Development of a System Framework for Implementation of an Enhanced Role-Based Access Control Model to Support Collaborative Processes

Xuan Hung Le, PhD; Dongwen Wang, PhD
University of Rochester Medical Center, Rochester, NY 14642

Abstract

We previously developed an enhanced Role-Based Access Control (RBAC) model to support information access management in the context of team collaboration and workflow. We report in this paper a generic system framework to implement the enhanced RBAC with three functional layers: (1) encoding of access control policies; (2) interpretation of the encoded policies; and (3) application of policies to specific cases and scenarios for information access management. Based on this system framework, we have successfully applied the enhanced RBAC model to the New York State HIV Clinical Education Initiative (CEI) for coordination of clinical education programs. An evaluation has shown that the enhanced RBAC can be effectively used for information access management in collaborative processes. Future work includes extension of this system framework to support the continuous development of the enhanced RBAC and deployment of it to other domain applications for clinical education, biomedical research, and patient care.

Keywords: Access control, computation model, information management, computer supported cooperative work, workflow, medical education

1 Introduction

Patient care, biomedical research, and clinical education depend on coordination and collaboration among partners from multiple disciplines in specific workflow contexts [1-7]. Information systems can be effectively used to facilitate team collaboration and workflow management [3, 5-15]. To develop information systems to present the right information to the right people at the right time, information access control is a critical requirement.

We previously developed an enhanced Role-Based Access Control (RBAC) model [16] to facilitate information access management in the context of team collaboration and workflow. Once the access policies are defined for specific applications based on the enhanced RBAC, we need to implement them to ensure that these policies are correctly interpreted and applied such as to grant particular users in certain roles the appropriate scope and level of access to the right information in specific workflow context to support team collaboration.

Many previous efforts on implementation of access control were based on an ad hoc approach pertinent to only specific applications [17-19]. In order to generalize to multiple domains, it is essential to develop a system framework for implementation of the core components of an access control model that are independent of specific applications. This approach was used by a few research to implement some well-defined access control models [20-22]. Since the enhanced RBAC model is unique in several aspects (for example, structures used to define the context of team collaboration and workflow) [16], its implementation needs to address these special challenges.

In this paper, we report the development of a system framework for implementation of the enhanced RBAC model. This system framework includes three functional layers: (1) encoding of information access control policies; (2) interpretation of the encoded policies; and (3) application of the policies to specific cases and scenarios for information access management. With these functional layers, the system framework can provide a flexible platform to develop and to implement policies for information access management in collaborative processes. To support management of information access, to simulate application of access control policies, and to present the access permissions in specific cases and scenarios, we have developed a demonstration tool with two primary functions: (1) selecting the combinations of users, roles, objects, operations, and workflow statuses; and (2) displaying the associated constraints and access permissions. We will use the New York State HIV Clinical Education Initiative (CEI) [18] as a specific example to illustrate the use of this system framework for implementation of information access control policies to facilitate collaborative processes.

The remainder of this paper is organized as follows. We first review the enhanced RBAC model in Section 2. We then provide an overview of the system architecture in Section 3. We describe the use of this system framework for access control policy encoding and interpretation in Section 4 and 5. We present a case study to apply the

enhanced RBAC model to the CEI project in Section 6. We report the development of the demonstration tool in Section 7. We highlight the findings from an evaluation study in Section 8. We discuss the contributions, limitations, and directions of future work in Section 9. We conclude the paper in Section 10.

2 Overview of the Enhanced RBAC

Previous research have proposed various access control models, such as Access Matrix [23], Rule-Based Access Control [24], Discretionary Access Control (DAC) [25], Mandatory Access Control (MAC) [25], Attribute-Based Access Control (ABAC) [26], Role-Based Access Control (RBAC) [27], and many others [19-22, 28-50]. Yet few of these works have addressed information access management in the context of team collaboration and workflow; neither have them been applied for coordination of clinical education programs. To address these specific needs, we have proposed the enhanced RBAC model [16] to support information access management in collaborative processes. The enhanced RBAC model [16] extends the core RBAC [51] through: (1) formulation of specific types of *universal constraints* to bind on user-role assignments, role-permission assignments, and access permissions; (2) definition of *bridging entities* and *contributing attributes* to support access management in collaborative environment; (3) extension of access permissions to include *workflow* context; and (4) synthesis of a *role-based access delegation* model targeting on specific objects to balance between flexibility and need-based access. In particular, we use the universal constraints to bundle the bridging entities, contributing attributes, and workflow contexts. These universal constraints are applied not only to restrict users' access but also to support team collaboration and workflow management (see [16] for details).

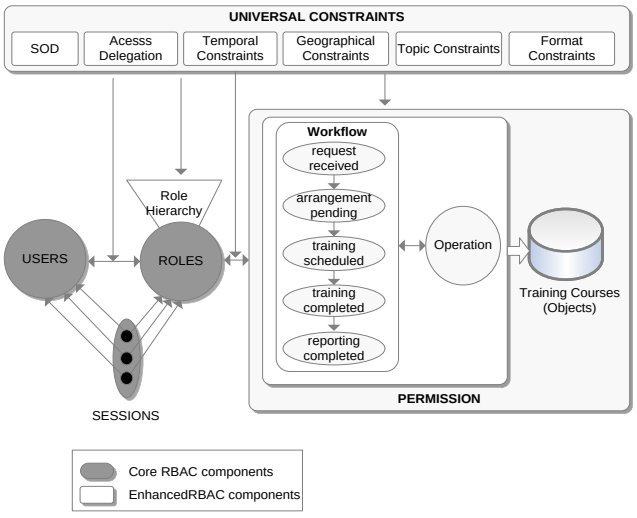

Figure 1. The enhanced RBAC Model

As shown in Figure 1, the enhanced RBAC model is comprised of six classes of elements: (1) users, (2) roles, (3) permissions, which can be further decomposed into: (4) objects, (5) operations, and (6) workflow statuses. With the inclusion of the workflow context into the enhanced RBAC model, we can define access permissions based on individual or classes of workflow stages. Through the introduction of universal constraints, we can define access policies to share information among collaborating parties with the bridging entities and contributing attributes. For example, we have defined *temporal constraint* for the CEI project to regulate information access at specific stages of training workflow; in addition, we have defined *geographical constraint*, *topic constraint*, and *format constraint* to facilitate information sharing among collaborating training centers based on location, content, and format of a training session. It is important to note that the universal constraint is an open, configurable structure. Additional types of constraints can be included to meet certain application requirements without breaking the core RBAC structure. Detailed descriptions of the enhanced RBAC can be found in a previous paper [16].

