Future Generation Computer Systems 78 (2018) 1–17

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

# ACROSS: A generic framework for attribute-based access control with distributed policies for virtual organizations

Edelberto Franco Silva [a,b,*], Débora Christina Muchaluat-Saade [b], Natalia Castro Fernandes [b]

[a] Federal University of Juiz de Fora, Juiz de Fora, MG, Brazil
[b] MídiaCom Laboratory, Fluminense Federal University, Niterói, RJ, Brazil

## HIGHLIGHTS

- A generic, extensible, and flexible framework of authentication and authorization for virtual organizations is proposed.
- The solution increases the agility to join or create a virtual organization.
- Support for identity federation, access control mechanisms, additional attributes and credential translation.
- Creates a new and modern solution of identity and access management for distributed-resources environment.

## ARTICLE INFO

*Article history:*
Received 15 June 2016
Received in revised form 12 June 2017
Accepted 21 July 2017
Available online 12 August 2017

*Keywords:*
Virtual organization
Identity and access management
Authentication
Authorization
Attribute-based access control

## ABSTRACT

Research interests about access control mechanisms for distributed resources have recently increased. In this scenario, users from different institutions access distributed resources, maintained by different organizations, in order to participate in a common research project, network, or testbed. Several challenges arise from these virtual organizations in order to give different types of access privileges to distinct types of resources, depending on the user profile and considering local and global access policies from partners. This work presents a generic and extensible authentication and authorization framework, named ACROSS, based on policies and attributes for virtual organizations. Our proposal creates a granular and scalable access control, which supports different authentication technologies and is independent of the kind of resource federation. In addition, ACROSS introduces a new concept of attribute generalization for access control, providing a transparent management based on access level computed from user attribute values and weights. Other works with similar goals have limitations restricting their integration with any kind of identity and resource federations. Also, these works present restrictions concerning environment and resource types. Hence, they are specific for usage in grid computing, testbed experimentation, or other distributed-resource environment. Differently from other proposals, ACROSS is a framework for supporting the development of new virtual organizations using any kind of resource sharing. ACROSS provides all A&A functionalities so that creating the virtual organization is no longer a challenge for new applications. We validate ACROSS using it on two scenarios: a real testbed and a testing environment composed of resources simulating a distributed open lab. The results show the feasibility to apply the proposal to different scenarios.



## 1. Introduction

In resource-distributed environments, such as in grid computing, cloud computing, and Future Internet (FI) testbeds, access control is a very important feature, once it is responsible for providing user access to distributed resources.

There are scenarios where different partners from different institutions access a shared distributed-resource environment, and resources are maintained by different administrators following distinct access policies. On the other hand, in those scenarios, partners should have common policies for sharing their resource infrastructure, making access control a huge challenge. We call such scenario a Virtual Organization (VO) [1].

* Corresponding author at: Federal University of Juiz de Fora, Juiz de Fora, MG, Brazil.
*E-mail addresses:* edelberto@ice.ufjf.br (E.F. Silva), debora@midiacom.uff.br (D.C. Muchaluat-Saade), natalia@midiacom.uff.br (N.C. Fernandes).

http://dx.doi.org/10.1016/j.future.2017.07.049
0167-739X/

In the literature, we can find several proposals to provide access control functionalities for distributed-resource environments, especially in grid computing [1], cloud computing [2,3], and FI testbeds [4]. Therefore, those are specific solutions for each specific scenario, which are usually difficult to be adapted to be used in a different context. For example, a framework for grid computing is rarely used in a cloud computing scenario. Other cases are applied only to extend or adapt a kind of authentication in a specific scenario or technology, as it is possible to see in [3].

This work presents a new proposal to obtain the benefits of identity and access management in VOs through a complete, flexible, and integrated authentication and authorization solution. We introduce a generic framework called ACROSS (**A**ttribute-based access **C**ont**RO**l and di**S**tributed policie**S**), which deals with identity federation and access control policies in order to facilitate identity management in VOs. ACROSS is a framework for access control based on policies and attributes for VOs, which respects the "X.812 — ISO/IEC 10181 — 3 : 1996" [5] standard framework for access control.

ACROSS is a complete authentication and authorization solution for VO, supporting many concepts of identity management and resources management. Among all benefits of using ACROSS, we highlight some characteristics it provides:

- a generic authentication and authorization framework with attribute-based access control and distributed policies for virtual organizations;
- support to different authentication technologies;
- independence of the kind of resource federation;
- a solution of attribute aggregation supporting multiple specific attribute providers for virtual organization scenarios and respecting the user privacy based on unique identity opaque attribute;
- a new model of user level classification based on his/her attributes and attribute-based access control concepts; and
- support to identity federation authentication and credential translation, making it easier to create credentials for a specific environment.

