Journal of Network and Computer Applications 38 (2014) 76–87

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A semantic authorization model for pervasive healthcare

Zang Li [a], Chao-Hsien Chu [a,b,*], Wen Yao [a]

[a] College of Information Sciences and Technology, The Pennsylvania State University, University Park, PA 16802, USA
[b] School of Information Systems, Singapore Management University, Singapore 179802, Singapore

ARTICLE INFO

Article history:
Received 26 October 2012
Received in revised form
16 May 2013
Accepted 10 June 2013
Available online 20 August 2013

Keywords:
Semantic access control
Authorization
RFID
Ontology
Pervasive healthcare

ABSTRACT

In this paper, we investigate how to secure sharing of complex data objects among pervasive information systems. To address the challenges posed by heterogeneous data sources, complex objects and context dynamics, we propose an advanced authorization model that supports specifying and enforcing authorizations in flexible and efficient ways. The model employs ontology and semantic web technologies to conceptualize data and explicitly express the relationships among concepts and instances involved in information sharing. Authorizations can be specified at different levels of the predefined concept hierarchies and be propagated to lower-levels. A novel decision propagation model is proposed to enable fast evaluation and updating of concept-level access decisions. To resolve conflicts among policies, we model a policy set as a semilattice, upon which a binary operation is defined to adapt to various requirements. Moreover, enabled by ontology reasoning tools, a flexible specification approach of authorization, namely rule-based policy generation, is developed to encode context dynamics, making the authorization enforcement adaptive to contexts.

1. Introduction

The adoption of the Electronic Health Record (EHR) and pervasive healthcare technologies have been viewed as a major step for the electronic healthcare (e-health) era. Under EHR, new care-related activities are provided via various applications such as evidence-based decision support, health information management, and outcomes reporting. With the development of pervasive healthcare systems, healthcare services become more efficiently and ubiquitously accessible; on the other hand, new expectations of pervasive access control have arisen accompanying with new paradigms of pervasive healthcare delivery. First, the protection object, healthcare data, is primarily data-centric rather than document-centric, and usually involves highly sensitive information such as patient medical histories, examination reports, radiology images, sophisticated equipment usage reports and blood bags tracking records, etc. Secondly, the pervasive healthcare information could be abused by corporations in deciding who should be promoted, by insurance companies in refusing coverage for people with poor health, and by spouses and their attorneys in divorce cases. Therefore, security threats that could expose medical information as well as personal privacy trigger the need for advanced access control models, which have to satisfy the following requirements:

(1) *Be enforceable over large-scale, distributed and heterogeneous systems*, while ensuring that the size of the policy repository is under control. It is expected that national integration would bring the pervasive healthcare system to a situation where a large volume of data records are shared and made available to a large number of users (Bilykh et al., 2003). Moreover, data sources maintained by these organizations are possibly syntactically and schematically heterogeneous, and user groups in these organizations have different role systems.
(2) *Be fine-grained over complex data objects.* An EHR is a complex object, composed of distributed sub-objects of different types of content, such as profile data, diagnosis reports, radiology images and so on. An access control system, dealing with such complex objects in a distributed environment, must ensure that different records and different portions of an EHR meet various protection requirements. For example, a patient's profile could be made available to every staff member of a hospital, whereas the medical records should be made available only to physicians and family members. Moreover, some sensitive elements of the medical records, such as HIV/AIDS diagnosis, should be hidden from general medical information during the sharing process, unless a special treatment option is indicated (Jin et al., 2009).
(3) *Be able to capture context dynamics and enforce context-aware authorizations.* Context, in our paper, is defined as any information used to characterize the situation of people and data objects.

* Corresponding author at: School of Information Systems, Singapore Management University, Singapore 179802, Singapore. Tel.: + 65 6828 0444; fax: + 65 6828 0919.
E-mail address: chchu@smu.edu.sg (C.-H. Chu).

1084-8045/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2013.06.006

Examples of context dynamics include: (a) any changes of relations, for example, patient can be assigned to different doctors in different curing stages; accordingly, some of the clinical data may not be available to previous doctor anymore but available to current doctor; (b) during emergencies doctors will be allowed to access all of patient's medical data and (c) changes of rules, for instance, research staffs are no longer able to access patients' clinical data after work or outside of hospitals. Obviously, it is impossible to update authorizations manually to respond to context dynamics, since thousands of people and data resources are involved in a pervasive healthcare system.

Example 1. Assume that in a small town there are two healthcare organizations: medical center and community clinic. They maintain different databases (*MCDS* for the medical center, *CCDS* for community clinic) and have different role structures. See Fig. 1.

The two data sources and database schemas—MCDS and CCDS—can be accessed in a pervasive healthcare system. If we have a requirement that "the doctors are allowed to view clinical data", then under the traditional access control system we define two schema-level policies

(1) (*Doctor*, */MCDS/DiagnosisFindings*, +), (*Doctor*, */MCDS/PhysicalExam*, +), (*Doctor*, */MCDS/HCDiagnosis*, +).
(2) (*Doctor*, */CCDS/DiagnosisReport*, +).

