Security Policy Integration based on Role-Based Access Control Model in Healthcare Collaborative Environments

Teo Poh Kuang[1], Hamidah Ibrahim[2]

Faculty of Computer Science and Information Technology
Universiti Putra Malaysia (UPM)
43400 UPM Serdang
Selangor, MALAYSIA
[1]pohkuang1985@yahoo.com.my, [2]hamidah@fsktm.upm.edu.my

ABSTRACT

Recently research is focused on security policy integration and conflict reconciliation among various healthcare organizations. However, challenging security and privacy risks issues still arisen during sharing sensitive patient data in different large distributed organizations. In this paper, we proposed an approach for integrating security policies based on Role-Based Access Control (RBAC) policy model that supports dynamic constraint rules and meta data information, reduces policy redundancy and resolves conflicts based on the types of policy redundancy and conflict. We believe this work can support dynamic updates and control policies in collaborative environments.

Keywords
Security Policy Integration, Role-Based Access Control, Collaborative Environment, Redundancy, Conflict

1.0 INTRODUCTION

Nowadays there are increasing needs for sharing data that contain personal information between different healthcare organizations Thus, there is a need for dynamic architectural in order to share data among different cross-organization in collaborative environments. However, often such data sharing may contain personal sensitive and confidential information about patient, such as family composition and DNA. It remains a challenge to ensure security and privacy issues for such data sharing in collaborative environment (Jurczyk & Xiong, 2008).

Security is concerns on confidentiality, integrity, and availability of patient data. Privacy typically concerns the patient right to keep their personal medical records. Thus, security can be seen as a key to privacy, as a necessary condition to assure it. Security privacy access control focuses on data sharing in cross-organization. Data sharing will carry out the integration policy among different cross-organization collaboration since each organization may specify its own security policies independently. Policy integration is a process to integrate the similarity security policies from the participating organization in order to govern the data sharing throughout the collaborations. The detection and resolution of policy redundancy and conflict are important to achieve availability, confidentiality, and integrity in policy integration process.

During the policy integration phase, the policies from different organizations to collaborate are compared and evaluated through similarity and logical reasoning before the organizations engage in collaborative environment. Various redundancy and inconsistencies between access policies from different healthcare units may occur during integration process. The policy redundancy and conflict resolution are important to resolve redundancy and inconsistencies before security policies can be integrated for healthcare collaboration.

Access control policy model is important to support dynamic set of users since the group of collaboration organizations may join or leave at runtime (He & Yang, 2009). Role-Based Access Control (RBAC) model has been widely investigated and applied to various applications for a period of time (Hung & Zheng, 2007). However, dynamic constraints in RBAC model have been neglected by existing approaches. This cannot guarantee the flexible security privacy policies for dynamic updates and control policies**.**

In this paper, we proposed an approach for integrating security policies based on RBAC policy model considering both dynamic constraints and meta data information. Besides that, an approach to filter and collect only the required policies from different organizations based on user's integration requirements is investigated. It is important for us to resolve policy redundancy and conflicts based on the types of policy redundancy and conflicts.

This paper is organized as follows. Section 2 provides the security policy specification and presents a case study that is used through out this paper. The types of policy redundancy and conflict are also discussed in Section 2. Related works are presented in Section 3. Section 4 presents the proposed approach for policy integration process based on RBAC model in healthcare

collaborative environments. Finally, Section 5 concludes the paper.

2.0 PRELIMINARIES

The security policy (SPL) in our work is defined as follows:

$$SPL = (R, CR, P, C),$$

where R is role, CR is credential, P is permission and is defined as a pair $<M, O>$, where M is an operation mode and O is an object of data (Park & Lee, 2007), and C is constraint. Constraint information that is included in the policy is temporal and spatial contexts, and meta data information.

The following case study is used to present how policies integration process worked through our proposed approach. This case study is a modified version of the case study given in Yau & Chen (2008). Assume that three organizations that are university, pharmaceutical company, and medical center intend to collaborate. Also, assume that the following security policies have been specified.

