC model, the notion of "attribute" is a very broad concept, without any restriction, which makes it possible to model devices, users, actions, as well as dates and places as attributes. For instance, it can be used to model the different rooms of a house, the IoT devices in it, the types of data that can be accessed, the possible roles of the people accessing data and even differentiate time slots [6]. So, like for ROWLBAC, the ABAC model allows to describe the context of almost any situation. Because of its higher expressiveness, it can even be used in more situations than ROWLBAC.
Because OBAC is not based on a well-defined model, it is quite difficult to evaluate the ability to generalize this approach [4]. In the end, the use of OBAC

in a system depends on the format of the used data. OrBAC and Multi-OrBAC, although very useful to easily and efficiently model the structure of a complex organization, cannot be generalized as much as the previous works [2]. The three central concepts of OrBAC, namely roles, views and activities, restrict its use to situations where these notions are relevant.
The KAos approach aims at generality by design, which makes it applica- ble to many new situations. However, it suffers from two particularly strong limitations. The first limitation relates to the choice of compiling rules in an intermediate, non-standard format, to improve performances. This choice makes it difficult to guarantee that any rule expressed in OWL could be actually compiled and the authors provides no theoretical proof giving such guarantee. The second limitation is the fact that some of KAoS features are not expressible in OWL and require to rely on the correctness of the implementation. This is for example the case for assigning priority to rules. This limitations make it difficult to reuse KAoS approach, instead, one would have to use the whole KAoS framework without much possibility of modifying it (the cost of modifying a source framework of this complexity being prohibitive).

Intelligibility for the end user The formal language used in ROWLBAC to express access rules is N3Logic [16], a language that allows the expression of human-understandable rules. Rules in ROWLBAC can enforce some desired properties that could not be expressed in the model, for instance "separation of duty" rules. Unfortunately, these kinds of rules can be complex and hard to understand. Two ways to model roles are presented in [16]. The first one allows the use of Description Logic reasoning to infer the hierarchy between the different roles, but the second one does not. As a consequence, rules in N3Logic must be written to enforce the inheritance of roles. These rules are short and simple. Finally, the last rules are defined to enforce the access control itself. Because of the simplicity of the RBAC model that ROWLBAC implements, these rules are short and they explicitly show the logic behind the authorization of an action.
Because of its greater expressiveness, ABAC [6] is less intelligible than ROWLBAC. Indeed, the contexts that can be described in ABAC are more complex and take into account way more aspects than just roles. And having more com- plex contexts means that the access rules associated to these contexts are likely to be more complex too.
With OBAC, the rules are defined using relations described directly in the data. The examples given in [4] are quite explicit. In order to understand the rules, the user only needs to have an idea of how the data are organized. In the end, with OBAC, the intelligibility of the rules depends on the intelligibility of the data themselves.
The OrBAC model is constrained by its key concepts: roles, views and activities [2]. However, unlike ROWLBAC which is only constrained by the notion of role, understanding the concepts behind the ideas of OrBAC is not trivial and requires some knowledge of the model, this complexity of which makes the access rules harder to understand. Multi-OrBAC even increases this complexity by adding the notion of organization, and with it, the ideas of "Role in an Organization", "View in an Organization", "Activity in an

Organization" and "Context in an organization" [2]. All these elements must be specified in the access rules. In the end, the rules in Multi-OrBAC, although allowing a precise control of data access, are hard to understand without prior knowledge of the model and the concepts behind it.
KAoS framework, with a user interface for rule expression in a syntax close to natural language, certainly is the most intelligible one for end users.

Overview The analysis previously carried out is summarized in table 1.

Table 1. Summary of the analysis

Name	Expressiveness	Generalisability	Intelligibility
RBAC	-	+	-
ABAC	++	++	+
OrBAC	+	-	–
Multi-OrBAC	++	-	-
OBAC	=	=	=
KAoS	++	–	+

4 Discussion and future work

The generalization of open-data is undoubtedly an improvement. This may explain why the issue of controlling access to accessible data-sets has only received little interest in the scientific community. Nevertheless, with the rise of e-governments and the increasing need for collaboration between Law Enforcement Agencies to fight crime at an international level (see [12] for an example on tax evasion) by using large amounts of data, the need for differentiated and semantic access control over data is likely to increase.
Using semantic technologies to ensure access control has undeniable advantages. First of all, the theoretical foundation of the semantic web are very solid and the technology itself has been in use for decades, which offers strong guarantee of reliability for a domain as sensitive as access control. Furthermore, semantic web and ontologies are strongly related to knowledge representation and do not use black box algorithms, so each decision of authorization or prohibition to access a resource by an entity is explicable.
However, these advantages come with several drawbacks that restrain the practical use of semantic technologies for access control. The most important limitation is the cost, both in time and resources, of tailoring an approach to

a particular use-case. Ontological engineering is known to require a substantial amount of conceptualization time before any implementation. Meanwhile, organizations such as national Law Enforcement Agencies are subject to frequent regulatory changes. In a pure semantic approach, each regulatory change would require non-negligible amount of time to update the system properly.
These considerations have led us to define a new approach based on a distinction between slowly evolving primary source of access control rules (i.e organic laws, international treaties) and fast evolving secondary source of access control rules (i.e organizational level regulation). We aim to develop a new approach that will use semantic web technologies for the modeling of the primary sources of access control rules, which applies to each organization and will use a reinforcement learning decision support system for the secondary sources of access control. The latter approach was experienced within the context of supporting end users in authorization management for the Android platform [13].
The Decision Support System, based on a Multicriteria Decision Analysis approach, will therefore be used to handle fast change in organizational policies relative to access control. Its scope, that is, the set of resources for which it will provide authorization, prohibition or permission, will be a subset of the resources managed by the semantic access control system. Indeed, the organizational policies are lower in the hierarchy of norms [11] and must therefore comply with the higher norms, for example a national police regulation must comply with organic laws of the nation the police belongs to.
What we aim is therefore to reuse the works on ontological-access control to model high-level (i.e. organic laws) access control regulation. Then to define an approach based on Multicriteria Decision Analysis to provide a finer and easier to modify access control at institution level.