3 System Architecture

To implement the enhanced RBAC model, we designed a system architecture with three layers: (1) Policy Encoding Layer, where policies regarding information access control for a specific application can be defined; (2) Policy Interpretation Layer, where the encoded access policies are interpreted based on specific combinations of users, roles, objects, operations, and workflow statuses as well as the universal constraints bound on them; and (3) Access Control Application Layer, where the encoded access control policies are applied to specific cases or scenarios to make decisions on granting or denying access.

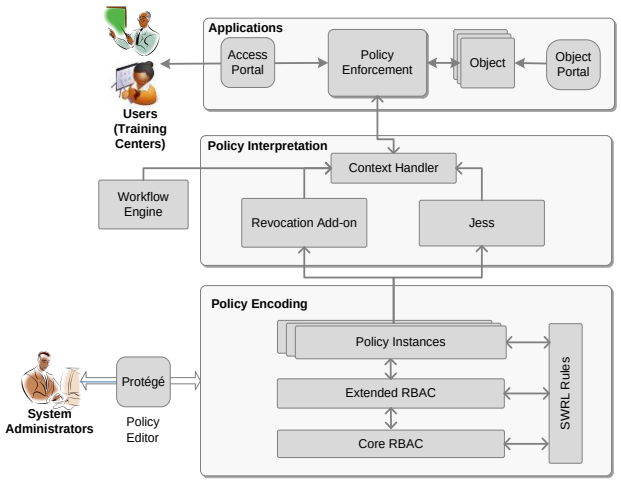

Figure 2. System Architecture

As illustrated in Figure 2, these three layers are functioning independently but meanwhile closely integrated to each other through information flows. Specifically, Layer (1) is where the system administrators specify access control policies through a policy editor. The outputs from this process are the encoded policies that are fed to Layer (2) once they are validated. Layer (2) is where the encoded policies are interpreted in specific application contexts. During this process, it requires particular application contextual information that comes from Layer (3). The results of policy interpretation in Layer (2) are then fed to Layer (3), where decisions on granting or denying access to specific cases and scenarios are made. To support policy encoding with the continuous development of the enhanced RBAC model, we have employed a three-level encoding schema to differentiate the core RBAC model, the model extension, and the policy instances. To interpret the encoded policies, we have leveraged a Java-based rule engine that can directly retrieve and process the encoded access policies from the policy encoding layer. To handle the workflow management, we assume there is an external workflow engine that can be integrated with the policy interpretation layer. Finally, the application layer implements system interfaces to retrieve application contextual information such as users, roles, objects, and operations. We describe the details of each layer in the following sections.

4 Encoding of Access Control Policies

To encode access control policies, we adopted an existing tool, Protégé (version 3.4.7) [52], as the editor. Protégé provides a flexible platform and a rich technical environment for knowledge acquisition and ontology development. We selected it as the editor mainly because of three reasons: (1) it supports a layered approach for model definition, which is helpful for continuous development of the enhanced RBAC model; (2) it differentiates ontological models from instances, which is a nice feature to support the development of the general enhanced RBAC model and the implementation of the specific access control policies when applied to particular domains and problems; and (3) it incorporates many add-ons, in particular, the Semantic Web Rule Language (SWRL) [53, 54] and the JESS rule engine [55, 56], which can be adopted for encoding and interpretation of the universal constraints.

Encoding of specific access control policies is based on the enhanced RBAC model. To build the enhanced RBAC in Protégé, we employed a two-level structure, with the core RBAC model as the basis and the extended model encoded on top of it. The core RBAC schema defines five basic components of the RBAC model, including *users*, *roles*, *permissions*, *operations*, and *objects*. The extended model