Organization *A* – University

Policy *U*1 = {Professor, Professor_ID, Access ∪ Update, Unpublished Paper Draft, (09:00 to 18:00 ∪ Other_Time) ∈ Temporal, Inner_Office ∈ Spatial, Y ∈ Privacy-Sensitive}

Policy *U*2 = {Graduate_Assistant, Assistant_ID, Access, Unpublished Paper Draft, (09:00 to 18:00) ∈ Temporal, Inner_Office ∈ Spatial, Y∈ Privacy-Sensitive}

Policy *U*3 = {Professor, Professor _ID, Access, Patient Information at collaborative medical center, (09:00 to 18:00) ∈ Temporal, (Inner_Office ∪ Outer_Office) ∈ Spatial,Y∈ Privacy-Sensitive}

Organization *B* - Pharmaceutical Company

Policy *P*1 = {(Scientist ∪ Directors), (Scientist_ID ∪ Director_ID), Access, Trial Participants List, (09:00 to 18:00) ∈Temporal, Inner_Office ∈ Spatial, Y∈ Privacy-Sensitive}

Policy *P*2 = {Director, Director_ID, Update, Trial Participants List, (09:00 to 18:00) ∈ Temporal, Inner_Office ∈ Spatial, Y∈ Privacy-Sensitive}

Organization *C* - Medical Center

Policy *M*1 = {Senior_Doctor, Senior_Doctor_ID, Forward, Patient Information, (09:00 to 18:00) ∈ Temporal, (Inner_Office ∪ Outer_Office) ∈ Spatial, Y∈ Privacy-Sensitive}

Policy *M*2 = {(Senior_Doctor ∪ Junior_Doctor), (Senior_Doctor_ID ∪ Junior_Doctor_ID), Access, Patient Information, (09:00 to 18:00) ∈ Temporal, (Inner_Office ∪ Outer_Office) ∈ Spatial, Y∈ Privacy-Sensitive}

Policy *M*3 = {Professor_University at collaborative university, Professor _ID, Access, Patient Information, (09:00 to 18:00) ∈ Temporal, Inner_Office ∈ Spatial, Y∈ Privacy-Sensitive}

Types of Policy Redundancy and Conflict

There are several types of policy redundancy and conflict identified in our work. In this paper, the terms conflict and inconsistencies are used interchangeably.

(a) Types of Redundancy

Policy redundancy is defined as unnecessary access control rules that exists when policies from different organizations are compared during policy integration process. Types of redundancy that are included in our work are redundancy between roles, redundancy between credentials, redundancy between permissions, redundancy between temporal and spatial constraints, and redundancy between meta data information.

(b) Types of Conflict

The types of inconsistencies considered in our work are role inconsistencies, credential inconsistencies, permission inconsistencies, constraint inconsistencies, and meta data information inconsistencies.

Role Inconsistencies: Role inconsistencies between policies from different organizations are present when there are roles in one that have no comparable roles in the other. For example, organization *A* might name attribute role of professor as "Professor" to access patient information but organization *C* would name the attribute role of professor as "Professor_University".

Credential Inconsistencies: Credential inconsistencies are identified when two organizations have different requirements on what needs to be established before the permissions associated with a role can be accessed. This could mean that equivalent roles in the two organizations have access to similar permissions but with a less stringent authorization requirement in one organization.

Permission Inconsistencies: Inconsistencies in the permission occur when organizations allocate different permission to comparable roles. Such an inconsistency means that when comparable roles have no equivalent permission between different organizations. This

inconsistency indicates that when a role in organization *A* has different rights to access permission than the comparable role in organization *B*.

Table 1: Analysis of Characteristics of the Approaches Proposed by Previous Works

Characteristics	Ahamed et al., 2007	Chi et al., 2008	He et al., 2009	He & Yang, 2007	He & Yang, 2009	Huang et al., 2009	Martino et al., 2008	Park & Lee, 2007	Yau & Chen, 2008	Yau & Yin, 2009
Security Policy Specifications		√					√		√	√
Policy Integration Process		√							√	
Policy Comparison			√	√	√	√			√	√
Policy Inconsistencies Checking			√		√	√			√	
Policy Inconsistencies Reconciliation			√		√				√	
Policy Redundancy Checking						√				
Encryption & Decryption										√
Types of Policy Redundancy						√				
Type of Collaboration Patterns			√	√	√					
Types of Policies				√						
Constraints Information	√	√				√	√	√		
Data Flow between Organizations		√								
Critically Aware	√									
Types of Policy Inconsistencies			√		√	√				
RBAC Policy		√	√	√	√	√	√	√		
Role Provisioning							√			
Privacy Preserving Concerns	√						√			√
Data Integration Process										√
Query Plan Wrapper										√
Query Plan Executor										√

