Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 109C (2017) 718–724

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Ambient Systems, Networks and Technologies
(ANT 2017)

Semantic Based Authorization Framework For Multi-Domain Collaborative Cloud Environments

Mohamed Hilia[a], Abdelghani Chibani[b,a,*], Thierry Winter[a], Karim Djouani[b,*]

[a]*Atos-Evidian, SA. Evidian BP 68 Avenue Jean Jaures, Les clayes sous bois 78340, France*
[b]*UPEC University, LISSI Laboratory, Vitry sur seine 94400, France*

Abstract

Currently, organizations are growing and continuously improving their services while reducing budget in a competitive market. This is achieved by reusing existing well designed and proved services delivered by third parties in the cloud. Additionally, multi-domain collaborative cloud environments are a promising approach that enables to build and deliver new adaptive, distributed and reliable services. In this case, the data interoperability, the process interoperability and the security open new challenges and issues. In this paper, we propose semantic-based decision making process and consistent with XACML architecture to deal with contextual access control in multi-domain collaborative cloud environments.

Keywords: Linked Data; Security Policies; Ontology Reasoning; Interoperability; Multi-domain

1. Introduction

The emergence of new Information and Communication Technologies such as Internet Of Things (IoT), Cloud Computing[16] and Semantic Web technologies[1] are commonly adopted and rolled out by several sectors such as healthcare, manufacturing, autonomous transport. These technologies bring new capabilities and lead to build sophisticated and intelligent services. Besides, the adoption of new communication supports and devices such as sensors, actuators, robotic systems, smart-phones, PDAs, etc. are leading to build smart integrated environments[12] such as smart spaces, smart cities or manufacturing plants. In such a way, these ecosystems deploy sophisticated technologies and tools (e.g. data analytics, monitoring) and deliver added-value features, adaptive processes and highly dependable services. Currently, organizations are growing and continuously improving their services while reducing building budget in a competitive market. This is achieved by reusing existing well designed and proved services delivered by third-parties[12]. For these reasons, multi-domain collaborative environments are a promising approach that enables to build and deliver new adaptive, distributed and reliable services. Multi-domain collaborative environments are

[*] Corresponding author. Tel.: +33-130803348
E-mail address: mohamed.hilia@evidian.com

10.1016/j.procs.2017.05.427

defined as trusted environments where several domains (i.e. organization) share, manage and perform processes in a decentralized manner to fulfill common business objectives. In this case, the data interoperability, the process interoperability and the security open new challenges and issues[6,14] . In addition, recent interesting research and industrial initiatives motivated the advantages of using linked data technologies for integrating data across distributed sources[3,8]. Establishing a circle of trust between partners does not resolve the confidentiality issues of the cloud data. Moreover, sensitive data should be kept private without affecting its availability. In this case, controlling data access is required, but is highly dependent on the contextual information of the collaborative domains. As a consequence, access control systems should be able to support new context information in order to address access control requirements in such complex systems[4,14]. On the one hand, several access control standards (e.g. SAML[11], XACML[15], RBAC[13]) have been proposed to work within inter-organizational environments, and on the other hand, semantic-based models (e.g. RDF) were recently adopted for sharing, exchanging and publishing cloud data[8]. Fine-grained access control authorizations in multi-domain cloud environments can be achieved by expressing security policies in XACML (eXtensible Access Control Markup Language)[15,14]. XACML is an access control standard based on the XML language. It aims at representing authorization policies, authorization requests and responses in a formal way. The XACML standard proposes a list of combining algorithms to evaluate multiple authorization policies. It provides a lot of flexibility as it is a very general purpose language and extremely extensible. XACML is considered by several achieved work as the best candidate to ensure access control in collaborative cloud environments[14,4]. Besides, in our knowledge, no access control using linked data and the XACML standard to enhance the authorization process in a multi-domain context was proposed. In this paper, we propose a semantic-based authorization approach for enabling contextual access control in multi-domain collaborative cloud environments where only the authorized partners should perform what they are permitted to do. By consequence, the permitted and denied accesses to this data is fully controlled.

The rest of this paper is organized as follows. Section 2 presents background information about Linked Data and access control mechanisms. Section 3 presents an overview on the proposed approaches for securing Linked Data and motivate the need behind the proposed Framework. Section 4 describes the security aspects of the ComVantage approach, while Section 5 depicts the framework architecture, gives the main advantages of this architecture and details how the authorization service can be enhanced with an ontology reasoning. The implementation aspects and results are presented in Section 7. Section 8 concludes and presents the ongoing work.

2. Background

Linked Data. It represents a set of best practices for modeling and interconnecting information in a widely accepted semantic way. Recently, a large linked Datasets have been publicly published such as DBPedia `http://wiki.dbpedia.org`, which essentially makes data available in RDF. Linked Data is created by using Resource Description Framework (RDF) as the base model. RDF handles information as a semantic network of single statements consisting of the triple model (subject, predicate, object). Every piece of knowledge is represented as triples and the triple entities are referenced by URIs. A named graph is a collection of RDF statements grouped together and also identified by a URI. SPARQL (SPARQL Protocol And RDF Query Language) is the most popular and dominant query language in the Semantic Web. It specifies the three following parts : *Query Language*, *Resulat Format* and *Access Protocol*. It uses a graph-based matching mechanism with powerful filter and aggregating functionality with additional support for named graphs. Nevertheless, Linked Data might also be a useful technology for industrial environments for sharing business data. This requires access control mechanisms to protect this data, and preserve its confidentiality.

Access Control Mechanisms. Controlling access to Linked Data requires the specification and enforcement of security policies. The policy specification is based on access control models such Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). In RBAC, roles are defined as a list of permissions, users are assigned to appropriate roles and access to resources is granted to one or more roles. RBAC policies have been the further adopted authorization mechanism used in enterprises for many years. ABAC, which was also designed for distributed systems, provides an alternative means of access control where the requester is unknown prior to the submission of the request. ABAC grants or denies access to resources, based on attributes of the requester and/or the resource. Early work on semantic access control policies was based on RBAC. However, most of the recent work in this area is based on ABAC[10]