References

1. Abou El Kalam, A., Deswarte, Y.: Multi-orbac: A new access control model for distributed, heterogeneous and collaborative systems. In: Proceedings of the IEEE Symposium on Systems and Information Security (2006)
2. Abou El Kalam, A., Deswarte, Y.: Multi-orbac: A new access control model for distributed, heterogeneous and collaborative systems. In: Proceedings of the IEEE Symposium on Systems and Information Security (2006)
3. Bradshaw, J., Dutfield, S., Benoit, P., Woolley, J.: Kaos: Toward an industrial-strength open agent architecture. Software Agents (01 1997)
4. Brewster,C., Nouwt, B., Raaijmakers, S., Verhoosel, J.:Ontology- based Access Control for FAIR Data. Data Intelligence **2**(1- 2), 66–77 (jan2020). https://doi.org/10.1162/DINT_A_00029, https://direct.mit.edu/dint/article/2/1-2/66/9993/Ontology-based-Access- Control-for-FAIR-Data
5. Das, S., Mitra, B., Atluri, V., Vaidya, J., Sural, S.: Policy Engineering in RBAC and ABAC, pp. 24–54. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-030-04834-1_2
6. Dutta, S., Chukkapalli, S.S.L., Sulgekar, M., Krithivasan, S., Das, P.K., Joshi, A.:

Context sensitive access control in smart home environments. In: 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). pp. 35–41 (2020). https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00018
7. Ferraiolo, D., Richard, D.: Role-based access controls. In: Proceedings of the 15th NIST-NSA National Computer Security Conference, Baltimore, Maryland (1992)
8. Imran-Daud, M.: Ontology-based Access Control in Open Scenarios: Applications to Social Networks and the Cloud. Ph.D. thesis, Universitat Rovira i Virgili. (2016)
9. Kalam, A., Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., Trouessin, G.: Organization based access con- trol. In: Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks. pp. 120–131 (2003). https://doi.org/10.1109/POLICY.2003.1206966
10. Kalam, A., Deswarte, Y.: Multi-orbac: un modèle de contrôle d'accès pour les systèmes multi-organisationnels (06 2006)
11. Kelsen, H.: Pure Theory of Law. University of California Press (1967), https://books.google.fr/books?id=8N5S6BjX3RAC
12. Khlif, H., Amara, I.: Political connections, corruption and tax evasion: a cross- country investigation. Journal of Financial Crime (2019)
13. Oglaza, A., Zaraté, P., Laborde, R.: KAPUER: A Decision Support Sys- tem for Privacy Policies Specification. Annals of Data Science **1**(3), 369– 391 (Dec 2014). https://doi.org/10.1007/s40745-014-0027-3, https://hal.archives-ouvertes.fr/hal-01387752
14. Papagiannakopoulou, E.I., Koukovini, M.N., Lioudakis, G.V., Dellas, N.L., Kaklamani, D.I., Venieris, L.S.: Leveraging semantic web technologies for access control. Emerging Trends in ICT Security pp. 493–506 (1 2014). https://doi.org/10.1016/B978-0-12-411474-6.00030-X
15. Sandhu, R., Ferraiolo, D., Kuhn, R.: The nist model for role-based access control. In: Proceedings of the fifth ACM workshop on Role-based access control - RBAC '00. pp. 47–63. ACM Press (2000). https://doi.org/10.1145/344287.344301
16. for Computing Machinery. Special Interest Group on Security, A.A.: SACMAT '08: proceedings of the 13th ACM Symposium on Access Control Models and Technologies: Estes Park, Colorado, USA, June 11-13, 2008. Association for Computing Machinery (2008)
17. Senthilkumar, S., Viswanatham, M.: Survey on data access control techniques in cloud computing. In: Proceedings of ICETETS 2016 (2016).
18. Uszok, A., Bradshaw, J.M., Lott, J., Breedy, M., Bunch, L., Feltovich, P., John- son, M., Jung, H.: New developments in ontology-based policy management: Increasing the practicality and comprehensiveness of kaos. In: 2008 IEEE Work- shop on Policies for Distributed Systems and Networks. pp. 145–152 (2008). https://doi.org/10.1109/POLICY.2008.47
19. Uszok, A., Bradshaw, J.M., Lott, J., Johnson, M., Breedy, M., Vignati, M., Whit- taker, K., Jakubowski, K., Bowcock, J., Apgard, D.: Toward a flexible ontology- based policy approach for network operations using the kaos framework. In: 2011-MILCOM 2011 Military Communications Conference. pp. 1108–1114. IEEE (2011).