Temporal and Spatial Constraint Inconsistencies: Temporal and spatial constraint inconsistencies occur when the location and time of the user to access information does not satisfy the temporal and spatial constraints of comparable role. For example, a professor in organization *A* can access the patient information at collaborative medical center between 09:00 to 18:00 whenever professor he is in the inner office or outer office. While for organization *C*, patient information can be accessed by a professor at collaborative university when he is at inner office between 09:00 to 18:00.

Meta Data Inconsistencies: Meta data inconsistencies are identified when the level of sensitivity in one organization is different from the other organization for the comparable roles.

3.0 RELATED WORK

Yau & Yin (2009) developed an approach that can collect only the required policies based on user's integration requirements and requests for collaboration. Ahamed et al. (2007) presented two possible privacy violations: unwanted health information disclosure and prevention of information leakage through context information to meet the challenges towards preserving privacy on pervasive healthcare environment. The elementary security and reliability requirements discussed in Matousek (2008) should be evaluated in our work in order to make sure that the probability of occurrence and level possible damage can be estimated.

Chi et al. (2008) investigated the workflow involvement of healthcare process in order to support and complement the transition of information and tasks among different

healthcare organizations. The purpose of this study is to propose a security access control model based on role-based access control for integrating healthcare information systems of various organizations. This work only extended RBAC model with role hierarchy, may not encompass the overall context associated with collaboration environment. This is not sufficient to guarantee that the privacy of patient information can be protected during data sharing in collaboration environment. Thus, there is a need to have cohesive policies to sensitive personal health information (Meingast et al., 2006). A case study among pharmacies, hospitals and clinics is presented in this work. However, their implementation is in a relatively small number of organizations.

There are a few previous works that use description logic reasoner to prove that two policies are suitable, or not suitable, for collaboration purposes. However, description logic used in these previous works cannot deal with meta data information (He et al., 2009). Park & Lee (2007) proposed a secure and intelligent Patient Information Service (PIS) based on Context Constraint Role-Based Access Control (CC-RBAC) in the next generation hospital considering ubiquitous intelligent environment. This work presents an access control

mechanism by using temporal and spatial context information to patient information. Temporal context information classifies time into two types - doctor's regular working time and other time. While spatial context information classifies location into three spaces - inner medical office, outer medical office in hospitals, and the other places. However, this work only focuses on access control in single organization, access control in order to integrate security policies and conflict reconciliation for collaboration environment has not been well studied.

Martino et al. (2008) proposed a multi-domain supported and privacy-aware role based access control to meet three crucial requirements when accessing Electronic Medical Records (EMR): access must be both secure and privacy preserving, access must be allowed to individuals from different organizations, and access could be confined based on meta information of the EMRs. Data profile that is proposed in this work is the mechanism provided in extended P-RBAC to store and manage meta data information. Meta data information currently included in data profiles in this work are: data-category, creator-name, creator-affiliation, date-of creation or valid-to, and privacy-sensitive (Y/N).

A number of studies concentrated on the different types of collaborations between organizations have been conducted. The analysis from these studies shows that different types of collaboration impose different ways of integration (He et al., 2009; He & Yang, 2009; He & Yang, 2007). Although these studies focused on business collaboration, they provide simple case studies on the more practical issues in healthcare domain. The goal of these research works is to identify security policies that belong to different application domains and provide analysis on authorization policy requirements for business collaboration, collaboration patterns and various security comparability and integration issues. Description logic that is encoded in these works can be used to determine the satisfiability of a concept. However, these studies only focus on policy consistency comparison and evaluation rather than policy integration process in collaborative environments. Besides that, these models have limitation, only some of the policy inconsistencies have been encoded in this authorization policy model. In addition, they did not investigate policy redundancy that may exist between policies. Policy conflict reconciliation according to the types of collaboration patterns in these works is also intractable.