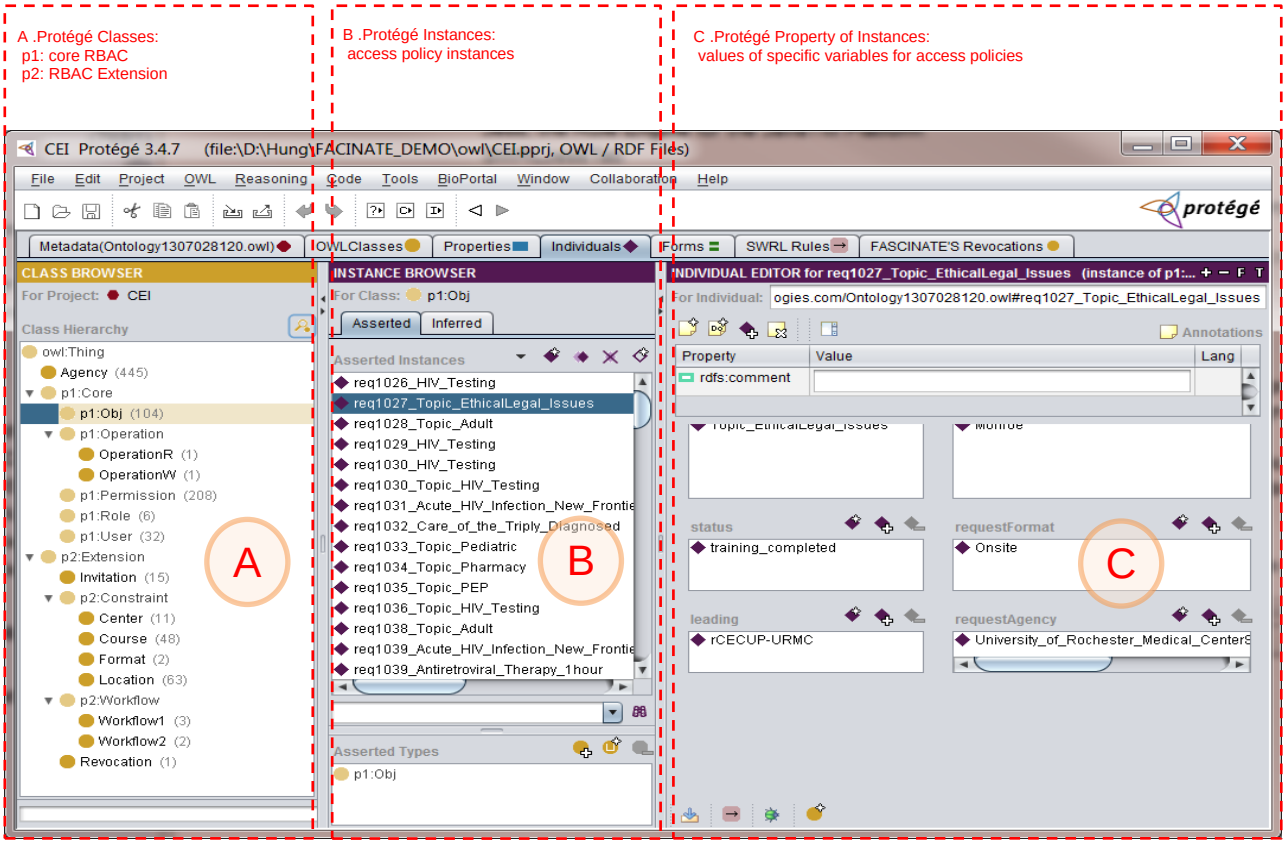

Figure 3. Three-Level Access Control Policy Encoding in Protégé

integrates additional representation elements such as *universal constraints*, *workflow statuses*, and constructs that are used for access delegation and revocation. With this two-level structure, we can easily support the continuous development of the enhanced RBAC model, for example, through defining new types of universal constraints. Once the enhanced RBAC is built, we can encode access control policies as instances of particular model elements. These policies can be grouped together based on individual or classes of applications. Figure 3 is a screenshot of using the Protégé tool to encode the enhanced RBAC model and the access control policy instances for the CEI project.

When defining access control policies for specific applications, we typically encode these policies as universal constraints. In the enhanced RBAC model, the *universal constraints* are defined in first-order predicate logic [16]. To encode these constraints in Protégé, we adopted a Protégé add-on [57] that incorporates a SWRL editor and a JESS rule engine for rule execution. A SWRL rule contains an antecedent part, which is referred to as the body of the rule, and a consequent part, which is referred to as the head of the rule. An example of an access control policy from the CEI project is shown in Figure 4(a). Translated into English, it means:

For any:

role (training center) `r`, training request `req`, workflow status w_i, operation `write`, training course `course`, training format `format`, agency `agency`, and location `loc`

If:

(1) the training request `req` is in workflow status w_i;
(2) the agency `agency` makes a training request `req` on training course `course` in training format `format`;
(3) the agency `agency` is at location `loc`;
(4) the role (training center) `r` is in charge of location `loc`;
(5) the role (training center) `r` is in charge of training course `course`; and
(6) the role (training center) `r` is in charge of training format `format`

Then:

The role (training center) `r` should have '`write`' permission to training request `req` in workflow status w_i.

Once encoded in SWRL through Protégé, this rule will be in the format shown in Figure 4(b).

Here the arguments in the rule, such as `?req` and `?course`, are directly mapped to the related classes (model elements) in Protégé and their instances can be easily retrieved by a rule engine for interpretation.

5 Interpretation of Access Control Policies

As described in Section 4, access control policies are encoded as SWRL rules. To interpret these policies, we use the JESS engine for rule execution. JESS is a rule engine and scripting environment written in Java programming language [55]. It is small, light-weight, and fast. JESS is a mature system that has been used to develop a broad range of applications [58-61]. It has already been integrated with Protégé and SWRL [57].

$\forall r \in ROLE, \forall req \in REQUEST, \forall w_i \in WORKFLOWSTATUS_I, \forall op_w \in OPERATION_{WRITE}, \forall course \in COURSE, \forall format \in FORMAT, \forall agency \in AGENCY, \forall loc \in LOCATION:$

$role\text{-}permission(r, req, w_i, op_w) \leftarrow$

$status(req, w_i) \wedge$ (1) bridging entity
$request(req, course, format, agency) \wedge$ (2) bridging entity

$location(agency, loc) \wedge$ (3) bridging entity
$inChargeLocation(r, loc) \wedge$ (4) geographical constraints
$inChargeCourse(r, course) \wedge$ (5) topic constraints
$inChargeFormat(r, format)$ (6) format constraints

(a) in first-order predicate logic

```
p1:rolePermission(?r,?p) ←
workflow1(?w) ∧
permissionRequest(?p,?req) ∧
permissionOperation(?p,?op) ∧
permissionStatus(?p,?w) ∧
operationW(?op) ∧

status(?req,?w) ∧                                   (1)
requestCourse(?req,?course)
    ∧ requestFormat(?req,?format)
    ∧ requestAgency(?req,?agency) ∧                 (2)
agencyLocation(?agency,?loc) ∧                      (3)
inChargeLocation(?r,?loc) ∧                         (4)
inChargeCourse(?r,?course) ∧                        (5)
inChargeFormat(?r,?format)                          (6)
```

(b) in SWRL

Figure 4. An Example of Access Control Policy for CEI

For a specific SWRL rule, the JESS engine can map its arguments directly to the corresponding Protégé classes, retrieve the instances under these classes, apply the logic of the SWRL rule, and generate new instances (typically user-role assignments and role-permission assignments) as the consequence of the execution. With these instances of user-role assignments and role-permission assignments, we can judge whether a specific user should be assigned to a particular role; we can also decide whether a specific role should have access to a particular object at certain stages of workflow with a distinctive operation. This entire process of argument mapping, rule interpretation, and new instance generation is built together as Protégé add-ons.

