Journal of Biomedical Informatics xxx (2013) xxx–xxx

Contents lists available at ScienceDirect

Journal of Biomedical Informatics

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

Evaluation of an Enhanced Role-Based Access Control model to manage information access in collaborative processes for a statewide clinical education program

Xuan Hung Le, Terry Doll, Monica Barbosu, Amneris Luque, Dongwen Wang *

University of Rochester Medical Center, Rochester, NY 14642, USA

ARTICLE INFO

Article history:
Received 25 June 2013
Accepted 15 November 2013
Available online xxxx

Keywords:
Access control
Information management
Computer supported cooperative work
Workflow
Medical education
Knowledge representation

ABSTRACT

Background: Managing information access in collaborative processes is a critical requirement to team-based biomedical research, clinical education, and patient care. We have previously developed a computation model, Enhanced Role-Based Access Control (EnhancedRBAC), and applied it to coordinate information access in the combined context of team collaboration and workflow for the New York State HIV Clinical Education Initiative (CEI) program. We report in this paper an evaluation study to assess the effectiveness of the EnhancedRBAC model for information access management in collaborative processes when applied to CEI.

Methods: We designed a cross-sectional study and performed two sets of measurement: (1) degree of agreement between EnhancedRBAC and a control system CEIAdmin based on 9152 study cases, and (2) effectiveness of EnhancedRBAC in terms of sensitivity, specificity, and accuracy based on a gold-standard with 512 sample cases developed by a human expert panel. We applied stratified random sampling, partial factorial design, and blocked randomization to ensure a representative case sample and a high-quality gold-standard.

Results: With the kappa statistics of four comparisons in the range of 0.80–0.89, EnhancedRBAC has demonstrated a high level of agreement with CEIAdmin. When evaluated against the gold-standard, EnhancedRBAC has achieved sensitivities in the range of 97–100%, specificities at the level of 100%, and accuracies in the range of 98–100%.

Conclusions: The initial results have shown that the EnhancedRBAC model can be effectively used to manage information access in the combined context of team collaboration and workflow for coordination of clinical education programs. Future research is required to perform longitudinal evaluation studies and to assess the effectiveness of EnhancedRBAC in other applications.

1. Introduction

1.1. Objective

Managing information access is a critical requirement to team-based biomedical research, clinical education, and patient care [1–7]. Effective information access depends on specific context of workflow and particular requirements of team collaboration [8–19]. We have developed a computation model through enhancement of Role-Based Access Control (RBAC) to support information access management in collaborative processes [20,21]. This model (hereafter referred to as EnhancedRBAC) can facilitate definition and enforcement of detailed, precise policies for data access, such that specific information can be shared among the members of a collaborative team in particular contexts of workflow and meanwhile its access by other irrelevant parties is restricted. In papers published previously, we described the EnhancedRBAC model and its implementation [20,21]. To examine the effectiveness of this approach to managing information access, here we report the details of an evaluation study to apply EnhancedRBAC to New York State (NYS) HIV Clinical Education Initiative (CEI) [22]. This evaluation study provides a first set of quantitative measures on effectiveness of the EnhancedRBAC model, using the CEI application as a specific example. In addition to these quantitative measures, we discuss qualitative evaluation metrics related to this case study based on guidelines proposed by others [23,24]. Although this particular research was driven by clinical education, our broader goal is to incrementally develop a generalizable system framework for information access management in collaborative processes such that we can apply this system framework to various applications for biomedical research, clinical education, and patient care.

* Corresponding author. Address: University of Rochester Medical Center, 601 Elmwood Avenue, Box 630, Rochester, NY 14642, USA. Fax: +1 585 273 1031.
E-mail address: dongwen_wang@urmc.rochester.edu (D. Wang).

1532-0464/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jbi.2013.11.007

1.2. Information access management, EnhancedRBAC, and system evaluation

Access to the right information in specific context is an essential requirement to biomedical research [3,5,8,12,14], patient care [1,2,4,7,9–11,17–19], and clinical education [6,22]. Various information systems have been developed and utilized in different scenarios to support information access management. For their optimal use, these systems need to be carefully designed to integrate with the application context [8–19]. Facilitation of information management in such context is a key element to provide appropriate level of information access, to improve team collaboration, and to enhance process management through the underlying information systems.

Previous research has proposed various information access control models [25–29]. These models can provide a general structure to define access policies and to enforce such policies in specific scenarios of information access. Yet few of these models have addressed information access management in the combined context of team collaboration and workflow. With regard to specific applications supporting access control, many have been developed for patient care [1,2,9–11,18,30–40] and biomedical research [8,12,14,15,41,42], but none of the previous works have been utilized to coordinate clinical education programs in collaborative workflow. To address these specific needs, we have proposed the EnhancedRBAC model to support information access management in collaborative processes [20,21]. For this purpose, we have: (1) formulated universal constraints to bind on user-role assignments, role-permission assignments, and access permissions, (2) defined bridging entities and contributing attributes to support access management in collaborative environment, (3) extended access permissions to include workflow context, and (4) synthesized a role-based access delegation model targeting on specific objects to balance between flexibility and need-based access. These constructs can be utilized to define policies for information access in specific domains and applications. Using the policies defined in the EnhancedRBAC model and the tools developed to interpret them, this system framework can be used: (1) to evaluate individual cases and scenarios of information access against the policies, and (2) to decide whether to grant or to deny access to specific information resources in collaborative workflow. We have developed formal representations of EnhancedRBAC in first order predicate logic and eXtensible Access Control Markup Language (XACML) [43]. We have implemented and adopted tools to encode and to interpret access control policies based on EnhancedRBAC [21]. Additional technical details of the EnhancedRBAC model and the associated tools for implementation can be found in previous papers [20,21].