Huang et al. (2009) identified the types of redundancy and inconsistency during the policy redundancy and inconsistency checking. The policy checking algorithm works in a wide variety of environments ranging from small to large organization, with a few to a large number of roles and comprising of complex access control constraints. However, this study did not look at conflict reconciliation and security policy integration process of different organization collaborations. This work only focuses on static RBAC constraints during the policy checking process and thus dynamic RBAC constraints have been neglected.

Yau & Chen (2008) presented an approach to security policies integration including a similarity-based policy adaption algorithm for changing collaborative groups and a negotiation-based policy generation protocol for the new resources generated by the collaboration as well as for conflict reconciliation. A similarity-based policy adaption algorithm and negotiation-based policy generation protocol are used to achieve dynamic security policy integration with minimum human intervention, which is related to our research. However, no details are given about how to generate the new security policy after conflict reconciliation. Negotiation-base conflict reconciliation proposed in this work take situation-aware compromise thresholds, which specify how much compromise an organization is willing to make for a specific collaboration during the conflict reconciliation process. The compromise makes between the participating organizations usually depends on the trust relations among them. This conflict reconciliation process selects weaker policy that cannot promise actual minimal damage that will bring to the participating organizations. Besides that, similarity-based security policy integration algorithm is limited to two organizations' policies similarity analysis.

Based on the above previous works, none of the approaches focus on the issues of integrating security policies based on RBAC policy model considering both dynamic constraints and meta data information. Thus, our work discussed RBAC issues under collaborative context, role hierarchy, separation of duty, and cardinality constraints and meta data information in collaboration environment to further guarantee the consistency policy integration will operate smoothly in multi-domain environment. It is necessary for us to carry out a larger, yet feasible, implementation that will provide the scenario required for a more comprehensive e-Healthcare system. Table 1 shows an analysis of characteristics of the approaches proposed by previous works.

4.0 THE PROPOSED APPROACH

Our approach aims at generating a new integrated security policy set among different healthcare organizations in collaborations. The following describes our proposed approach which consists of three phases, namely: filteration phase, policy comparison checking phase, and new policy generation phase. Figure 1 shows our overall approach for policy integration, redundancy resolution and conflict resolution based on RBAC model which considers both dynamic constraints and meta data information.

4.1 Filteration Phase

Each organization may specify its own security policies independently. Policy filteration filters the policies from those organizations that are related and required based on organization's collaboration before the organizations engage in collaboration.

Example, let say professor from the university intends to access the trial participants list at pharmaceutical company. However, the trial participants list is provided by medical center to pharmaceutical company. After the collaboration request is submitted by university, pharmaceutical company, and medical center to collaborate, the filteration phase will filter and find the related and required policies from these three organizations based on the request. Thus, only policies *U*3, *P*1, and *M*3 are considered in policy integration process after policy filteration phase.

4.2 Policy Comparison Checking Phase

It is a challenging task to generate the global similarity policy for collaboration purposes since each organization may specify its own security policies. Policy comparison checking is important and necessary phase during policy integration process. There are two types of policy checking which are policy redundancy checking and policy conflict checking. The types of policy redundancy are identified in policy redundancy checking. The main purpose of policy redundancy is to ensure that there are no redundant specifications in describing the integrated policies. The redundancy resolution resolves the policy redundancy based on the types of redundancy. Example, referring to the previous case study, policies *U*3 and *M*3 cause policy redundancy. The types of redundancy exist between these two policies are credential redundancy, permission redundancy, and meta data redundancy. Redundancy resolver resolves the redundancy policy between policies *U*3 and *M*3 by removing policy *U*3.

The consistency of access policies of different organizations needs to be evaluated. Therefore, collaborations can reveal the inconsistencies between the participating policies. The type of conflicts is identified after a policy checking reveals that policy inconsistencies exist between the organizations. Policy consistency checking compares all possible similarities based on relationship between the policies. Policies comparison can be classified into four possible ways that are: they can be exactly matching to one another; one can be inclusively matching with others if one can be a subset of the other, and one can be correlated with others if some components from one may occur in the other while still retaining some unique features, or one is disjoint with the other if they could be completely different with no overlap.