A limitation of SWRL and JESS is that they only support monotonic reasoning and hence cannot delete existing instances in Protégé. This presents a challenge to interpretation of access control policies when access revocation is required (and thus need to delete specific instances of role-permission assignments). To address this issue, we have developed a separate Protégé add-on that is specifically used for access revocation. This Protégé add-on searches and removes all relevant instances when interpreting a rule to revoke access permissions.

6 Application Layer

The application layer is where the access control policies are applied to specific cases and scenarios to make decisions on granting or denying access. This layer includes four major components: (1) a policy enforcement module, (2) an access portal, (3) an object portal, and (4) an object storage (see Figure 2). The access portal provides an interface for system users in particular roles. The policy enforcement module is linked with the policy interpretation layer to make decisions to grant or to deny access based on users, roles, objects, workflow statuses, operations, and constraints. The object portal provides a mechanism to generate new objects and to retire old objects. Once an object is generated, it stays in the object storage, where the policy enforcement module can search based on criteria defined in universal constraints. It is important to note that the specific functions and procedures defined at this layer may differ from application to application.

We use the CEI project [18] as an example to illustrate the functions of the components at the application layer. As a New York State sponsored clinical education program, CEI is targeting on agencies (hospitals, clinics, community healthcare centers, etc.) that provide healthcare to HIV patients. Since the New York City metropolitan area and the Upstate New York region have very different needs in HIV clinical education, CEI differentiates its training programs based on training topics, geographical areas, and training formats (in-person training vs. online program). For this purpose, CEI has sponsored three special topic training centers: (1) Testing, Post-Exposure Prophylaxis, and Diagnosis Center (TPDC), (2) Prevention and Substance Use Center (PSUC), and (3) Mental Health Center (MHC). These centers are in charge of their respective training topics for the entire New York State. In addition, CEI has sponsored a Clinical Education Center for Upstate Providers (CECUP), which is in charge of all training topics for the agencies located in the Upstate New York region. Beyond the in-person training programs, the CEI is engaging in online education through its Technology Center (TC). Thus, for a specific training session, multiple training centers may need to work collaboratively to contribute their resources and expertise in order to deliver the training service. Here each training center's contribution depends on the topic, location, and format of that training session. To manage information access in this context, those training centers participated in collaboration for a specific training session need to have shared access to the information for that training session, while the other centers not directly involved in the collaboration should not have access. The collaboration model is shown in Figure 5. In terms of training workflow, the entire lifecycle of a CEI training session includes five stages: *request received*, *arrangement pending*, *training scheduled*, *training completed*, and *reporting completed*. The level of information access among the collaborating training centers may change at different stages of a training session. Thus, the access control policies need to be defined based on individual or classes of workflow stages (see Figure 1). When applying the access control policies to a specific case and scenario, we need to manage the change of access permissions along the training workflow through the underlying access control system.

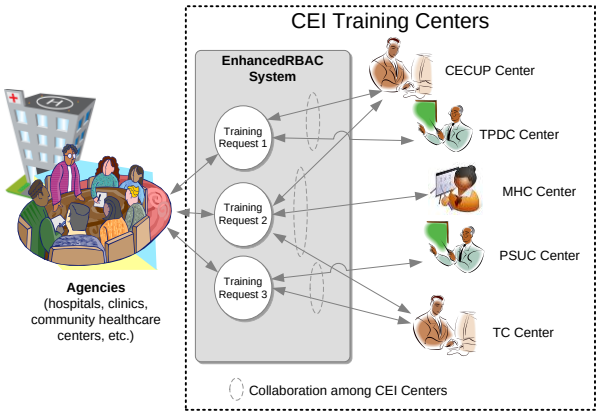

Figure 5. Collaborations in CEI

To apply the enhanced RBAC model to CEI for information access management, we mapped the components of the enhanced RBAC to specific entities in the CEI program. These mappings include: (1) training session ←→ object, (2) training center ←→ role, (3) employee of a training center ←→ user, and (4) stage of a

training session ←→ workflow status. We defined two types of operations, 'read' (reviewing training data) and 'write' (documenting training activities, inviting other centers for collaboration, etc.). Through the access portal and object portal, we imported the CEI program data for the period between April 1, 2011 and June 30, 2011, including 409 agencies, 104 training sessions, 17 users (employees), 6 roles (training centers), and 44 user-role assignments. These data are transformed as Protégé instances. Through the policy enforcement module and the execution of the universal constraints encoded as SWRL rules, we can generate all role-permission assignments that define the level of access to specific training sessions by particular training centers in certain stages of training workflow. We report the findings from an evaluation study in Section 8.

7 Demonstration Tool

We have developed a demonstration tool for two purposes: (1) to provide a user interface to support the management of information access; and (2) to present access permissions under specific combinations of users, roles, objects, operations, and workflow statuses. We implemented this tool as a Java application, with a screenshot shown in Figure 6. The user interface of the demo tool includes four portions: (1) Portion A: lists of all available users, roles, objects, and workflow statuses; (2) Portion B: selections of specific users, roles, objects, and workflow statuses for examinations of information access management; (3) Portion C: execution results after applying the access control policies defined in the enhanced RBAC to the selected users, roles, objects, and workflow statuses; and (4) Portion D: execution traces and system logs. Here items in Portion B are a subset selected from Portion A. Once the items in Portion B are selected, we can click the "run" button to generate the results in Portion C. These results include: (1) all validated predicates (relations among users, roles, objects, operations, workflow statuses, and other entities) defined in the system; (2) all validated user-role mappings and role-permission mappings; and (3) assignments of permissions to users under specific roles at particular workflow stages. With these functions, the demo tool can be effectively used to examine access permissions in specific cases and scenarios.