This method of policy specification on heterogeneous data sources adds burdens to the policy designers, as they have to be familiar with various database schemas. The authorization model needs to deal with distributed data records of different database types (e.g., relational vs. XML), schemas (structures and names) and even data types (radiology images vs. diagnosis text). Moreover, the advanced authorization model is required to capture context automatically and to enforce context-aware authorizations efficiently.

The contribution of our work is to propose an advanced authorization (access control) model that can address the aforementioned requirements in a systematic, flexible and efficient way. By applying ontology technologies, the proposed model, on the one hand, allows specifying, propagating, and computing authorizations over concept hierarchies in the abstract world, thus achieving benefits including: (a) structural heterogeneity across data sources is eliminated; (b) concept-data mapping can be conducted by local schema designers of data sources, so that policy designers working on a mediation server only need to develop authorizations over the ontology layer, rather than knowing syntactic structures of distributed data sources; and (c) the size of policy repository can be greatly reduced. On the other hand, enabled by ontology inference tools, the model is able to encode the authorization restrictions posed by the physical world, thus allowing the model to capture context dynamics and condition for the enforcements of context-aware authorizations, and define authorizations in a flexible way.

	Medical Center	Community Clinic
Database Schema	**DiagnosisFindings**(Patient, Test, Findings, Device, Date, DiagnosedBy) **PhysicalExam**(Skin, Eyes, MentalHR, Pulse, Organs) **HCDiagnosis**(Procedures, Date, DiagnosedBy, Report) **PersonalInfo**(Name, Gender, DoB, Address, InOut) **FamilyHistory**(MotherHR, FatherHR, SiblingsHR) **SocialHistory**(MaritalStatus, Occupation, DietaryPattern, DrugUse)	**DiagnosisReport**(Patient, Report, Time, Doctor, Equipment) **Patient**(Name, Birthday, Address, Sex)
User Group	MedicalStaff — ResearchStaff — Doctor — Nurse	MedicalStaff — Physician — Nurse — Pharmacist

Fig. 1. Data schemas and user groups.

2. Related works

There have been many research works focusing on securing information sharing across distributed information systems using different types of access control methods: discretionary access control (Jonscher and Dittrich, 1994), role based access control (RBAC) (Sandhu et al., 1996) and attribute-based access control (ABAC) (Bonatti and Samarati, 2000). These models cannot support specifying authorizations over abstract concepts and propagating authorization decisions in multi-dim hierarchies.

There are a few research works focusing on security framework of pervasive healthcare. Poulymenopoulou et al. (2012) proposed an access control framework for providing role-based context-aware authorization services with regard services invocation and patient information accesses; however this paper only considered authorization mechanism inferred by context information and it did not systematically state how to abstract and protect pervasive entities. Zhang and Liu (2010) described an EHR security reference model for managing security issues in healthcare clouds, which proposed important core components in securing an EHR cloud; however, this paper did not provide much detail on how to design and implement an access control model.

Recently, as XML becomes the most popular languages to facilitate the sharing of structured or semi-structured data across information systems, access control mechanisms for XML data sources has been investigated in a number of studies (Bertino et al., 2000; Damiani et al., 2002). Other notable XML extensions for security and privacy include Wang et al. (2004), Cranor et al. (2002), Ashley et al. (2003), Hughes et al. (2004), Kim et al. (2007). However, these models are inadequate for the protection of EHR information. One major reason is that EHR is a complicated object, of which segments are document-centric and distributed over many data sources; however the access of EHR is usually entity-centric (e.g., patient-centric). The models we discussed allow specifying authorizations in terms of document identifiers (or locations), rather than in terms of entities' identifiers and content types of EHR segments.

Some interesting access control models including Adam et al. (2002) and Qin and Atluri (2003) applying concept-level authorizations were developed. Pan et al. (2006) proposed a semantic access control enabler (SACE) to enable semantic access control on the Web. The system integrated heterogeneity resolution and access control into one process. Although we borrow the idea of conceptualizing objects and users from their works, our work is substantially different. The differences come from many aspects. The major one is that our model allows specifying two forms of semantic authorizations, including concept-level authorizations in the abstract world and context-aware authorization in the physical world. Another significant one is that our model allows defining concept hierarchies in multiple dimensions and employs decision propagation algorithms to efficiently compute final views for requestors.

Semantic web technologies have been recently used for modeling authorizations (Finin et al., 2013; Tonti et al., 2003). In Atallah et al. (2007), a semantic access control model was developed based on RBAC, where semantic web technologies are employed to resolve the heterogeneity among databases. In Carminati et al. (2009), users and resources in social networks are modeled as semantic web entities and ontology reasoned are employed to derive security rules. The last two models share the idea of using ontology to solve heterogeneities and conduct inference; however, their models do