The policies between different organizations are considered permitted if they are exactly matching to one another. Otherwise, policy inconsistency exists between policies. If the conflict reconciliation cannot resolve the policy conflict, then the request for collaboration between organizations is rejected.

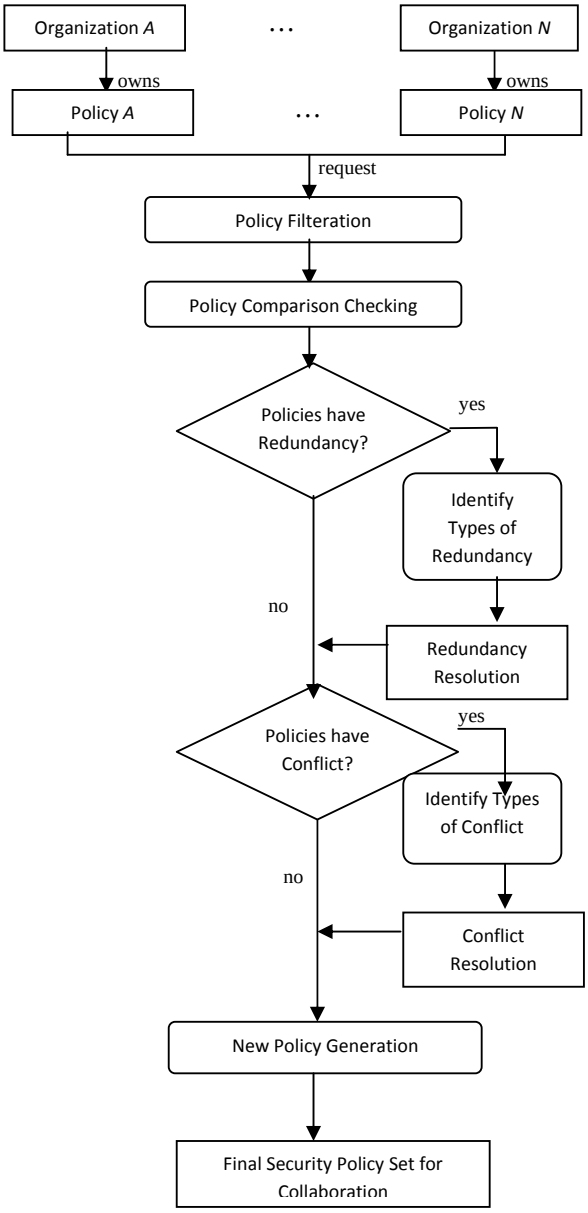

Figure 1: Overall Approach for Policy Integration, Redundancy Resolution, and Conflict Resolution based on RBAC Model

For example, policy *U*3 states that a professor is allowed to access patient information at collaborated medical center from 09:00 to 18:00 when he is at inner office or outer office. However, policy *M*3 states that a professor from collaborated university can only access patient information on regular working hour from 09:00 to 18:00 and at inner office. Thus, there are inconsistencies between policies *U*3 and *M*3 that are temporal and spatial constraint inconsistencies. To briefly conclude, policy

*M*3 is more restricted than policy *U*3. Conflict resolver resolves the conflict based on the types of conflict that are identified.

From the above example, it is desirable to enforce restricted access policies in order to achieve confidentiality of patient information by restricting the access only at inner office from 09:00 to 18:00. Thus, we remove policy *U*3 and maintain policy *M*3 since policy *M*3 is more restricted than policy *U*3. It seems like there is no direct relationship between policies *P*1 and *M*3. However, because policy *M*3 at medical center allows professor from collaborative university to access patient information, thus it is reasonable to grant permission to professor to access trial participant list at pharmaceutical company that is provided by medical center.