8 Highlights of Results from an Evaluation

To evaluate the effectiveness of using the enhanced RBAC model for information access management in collaborative processes, we implemented the model with the system

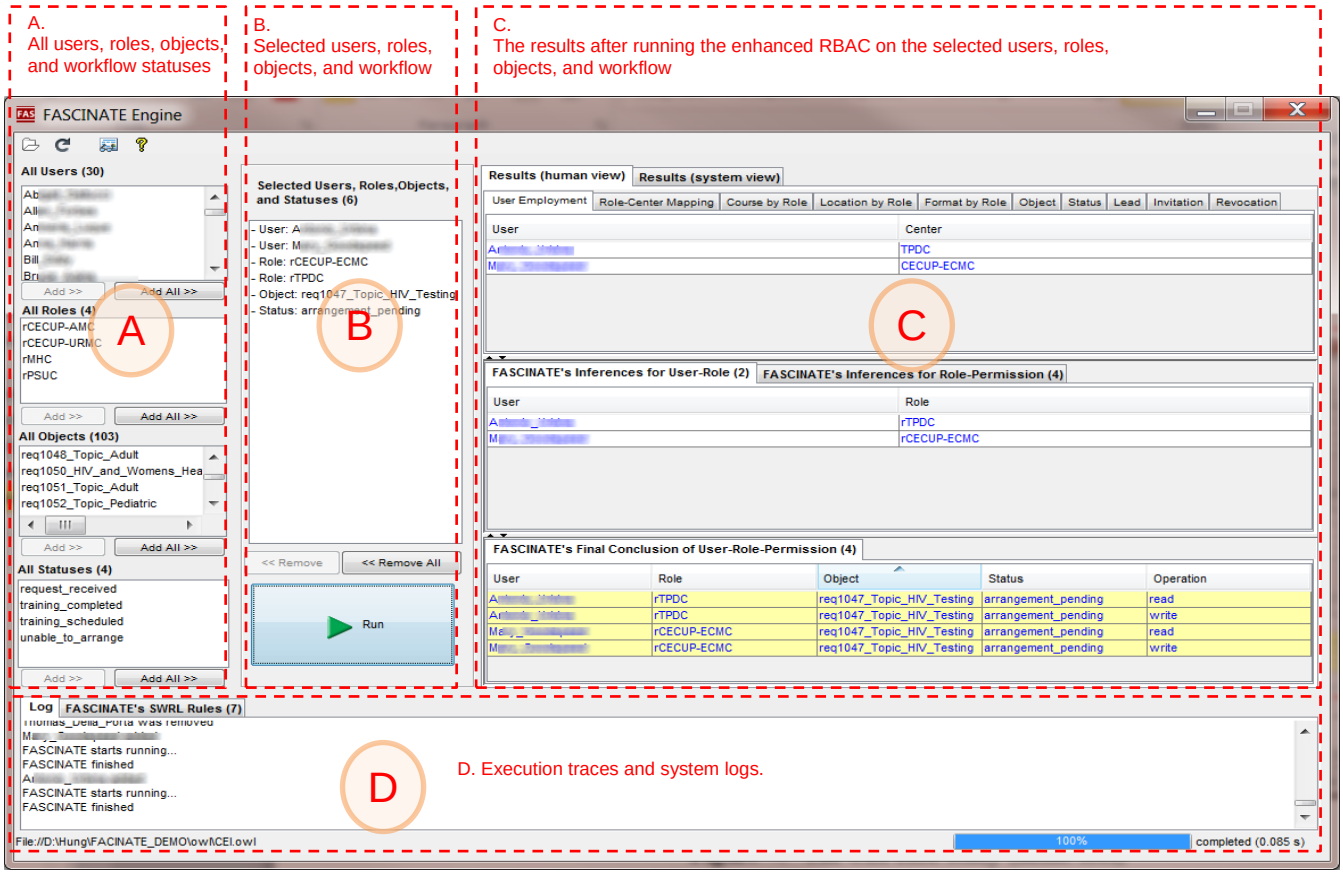

Figure 6. A Screenshot of the Demo Tool Showing Access Management for CEI

framework described above and applied it to the CEI project. We designed a cross-sectional study [62] with 9152 study cases and performed two sets of measurements: (1) degree of agreement between the results generated by the enhanced RBAC and those generated by a control system (CEI Admin [16]) in production use; and (2) performance of the enhanced RBAC based on a reference standard developed by a human expert panel. With the kappa [62] value in the range of 0.80-0.89, the enhanced RBAC has demonstrated a high level of agreement with the control system. When evaluated against the reference standard, the enhanced RBAC model has achieved sensitivities in the range of 97%-100%, specificities at the level of 100%, and accuracies in the range of 98%-100%. Error analyses have shown the imperfect sensitivity was due to mistakes in preparing invitation data for the study cases to feed the enhanced RBAC. Additional details of this evaluation study can be found elsewhere [63].

9 Discussion

Using a layered approach to implement access control policies have been reported by others [8, 33, 45, 64]. For example, implementation of the eXtensible Access Control Markup Language (XACML) [64] was based on a series of function modules/points such as Policy Administration Point (PAP), Policy Decision Point (PDP), Policy Enforcement Point (PEP), and Policy Information Point (PIP). However, the early versions of XACML did not provide native support to RBAC. Even the specialized XACML profiles were not able to support many relevant constraints. To address this issue, there was a previous exploration to introduce XACML+OWL, a framework that integrates OWL ontologies and XACML policies, to support RBAC [65]. In our implementation of the enhanced RBAC, the system framework and its functional layers can be mapped to many functional modules in XACML implementation. Specific mappings include: the Protégé environment in the enhanced RBAC is functioning as PAP; the JESS engine and revocation add-on are functioning as PDP; the policy enforcement module in Application Layer is functioning as PEP; and the Access Portal and Object Portal in Application Layer are functioning as PIP. Beyond the standard XACML implementation, we have defined unique structures in the enhanced RBAC system framework. These structures including: (1) an external workflow engine to manage workflow context; (2) a three-level schema for definition of access control policies to differentiate the core RBAC, the extension of RBAC, and the policy instances; and (3) specific entities and relations defined for particular applications, which are processed through the Context Handler. The mappings between the functional components of the enhanced RBAC system framework and the standard XACML implementation are shown in Figure 7. Here the integration with an external workflow engine in (1) can support access management in specific context of workflow, which is an enhancement of the core RBAC model. The three-level schema for definition of access control policy in (2) can facilitate the continuous development of the enhanced RBAC model. The application-specific entities and relations defined in (3) can custom-tailor the system framework to particular domain applications for effective implementation of access control policies. These features define the unique contributions of this work.

