Generic Access Control Model and Semantic Mapping Between Heterogeneous Policies

Samira Haguouche, Computer Science Department, Cadi Ayyad University, LISI Laboratory, Marrakech, Morocco
Zahi Jarir, Computer Science Department, Cadi Ayyad University, Marrakech, Morocco

ABSTRACT
This article aims to ensure a dynamic set up of access control policies across collaborating organizations where these organizations adopt heterogeneous access control models. To attain this objective, this contribution started with a survey on existing access control models, and their specificities on collaboration. Based on this survey, it remains that the topic on access control collaboration still open despite the efforts made. Therefore, in this article a generic representation of access control concepts is proposed. This generic representation considers the process of semantic mapping between policies of heterogeneous access control systems. In this fact an ontology-based semantic mapping is proposed. This mapping has the advantage to optimize the administrators’ involvement by combining linguistic-based and upper-ontology based matching techniques with a user-based constraint strategy for ontology matching.

KEYWORDS
Access Control, Collaborative Environment, Generic Access Control Model, Heterogeneous Access Control Models, Ontology Matching, Semantic Mapping, Ontology

INTRODUCTION
Access control is the process of mediating every request to access a resource or data and determining whether the request should be granted or denied. Access control studies have identified several useful access control models (Haguouche & Jarir, 2015b), which provide a formal representation of policies and address various aspects of access control problem.

In a multi-organizational collaboration, access control becomes more challenging owing to the fact that collaborating organizations could adopt different access control models and use heterogeneous systems and policies to control access to their resources. When multiple organizations need to collaborate with each other, they typically exchange services and resources based on certain restrictions described in the access control policy. This policy is defined according to an access control model and concerns entities specific to the concerned organization. To consume the service, the policy should be translated to be readable by the access control system of the consumer organization.

DOI: 10.4018/IJTD.2018100104

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
To ensure interoperability between heterogeneous access control systems, the aim of this paper is to suggest an approach having the advantage to translate dynamically described access control policies from one model to another. To this end, we define a generic access control model, to which we have given a skeleton outline in a previous work (Haguouche & Jarir, 2015b). This generic model specifies generic concepts we rely on to automatize the mapping. The dynamic mapping involves two kinds of automation: syntactic transformations and semantic correspondences. To achieve syntactic transformations, we have proposed an algorithm based on XACML grammar to translate access control policies.

We focus, in this paper, on the second type which concerns the semantic correspondences between heterogeneous access control systems. Thus, we propose an ontology based semantic mapping that optimizes the administrators’ involvement by combining linguistic-based (Than-Le Bach, Dieng-Kuntz, & Gandon, 2004) and upper-ontology based matching techniques (Mascardi, Locoro, & Rosso, 2010) with a user-based constraint strategy for ontology matching (Lin & Sandkuhl, 2008).

The rest of this paper is organized as follows: Section “Genericness of access control models concepts” surveys the concepts of existing access control models and proposes a generic model, whereas section “Mapping between heterogeneous access control systems” shows how we base on generic concepts and correspondence between constraints in policies to address the mapping. We describe thereafter in section “Ontology matching process” the process proposed to ensure the semantic mapping using ontologies. In section “Related work”, we compare our contribution with some related papers and finally, we summarize the work and highlight the future work in the section “Conclusion”.

**GENERICNESS OF ACCESS CONTROL MODEL CONCEPTS**

The abstraction of access control involves three elements of access control systems (Samarati & Capitani, 2001):

1. The policy that defines the high-level rules according to which access control is regulated;
2. The model that provides a formal representation of the access control policies and tries to ensure a level of abstraction over the access control components;
3. The mechanism that defines the low-level functions that implement the controls imposed by the policy and formally stated in the model.

Several models for access control exist in the literature such as IBAC (Shen & Dewan, 1992), RBAC (Sandhu, Coyne, Feinstein, & Youman, 1996), ABAC (Yuan & Tong, 2005), etc. In (Haguouche & Jarir, 2015b), we studied access control models characterized by innovative elements or abstractions to describe access control policies. Thereafter we identified four main common entities:

- The Requestor that represents the entity requesting access to the resource; it can be a user, a running process or an abstract entity such a role;
- The Requestee which is the entity requested for access or use. It is concerned with the access control rule;
- The Access type that defines the action performed on the requestee;
- The Context that represents every contextual element that depends neither on the requestor nor on the requestee and that can influence the access control (e.g. location, time, etc.).

Each access control model defines a set of concepts to describe these four entities or to define an abstraction of some of them. Table 1 shows a correlation between the access control models concepts and the four aforementioned generic entities.
Perceived Utility in Online Auctions: A Joint-Effect of Vendor, Product and Pricing
[www.igi-global.com/article/perceived-utility-in-online-auctions/113762?camid=4v1a](www.igi-global.com/article/perceived-utility-in-online-auctions/113762?camid=4v1a)

Transfer of Information Technology to the Arab World: A Test of Cultural Influence Modeling
[www.igi-global.com/chapter/transfer-information-technology-arab-world/23710?camid=4v1a](www.igi-global.com/chapter/transfer-information-technology-arab-world/23710?camid=4v1a)