To satisfy these requirements and benefits, ACROSS was modelled and modularized, allowing the deployment of each module independently from the others. As a consequence, ACROSS allows the update of any module whenever necessary.

The rest of this article is organized as follows. Section 2 shows an essential background of technologies, standards, and concepts necessary to understand this proposal. Section 3 details our proposal and presents a comparison between our proposal and related work. Section 4 presents the validation results, and in Section 5, conclusions and future works are described.

## 2. Background

### 2.1. Related technologies

Since Kerberos was introduced in 1987 [6] addressing authentication, authorization, and accounting, many studies and solutions were proposed for Identity and Access Management (IAM) [7]. In IAM, the Identity Management (IdM) is responsible for ensuring the quality of identity information such as identifiers, credentials, and attributes and using it for authentication, authorization, and accounting processes.

An identity federation enables transparent access to its users to the services offered by the members and partners. This federation is supported by communication and message exchange standards, such as SAML (Security Assertion Markup Language) [8]. In an identity federation the user has only a single credential, created in his/her home institution, which allows the transparent and single sign on access.

The most used standard for web authentication in identity federations is SAML standard. This standard has two main types of entities that compose an Authentication and Authorization (A&A) identity federation environment: the Identity Provider (IdP), responsible for storing and providing information about users and their authentication; and, the Service Provider (SP), responsible for offering one or more services or resources. The most widespread solution of SAML is Shibboleth, which implements SAML and allows web applications to enjoy the facilities provided by the federated identity model, such as the concept of Single Sign-On (SSO).

Authorization and access control mechanisms are responsible for associating access rights to resources for a user identity, describing his/her rights and ensuring that they are respected. Therefore, an identity federation is responsible for helping this step, validating the user credential and enabling authorization procedures.

XACML (eXtensible Access Control Markup Language) [9] is an XML-based standard language for declaring security policies by OASIS, and implements ISO/IEC 10181-3 [5], the ITU X.812 recommendation. Fig. 1(a) presents an overview of the X.812 model. In the figure, we see two essential components: Access Control Enforcement Functions (AEF) and Access Control Decision Functions (ADF). The main idea of the authorization framework is that AEF ensures that all access requests pass through ADF, where ADF decides, based on a set of rules or policies, the authorization result. In XACML, these components are renamed: AEF is equivalent to Policy Enforcement Point (PEP) and ADF is equivalent to Policy Decision Point (PDP). XACML presents two more components, Policy Administration Point (PAP) and Policy Information Point (PIP), as we can see in Fig. 1(b). PAP allows the manager to add or edit policies, and PIP is responsible to store additional attributes for resources, subjects, and the environment itself.

The main access control mechanisms are ABAC (Attribute-Based Access Control) and RBAC (Role-Based Access Control). ABAC [10] is an access control mechanism where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject. A guide with common concepts to create a unified ABAC access control mechanism, based on XACML architecture and X.812 standard is available in [10]. ABAC provides flexible mechanisms to apply distributed policies and access control based on user and resource attributes. Role-based access control (RBAC) [11] is a classic standardized control access mechanism widely used. It is based on roles, which facilitates its implementation, but does not make it as flexible as ABAC, requiring creating specific rules for specific roles.

Another topic that deserves to be highlighted is the resource discovery and reservation in virtual organizations for resource sharing. In Future Internet testbeds, an important proposal is the Slice-Based Federation Architecture (SFA) [12], which is currently used in testbeds such as OneLab, FIBRE (Future Internet Brazilian Environment for Experimentation) [4], and PlanetLab. In SFA-based FI testbeds, users supply their credentials to get access authorization to a set of resources located in different institutions, such as a set of computers and a minimal specified bandwidth. Resources are managed using SFA messages, both to discover and to reserve them.

Although SFA is an important initiative to create a federation of FI testbeds, it presents open issues related to A&A. Briefly, this occurs because its proposal is focused on interconnecting resources through a *resource federation*. The A&A ends up in background, composed only of a simple authentication mechanism based on X.509 certificates and static profiles.

Although we introduced SFA, this paper only addresses the authentication and authorization in VO. Therefore, algorithms and techniques of resource discovery and allocation are not our focus.