Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 110 (2017) 174–181

Procedia Computer Science

www.elsevier.com/locate/procedia

The 14th International Conference on Mobile Systems and Pervasive Computing
(MobiSPC 2017)

Spatial Connector: Mapping Access Control Models for Pervasive Computing and Cloud Computing

Ichiro Satoh[a]

[a]National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

Abstract

Services on pervasive computing are delegated or offloaded to cloud computing platforms, because pervasive computing devices have only limited resources. However, access control models in pervasive computing environments and cloud computing platforms are different, where the former tends to be context-dependent and the latter to be subject-based, e.g., role-based access control (RBAC). To connect such different models, we propose a framework for managing context-aware services executed at pervasive computing and cloud computing. The framework is constructed as a world model for specifying contextual information in the real world. This paper describes the design and prototype implementation of the proposed model.

Keywords: Access control model, context-awareness, cloud computing

1. Introduction

Mobile and pervasive computing devices are expected to provide rich services, e.g., context-aware services, but they have have only limited computational resources. To support services which are intensive tasks, they need to be delegated or offloaded to the external servers, e.g., cloud computing platforms. When such services are executed at servers on behalf of pervasive computing devices, we need to make the services to access computational resources from the servers under appropriate access controlling. However, the notion of security in pervasive computing is different from in cloud computing. In fact, access control models in most existing cloud computing platforms tend to be subject-centric in the sense that permissions are provided according to subjects, e.g., users. On the other hand, access control models for context-aware services tend to be context-dependent in the sense that *context* is the first-class principle that explicitly guides both policy specification and enforcement process and it is not possible to define a policy without the explicit specification of the context that makes policy valid. At a high level, the term context is

* Ichiro Satoh. Tel.: +81-3-4212-2546.
E-mail address: ichiro@nii.ac.jp

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.06.075

defined as any information that is useful for characterizing the state or the activity of an entity or the world in which this entity operates.

This paper proposes a framework for managing context-aware services executed at pervasive computing environments and cloud computing. It is used to pull back software from/to pervasive computing devices to/from cloud computing during an offloading action. It is constructed based on a world model for contexts in the real world. The model can activate/deactivate pervasive services in accordance with changes in the real world. It can also bridge between a context-centric access control model in a pervasive computing environment and subject-based access control models in cloud computing platforms. The framework enables context-aware services executed at cloud computing to access computational resources and information under an access control model for pervasive computing environments. Software for context-aware services should utilize the knowledge created by context providers accessible through a communication interface between programs running at pervasive computing devices and cloud infrastructures.

2. Related Work

This section briefly highlights several existing access models that have influenced our work with access control models for cloud computing and context-aware services.

Conventional access control models can be classified into three types: mandatory access control (MAC), discretionary access control (DAC), and role-based access control (RBAC)[5,7,12]. RBAC is an alternative to traditional approaches, i.e., DAC, and MAC. In RBAC, users are assigned roles and roles, are assigned permissions. The principle motivation behind RBAC is the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure.

In cloud computing, access control is one of the most important issues. Cloud computing is often characterized by its multi-tenancy and virtualization features. These features have unique security and access privilege challenges due to the sharing of resources among potential untrusted tenants. RBAC is a key technology for cloud computing platforms and is well-suited for multi-domain architecture; it is applicable in cloud systems that deal with health records, stock trading and pairing, and social networking. The RBAC model is used by many cloud computing platforms, e.g., Microsoft Azure and OpenStack. To achieve multi-tenancy in a single data storage system in cloud computing, several researchers proposed approaches to encrypt data before uploading the data to the cloud by using some cryptographic algorithms so that the data were protected from other tenants. Since access control models in cloud computing platforms are often imposed by the platforms, it is difficult to introduce other models into the platforms.

There have been several attempts to extend RBAC with the notion of context-awareness. By using the uniform notion of a role to capture both user and environmental attributes, our model enables the definition of context-aware security policies. Roles can also make it easy to define and understand complex security policies; adding environment roles to the model was necessary to support the advanced access control requirements that we are faced with in pervasive computing systems. However, RBAC approaches assume that permissions are first associated with roles, and subsequently subjects are assigned to roles. In context-aware services, permissions should first be associated with contexts, and subsequently subjects are associated with the contexts they are currently operating in. To solve these problems, Covington et al.[4] allow administrators to specify the environmental context through a new type of role called environmental role to generalize traditional RBAC. Their approach aimed to overcome the inherent subject-centric nature of RBAC. Georgiadis et al.[6] proposed a context-based term based on control by integrating RBAC and team-based access control (TMAC)[16].

There are mismatches between access control models in cloud computing and context-aware applications. Conventional security solutions, including RBAC, seem inadequate to control accesses to resources and interoperability among entities in cases of frequent context changes as we discussed in the first section. In fact, conventional subject-based access control systems exploit user identity or role information to determine the set of user permissions. Permissions are tightly coupled to the identity or role of the subject requesting a resource access, whereas context information can only further limit the applicability of the available permissions. However, context-aware services are often required to be provided in appropriate contexts. For example, electric lights in a room should be controlled by the people in the room instead of by anyone outside the room, even when the people are not registered. Our framework considers context as the primary basis rather than the subjects, e.g., the users. Therefore, access control models in pervasive computing systems tend to be different. Nevertheless, to offload intensive tasks from pervasive computing