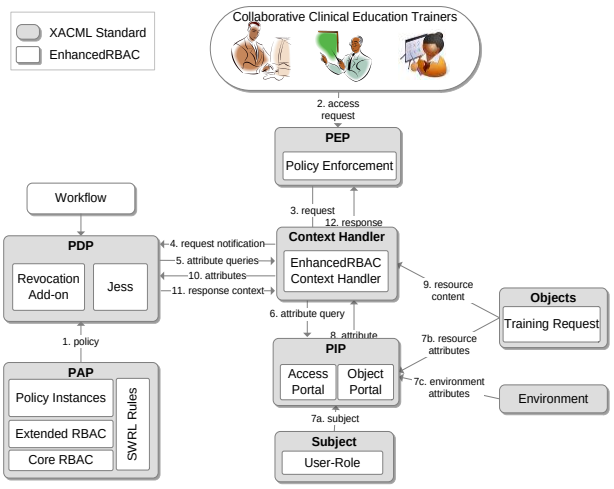

Figure 7. Mapping the enhanced RBAC Framework to XACML

To manage information access for team collaboration, we have defined bridging entities and contributing attributes [16] and incorporated these concepts as specific types of universal constraints. From the CEI project, we have developed geographical constraints, training topic constraints, and training format constraints to model specific types of contributing attributes. Additional types of universal constraints can and will be identified from other applications. Many types of universal constraints (including the ones identified from the CEI project) can be generalized and applied to a group of similar applications. As a long term goal, we plan to assemble these constraints to formulate a UNIversal Constraint ONtology (UNICON), which can be utilized as a knowledge base to drive information access management in a variety of situations [16]. Since Protégé is an ontology development tool, its incorporation into the system framework for the enhanced RBAC implementation will effectively support this long term goal.

To leverage the reported system framework to implement the enhanced RBAC model, we used the CEI project as a specific example. Since CEI has complex requirements on information access in the context of team collaboration and workflow management, it is a perfect selection to examine the feasibility of this system framework for effective implementation of the enhanced RBAC model. Meanwhile, the generalizability of the system framework for

implementation of the enhanced RBAC model needs to be tested in other applications. Our future work includes applications of this system framework for additional domain problems in clinical education, biomedical research, and patient care.

10 Conclusion

We have successfully developed a system framework to implement the enhanced RBAC model for information access management in collaborative processes. An initial evaluation has shown that this system framework can be effectively used for coordination of clinical education programs and to manage information access in the context of team collaboration and training workflow. Future work includes extension of this system framework to support the continuous development of the enhanced RBAC model and deployment of it to other domain applications for clinical education, biomedical research, and patient care.

Acknowledgment:

The CEI project is sponsored by the New York State Department of Health AIDS Institute. We would like to thank the other CEI team members at the University of Rochester Medical Center (Dr. Amneris Luque, Terry Doll, Monica Barbosu, and Thomas Della Porta) for their contributions to develop the CEI Admin system and to evaluate the enhanced RBAC model. We would also like to thank CEI program staff (Howard Lavigne, Dr. Cheryl Smith, Lyn Stevens, Dr. Bruce Agins) and colleagues from other CEI Training Centers for their support.

References

[1] B. J. Nijhuis, H. A. Reinders-Messelink, A. C. de Blecourt *et al.*, "A review of salient elements defining team collaboration in paediatric rehabilitation," *Clin Rehabil,* vol. 21, no. 3, pp. 195-211, Mar, 2007.

[2] J. Maas, W. Kamm, and G. Hauck, "An integrated early formulation strategy--from hit evaluation to preclinical candidate profiling," *Eur J Pharm Biopharm,* vol. 66, no. 1, pp. 1-10, Apr, 2007.

[3] J. Kunzi, P. Koster, and M. Petkovic, "Emergency access to protected health records," *Stud Health Technol Inform,* vol. 150, pp. 705-9, 2009.

[4] C. Lovis, S. Spahni, N. Cassoni *et al.*, "Comprehensive management of the access to the electronic patient record: towards trans-institutional networks," *Int J Med Inform,* vol. 76, no. 5-6, pp. 466-70, May-Jun, 2007.

[5] A. Ferreira, A. Correia, A. Silva *et al.*, "Why facilitate patient access to medical records," *Stud Health Technol Inform,* vol. 127, pp. 77-90, 2007.

[6] M. J. Halsted, L. A. Perry, T. P. Cripe *et al.*, "Computers in radiology - Improving patient Care: The use of a digital teaching file to enhance clinicians' access to the intellectual capital of interdepartmental conferences," *American Journal of Roentgenology,* vol. 182, no. 2, pp. 307-309, Feb, 2004.

[7] S. E. Ross, and C. T. Lin, "The effects of promoting patient access to medical records: A review," *Journal of the American Medical Informatics Association,* vol. 10, no. 2, pp. 129-138, Mar-Apr, 2003.

[8] J. H. Gennari, C. H. Weng, J. Benedetti *et al.*, "Asynchronous communication among clinical researchers: A study for systems design," *International Journal of Medical Informatics,* vol. 74, no. 10, pp. 797-807, Oct, 2005.