4.3 New Policy Generation Phase

Finally, the new security policy set is generated for the collaborating organizations. Our access control model is enforced with privacy policies to ensure that we can meet the security and privacy purposes for data sharing. It is important to generate a common set of policies accepted by different organizations. Hence, the integrated security policy set should be able to handle all possible data access requests by users from different organizations in collaborations which address the security concerns from different organizations. Example, referring to the case study, the final security policy set based on the user's collaboration request is as follows:

Final Policy = {Professor, Professor_ID, Access,
Trial Participants List,
(09:00 to 18:00)∈ Temporal,
Inner_Office ∈ Spatial,
Y∈Privacy-Sensitive}

5.0 SUMMARY

To briefly summary, we proposed an approach for integrating security policies based on Role-Based Access Control (RBAC) policy model considering both dynamic constraints and meta information. Besides that, an approach to filter and collect only the required policies from different organizations based on user's integration requirements is investigated. It is important for us to resolve policy redundancy and conflicts based on the types of policy redundancy and conflict. The next stage of our work is to prove the correctness and completeness of the proposed approach.

REFERENCES

Ahamed, S. I., Talukder, N., & Kameas, A. D. (2007). Towards Privacy Protection in Pervasive Healthcare. *In Proceedings of the 3rd IET International Conference on Intelligent Environments (IE 07)*, pp. 296-303.

Chi, H., Jones, E. L., & Zhao, L. (2008). Implementation of a Security Access Control Model for Inter-Organizational Healthcare Information Systems. *In Proceedings of the Asia-Pacific Services Computing Conference, APSCC '08, IEEE*, pp. 692-696.

He, D. D., Compton, M., Taylor, K., & Yang, J. (2009). Access Control: What is Required in Business Collaboration? *In Proceedings of the 20th Australian Database Conference (ADC 2009)*, pp. 107-116.

He, D. D., & Yang, J. (2007). Security Policy Specification and Integration in Business Collaboration. *In Proceedings of the IEEE International Conference on Services Computing (SCC 2007)*, pp. 20-27.

He, D. D., & Yang, J. (2009). Authorization Control in Collaborative Healthcare Systems. *In the Journal of Theoretical and Applied Electronic Commerce Research*, 88-109.

Huang, C., Sun, J., Wang, X., & Si, Y. (2009). Security Policy Management for Systems Employing Role Based Access Control Model. *In Information Technology Journal*, 726-734.

Hung, P. C. K., & Zheng, Y. (2007). Privacy Access Control Model for Aggregated e-Health Services. *In Proceedings of the 2007 Eleventh International IEEE EDOC Conference Workshop (EDOCW'07)*, pp. 12-19.

Jurczyk, P., & Xiong, L. (2008). Towards Privacy-Preserving Integration of Distributed Heterogeneous Data. *In Proceedings of the 2nd PhD Workshop on Information and Knowledge Management*, pp. 65-72.

Martino, L. D., Ni, Q., Lin, D., & Bertino, E. (2008). Multi-domain and Privacy-aware Role Based Access Control in eHealth. *In Proceedings of the Second International Conference on Pervasive Computing Technologies for Healthcare*, pp. 131-134.

Matousek, K. (2008). Security and Reliability Considerations for Distributed Healthcare Systems. *In Proceedings of 2nd Annual IEEE International Carnahan Conference on Security Technology (ICCST 2008)*, pp. 346-348.

Meingast, M., Roosta, T., & Sastry, S. (2006). Security and Privacy Issues with Health Care Information Technology. *In the Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA*, pp. 5453 - 5458.

Park, J. H., & Lee, D. G. (2007). PIS-CC RBAC: Patient Information Service based on CC_RBAC in Next Generation Hospital considering Ubiquitous Intelligent Environment. *In Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07)*, pp. 196-200.

Yau, S. S., & Chen, Z. (2008). Security Policy Integration and Conflict Reconciliation for

Collaboration among Organizations in Ubiquitous Computing Environments. *In Proceedings of the 5th International Conference on Ubiquitous Intelligence and Computing, Oslo, Norway*, pp. 3-19.

Yau, S. S., & Yin, Y. (2009). A Privacy Preserving Repository for Data Integration across Data Sharing Services. *IEEE Transactions on Services Computing*, pp. 130-140.