With regard to evaluation of access control systems for biomedical applications, few studies have been reported in the literature. Fernandez-Aleman et al. reviewed the security and privacy mechanisms used in electronic health records, including features such as access control models, general approaches for access management, and emergency access [44]. Nevertheless, few details were available on evaluation of these systems. Hu et al. proposed guidelines for evaluation of access control systems with a set of evaluation metrics, concentrating mainly on qualitative measures [23,24]. In addition to these qualitative measures, the widely accepted metrics for evaluation of biomedical information systems are quantitative measures on system effectiveness, such as accuracy of diagnoses or correctness of clinical decisions generated by systems when compared with the ground truth [45]. For the study reported in this paper, our primary focus is the quantitative measures on effectiveness of EnhancedRBAC when applied to CEI (see details in Section 2). In Section 4.3, we select a set of qualitative metrics proposed by Hu et al. [23,24] and discuss the specific features related to EnhancedRBAC.

1.3. New York State HIV Clinical Education Initiative

Development of EnhancedRBAC was driven by the NYS HIV CEI program [22]. CEI is sponsored by the NYS Department of Health AIDS Institute. It has been engaging in HIV clinical education for two decades to address the education needs of community healthcare providers, aiming to disseminate the latest clinical knowledge and to improve HIV patient care. The CEI program has created multiple training centers, including: (1) Mental Health Center (MHC); (2) Prevention and Substance Use Center (PSUC); (3) Testing, Post-Exposure Prophylaxis, and Diagnosis Center (TPDC); and (4) Clinical Education Center for Upstate Providers (CECUP), which can be further segmented into Albany Medical Center (AMC), University of Rochester Medical Center (URMC), and Erie County Medical Center (ECMC) catchment areas. Each of these centers is in charge of a range of educational activities based on the training topics, training formats, and geographical locations (see Fig. 1). In every day operation, a specific CEI training session may require expertise and resources from multiple CEI Centers. Thus, coordination and collaboration among the CEI Centers is critical. In terms of information access, the CEI project requires to grant access permissions to staff from specific CEI Centers collaborating on a particular training session, such that they can review the relevant data and to coordinate the training activities. For staff from the other CEI Centers not directly involved in the collaboration, access permissions should be denied to ensure data confidentiality and to reduce information overload. With regard to workflow, a specific training session typically consists of several stages that progress forward in a sequence: training requested by an agency (*request-received*), CEI staff calling back and training arrangement pending (*arrangement-pending*), scheduling of training (*training-scheduled*), and completion of training (*training-completed*). In certain scenarios, for example, when the target audiences are not clinicians, CEI will not directly provide training (*unable-to-arrange*) but instead refer those requests to other training programs. From the perspective of information access management, CEI posits a set of complex requirements. For example, if 'Catholic Health Systems', a healthcare organization located in Buffalo area, has just requested (workflow status 'request-received') an onsite training on topic 'HIV testing', both 'Mary', a staff from 'CECUP-ECMC', and 'Paul', a staff from 'TPDC', should be granted access to this request such that they can review the request details ('read' access) and document communications for training arrangement ('write' access); and meanwhile access to this request by 'David', a staff from 'PSUC', should be denied. This is because: (1) according to the access policies based on training formats, topics, and geographical locations, CECUP-ECMC and TPDC are the two collaborating CEI Centers for this training request while PSUC has no responsibility to participate; and (2) according to another policy (Policy-3b), any collaborating CEI Center can document the communications related to a newly-received training request.

To manage training information and to support collaboration among CEI Centers in specific context of workflow, we have developed the CEIAdmin system. Information access management in CEIAdmin is implemented in an ad hoc approach with hard-coded logic, which cannot be easily changed (need to rewrite the code that will likely interfere with other functions of the system) and consistently managed (the logic may scatter around in different places of the system). In contrast, information access management in EnhancedRBAC is based on standard, centralized access policies that can be flexibly defined, updated, and enforced by specific application requirements. For this evaluation study, we defined access policies for the CEI project with the EnhancedRBAC model (see Fig. 2 for a specific example to encode Policy-3b as a universal constraint) [20]. We then implemented these policies through the EnhancedRBAC system framework (see Fig. 2 for application of

Please cite this article in press as: Le XH et al. Evaluation of an Enhanced Role-Based Access Control model to manage information access in collaborative processes for a statewide clinical education program. J Biomed Inform (2013), http://dx.doi.org/10.1016/j.jbi.2013.11.007