[9] A. Biswas, K. C. Mynampati, S. Umashankar *et al.*, "MetDAT: a modular and workflow-based free online pipeline for mass spectrometry data processing, analysis and interpretation," *Bioinformatics,* vol. 26, no. 20, pp. 2639-40, Oct 15, 2010.

[10] L. Donelson, P. Tarczy-Hornoch, P. Mork *et al.*, "The BioMediator system as a data integration tool to answer diverse biologic queries," *Stud Health Technol Inform,* vol. 107, no. Pt 2, pp. 768-72, 2004.

[11] A. Hannan, "Providing patients online access to their primary care computerised medical records: a case study of sharing and caring," *Inform Prim Care,* vol. 18, no. 1, pp. 41-9, 2010.

[12] A. Geissbuhler, "Access to health information: a key for better health in the knowledge society," *Yearb Med Inform,* pp. 20-1, 2008.

[13] D. A. Lindberg, and B. L. Humphreys, "Rising expectations: access to biomedical information," *Yearb Med Inform,* pp. 165-72, 2008.

[14] R. Buyl, and M. Nyssen, "MedSkills: a learning environment for evidence-based medical skills," *Methods Inf Med,* vol. 49, no. 4, pp. 390-5, 2010.

[15] R. J. Reynolds, and C. S. Candler, "MedEdPORTAL: educational scholarship for teaching," *J Contin Educ Health Prof,* vol. 28, no. 2, pp. 91-4, Spring, 2008.

[16] X. H. Le, T. Doll, M. Barbosu *et al.*, "An Enhancement of the Role-Based Access Control Model to Facilitate Information Access Management in Context of Team Collaboration and Workflow for Coordination of Clinical Education Programs," *J Biomed Inform (in press),* 2012.

[17] M. D. Rodrı´guez, J. Favela, E. A. Martı´nez *et al.*, "Location-aware access to hospital information and services," *IEEE Transactions on Information Technology in Biomedicine* vol. 4, pp. 448–455, 2004.

[18] "The New York State HIV Clinical Education Initiative," http://www.ceitraining.org. .

[19] G. H. Motta, and S. S. Furuie, " A contextual role-based access control authorization model for electronic patient record," *IEEE Transaction on Information Technology in Biomedicine,* vol. 7, no. 3, pp. 202-207, 2003.

[20] M. Alam, X. Zhang, K. Khan *et al.*, "xDAuth: a scalable and lightweight framework for cross domain access control and delegation," in Proceedings of the 16th ACM symposium on Access control models and technologies, Innsbruck, Austria, 2011, pp. 31-40.

[21] C. K. Georgiadis, I. Mavridis, G. Pangalos *et al.*, "Flexible team-based access control using contexts," in Proceedings of the sixth ACM symposium on Access control models and technologies, Chantilly, Virginia, United States, 2001, pp. 21-27.

[22] Q. Ni, E. Bertino, J. Lobo *et al.*, "Privacy-Aware Role-Based Access Control," *Acm Transactions on Information and System Security,* vol. 13, no. 3, pp. -, Jul, 2010.

[23] B. W. Lampson, "Dynamic protection structures," in AFIPS Conference, Las Vegas, Nevada, 1969, pp. 27–38.

