Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2023) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

27th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2023)

Translating Usage Control Policies to Semantic Rules: A Model using OrBAC and SWRL

Nouha Laamech[a,*], Manuel Munier[a], Congduc Pham[b]

[a] *Universite de Pau et des Pays de l'Adour, E2S UPPA, LIUPPA, Mont-de-Marsan, France*
[b] *Universite de Pau et des Pays de l'Adour, E2S UPPA, LIUPPA, Pau, France*

Abstract

The increasing volume of data in various environments such as IoT and the need to maintain data privacy and security have led to the development of usage control models. Usage control policies are models that enable fine-grained access control over data by enforcing restrictions on how users can use the data. Semantic mechanisms, on the other hand, use context and meaning to identify potential security threats and prevent them from accessing sensitive information. Although not widely explored, merging these two techniques could create an efficient mechanism to help ensure the confidentiality, integrity, and availability of critical data and resources. This paper aims to encourage this research path by proposing a translation model that converts usage control rules into SWRL. In particular, we consider during our approach the notions of context, permission and prohibition. The proposition is validated by constructing a multi-layer proof of concept that use ontologies and OWL for implementing the translation model. Furthermore, to ascertain the practicality of our approach, a time processing evaluation is conducted, and the results are found to be satisfactory.

Keywords: Usage Control, Semantic Web Rule Language, Security;

1. Introduction

Nowadays, the distinctive focus on generating collaborations between smart devices to achieve efficient performance, as well as the requirement for third-party involvement, exposes devices, actors, and the entire connected system to potential security and safety issues. To address this, controlling and restricting access to resources is one of the fundamental mechanisms used to restoring order and ensuring transparency [1]. Therefore, access control models such as MAC [2], DAC [3] and RBAC [4] have emerged. These models are based on the establishment of a set of

* Corresponding author. Tel.: +33 5 58 51 37 00.
E-mail address: laamech.nouha@univ-pau.fr