[24] L. J. LaPadula, and D. E. Bell, *Secure Computer Systems: Mathematical Foundation*, vol. 1, Hansom AFB, Bedford, Mass, 1973.
[25] D. T. C. S. E. C. (TCSEC), "DoD 5200.28-STD Foundations " *MITRE Technical Report 2547*, 1973.
[26] Y. C. Chen, L. Y. Yeh, and J. L. Huang, "ABACS: An Attribute-Based Access Control System for Emergency Services over Vehicular Ad Hoc Networks," *Ieee Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 630-643, Mar, 2011.
[27] D. R. Ferraiolo, S. Sandhu, D. R. Kuhn *et al.*, "Proposed NIST standard for role-based access control," *ACM Transactions on Information System Security*, vol. 4, no. 3, pp. 224–274, 2001.
[28] P. W. L. Fong, and I. Siahaan, "Relationship-based access control policies and their policy languages," in Proceedings of the 16th ACM symposium on Access control models and technologies, Innsbruck, Austria, 2011, pp. 51-60.
[29] S. Yamada, and E. Kamioka, "Access control for security and privacy in ubiquitous computing environments," *Ieice Transactions on Communications*, vol. E88b, no. 3, pp. 846-856, Mar, 2005.
[30] C. A. Ardagna, S. D. C. di Vimercati, S. Foresti *et al.*, "Access control for smarter healthcare using policy spaces," *Computers & Security*, vol. 29, no. 8, pp. 848-858, Nov, 2010.
[31] E. Y. Li, T. C. Du, and J. W. Wong, "Access control in collaborative commerce," *Decision Support Systems*, vol. 43, no. 2, pp. 675-685, Mar, 2007.
[32] F. H. Li, W. Wang, J. F. Ma *et al.*, "Action-based access control model," *Chinese Journal of Electronics*, vol. 17, no. 3, pp. 396-401, Jul, 2008.
[33] X. H. Le, S. Lee, Y. K. Lee *et al.*, "Activity-oriented access control to ubiquitous hospital information and services," *Information Sciences*, vol. 180, no. 16, pp. 2979-2990, Aug 15, 2010.
[34] F. L. G. Vela, J. L. I. Montes, P. P. Rodriguez *et al.*, "An architecture for access control management in collaborative enterprise systems based on organization models," *Science of Computer Programming*, vol. 66, no. 1, pp. 44-59, Apr 15, 2007.
[35] I. Ray, R. France, N. Li *et al.*, "An aspect-based approach to modeling access control concerns," *Information and Software Technology*, vol. 46, no. 9, pp. 575-587, Jul 1, 2004.
[36] R. Bobba, O. Fatemieh, F. Khan *et al.*, "Attribute-Based Messaging: Access Control and Confidentiality," *Acm Transactions on Information and System Security*, vol. 13, no. 4, pp. -, Dec, 2010.
[37] X. Feng, M. Jun, H. Hao *et al.*, "Context-aware role-based access control model for Web services," *Grid and Cooperative Computing Gcc 2004 Workshops, Proceedings*, vol. 3252, pp. 430-436, 2004.
[38] A. N. Ravari, J. H. Jafarian, M. Amini *et al.*, "GTHBAC: A Generalized Temporal History Based Access Control Model," *Telecommunication Systems*, vol. 45, no. 2-3, pp. 111-125, Oct, 2010.
[39] J. Bacon, K. Moody, and W. Yao, "A model of OASIS role-based access control and its support for active security," *ACM Transaction on Information System Security*, vol. 5, no. 4, pp. 51, August, 2002.
[40] M. Peleg, D. Beimel, D. Dori *et al.*, "Situation-Based Access Control: privacy management via modeling of patient data access scenarios," *J Biomed Inform*, vol. 41, no. 6, pp. 1028-40, Dec, 2008.
[41] S. Barker, M. J. Sergot, and D. Wijesekera, "Status-Based Access Control," *Acm Transactions on Information and System Security*, vol. 12, no. 1, pp. -, Oct, 2008.
[42] P. Periorellis, and S. Parastatidis, "Task-based access control for virtual organizations," *Scientific Engineering of Distributed Java Applications*, vol. 3409, pp. 38-47, 2005.
[43] F. Almenarez, A. Marin, C. Campo *et al.*, "TrustAC: Trust-based access control for pervasive devices," *Security in Pervasive Computing, Proceedings*, vol. 3450, pp. 225-238, 2005.
[44] S. H. Chae, W. Kim, and D. K. Kim, "uT-RBAC: Ubiquitous role-based access control model," *Ieice Transactions on Fundamentals of Electronics Communications and Computer Sciences*, vol. E89a, no. 1, pp. 238-239, Jan, 2006.
[45] J. Park, and R. Sandhu, "The UCON_{ABC} usage control model," *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 1, pp. 128-174, 2004.
[46] M. Nabeel, E. Bertino, M. Kantarcioglu *et al.*, "Towards privacy preserving access control in the cloud," in 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 2011, pp. 172 - 180
[47] P. Rao, D. Lin, E. Bertino *et al.*, "Fine-grained integration of access control policies," *Computers & Security*, vol. 30, no. 2-3, pp. 91-107, Mar-May, 2011.
[48] E. Bertino, C. Bettini, E. Ferrari *et al.*, "An access control model supporting periodicity constraints and temporal reasoning," *Acm Transactions on Database Systems*, vol. 23, no. 3, pp. 231-285, Sep, 1998.
[49] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," *ACM Trans. Inf. Syst. Secur.*, vol. 4, no. 3, pp. 191-233, 2001.
[50] M. L. Damiani, E. Bertino, and P. Perlasca, "Data security in location-aware applications: an approach based on RBAC," *International Journal of Information and Computer Security*, vol. 1, no. 1, pp. 5-38, 2007.
[51] R. S. Sandhu, E. J. Coyne, H. L. Feinstein *et al.*, "Role based access control models," *Computer*, vol. 29, no. 2, pp. 38-&, Feb, 1996.
[52] "Protégé," http://protege.stanford.edu.
[53] M. T. O'Connor, H. Knublauch, S. Tu *et al.*, "Supporting rule system interoperability on the semantic web with SWRL," *Semantic Web - Iswc 2005, Proceedings*, vol. 3729, pp. 974-986, 2005.
[54] "SWRLJessTab," http://protege.cim3.net/cgi-bin/wiki.pl?SWRLJessTab.
[55] H. E. Friedman, *Jess in Action: Java Rule-Based Systems*, Greenwich, CT, USA: Manning Publications Co., 2003.
[56] "Jess, the Rule Engine for the JavaTM Platform," http://www.jessrules.com.
[57] H. Eriksson, "Using JessTab to integrate Protege and Jess," *Ieee Intelligent Systems*, vol. 18, no. 2, pp. 43-50, Mar-Apr, 2003.
[58] J. Kopena, and W. C. Regli, "DAMLJessKB: A tool for reasoning with the Semantic Web," *Ieee Intelligent Systems*, vol. 18, no. 3, pp. 74-77, May-Jun, 2003.
[59] E. Wang, and Y. S. Kim, "A teaching strategies engine using translation from SWRL to Jess," *Intelligent Tutoring Systems, Proceedings*, vol. 4053, pp. 51-60, 2006.
[60] P. Moraitis, E. Petraki, and N. I. Spanoudakis, "Engineering JADE agents with the Gaia methodology," *Agent*

Technologies, Infrastructures, Tools, and Applications for E-Services, vol. 2592, pp. 77-91, 2002.

[61] B. N. Grosof, M. D. Gandhe, T. W. Finin *et al.*, "Sweetjess: Translating DAMLRuleML to JESS," in International Workshop on Rule Markup Languages for Business Rules on the Semantic Web, 2002.

[62] C. P. Friedman, and J. Wyatt, *Evaluation Methods in Biomedical Informatics*, 2nd ed.: Springer Verlag New York Inc., 2006.

[63] X. H. Le, T. Doll, M. Barbosu *et al.*, "Evaluation of an Enhanced Role-Based Access Control Model to Support Information Access Management in Collaborative Processes," *Technical Report 12-03, 2012. Biomedical Informatics Research and Development Center. University of Rochester. Available at: http://birdlab.org/papers/technical_reports/evaluation.pdf.*, 2011.

[64] OASIS. "eXtensive Access Control Modelling Language, available at http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cd-1-en.html."

[65] R. Ferrini, and E. Bertino, "Supporting RBAC with XACML+OWL," in Proceedings of the 14th ACM symposium on Access control models and technologies, Stresa, Italy, 2009, pp. 145-154.