American Journal of Economics and Business Administration 3 (1): 101-111, 2011
ISSN 1945-5488

# Security Extensible Access Control Markup Language Policy Integration Based on Role-Based Access Control Model in Healthcare Collaborative Environments

Teo Poh Kuang, Hamidah Ibrahim, Nur Izura Udzir and Fatimah Sidi
Department of Computer Science
Faculty of Computer Science and Information Technology,
University Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

**Abstract:** Recently research is focused on security policy integration and conflict reconciliation among various healthcare organizations. **Problem statement:** However, challenging security and privacy risk issues still arisen during sharing sensitive patient data in different large distributed organizations. Though eXtensible Access Control Markup Language (XACML) has a powerful capacity of expression, it does not support all the elements character of RBAC. Thus, it has not been built to manage security in large distributed systems in healthcare domain since each organization may join or leave at runtime. The policy redundancy and conflict resolution are important to resolve redundancy and inconsistencies before security policies can be integrated for healthcare collaboration. Existing approaches did not look at policy redundancy and conflict resolution process based on the types of redundancy and conflict for dynamic set of organizations collaboration. Besides that, a policy integration mechanism in order to generate actual security policy integration is not in well studied. **Approach:** In this study, we proposed an approach for integrating security XACML policies based on RBAC policy model considering both 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. **Results:** From the observation and literature analysis, it can be concluded that our work could provide the maximum confidence for pre-compile a large amount of policies and only return the most similar policies for policy integration. Besides that, our approach proved that the more restrict policy will be generated during the policy integration. **Conclusion:** Our work can guarantee the completeness as well as consistency of the access control policy. It is recommended that the dynamic constraints such as dynamic Separation Of Duty (SOD) should be considered because we believe this consideration can support dynamic updates and control policies in collaborative environments.

**Key words:** XACML, security policy integration, role-based access control, collaborative environment, redundancy, conflict, Separation Of Duty (SOD), Role-Based Access Control (RBAC), Discretionary Access Control (DAC)

## INTRODUCTION

Nowadays there are increasing needs for sharing data that contain personal information between different organizations such as federal, state and local government, commercial health insurance company and self-pay patient (Frezza and Chiriva-Internati, 2005). There is a risk of having large amounts of widely accessible during sharing data in collaborative environments (El-Sofany, 2008). For example, the patient treatment payment method chosen was cost reimbursement by health insurance company (Frezza, 2005) to hospitals reveal that it is necessary to have cooperative environment between hospital and health insurance company. 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 and Xiong, 2008).

One of the fundamental key to successful security and privacy data sharing between different healthcare organizations in collaborative environments is to

**Corresponding Author:** Teo Poh Kuang, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

address security issues to patient data: confidentiality, integrity and availability. Confidentiality is related to the disclosure of data, integrity is related to modification of the data and availability is related to the denial of access to data (Wahsheh and Alves-Foss, 2008). Privacy typically concerns the patient right to keep their personal medical records. There are 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 (Ahamed *et al*., 2007). 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 policies from the participating organization in order to govern the data sharing throughout the collaborations. In order to protect sensitive data access by unauthorized users in collaborative environment, security features cannot be assured by one organization, but is a shared responsibility among all stakeholders who are using the sharing communication infrastructure (Fahad, 2010).

Some of the research that use eXtensible Access Control Markup Language (XACML) for policy integration include Lin *et al*. (2007); Mazzoleni *et al*. (2006); Rao *et al*. (2009). XACML is a declarative access control policy language implemented in XML. It is a processing model for the purpose to describe how to interpret the policies. XACML is intended to provide policy integration and conflict resolution. Access control model such as Discretionary Access Control (DAC), Mandatory Access Control, Role-Based Access Control (RBAC) as well as door access control for building security (Wahyudi *et al*., 2007) was investigated by researchers nowadays in order to protected sensitive information from unauthorized access. RBAC is a most popular access control model to compromise security features since it has many excellent properties, such as role hierarchy, separation of duty, cardinality constraints, or context constraints. Though XACML has a powerful capacity of expression, it does not support all the elements character of RBAC. Thus, it has not been built to manage security in large distributed systems in healthcare domain collaborations since each organization may join or leave at runtime.

There is a need to have cohesive policies to sensitive personal health information (Meingast *et al*., 2006). 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. The detection and resolution of policy redundancy and conflict are important to achieve availability, confidentiality and integrity in policy integration process. Various redundancies and inconsistencies between access policies from different healthcare units may occur during integration process. The policy redundancy and conflict resolution are important to resolve redundancies and inconsistencies before security policies can be integrated for healthcare collaboration.

Previous works are limited in identifying policy rules specifying the same attribute in policy similarity process (Lin *et al*., 2007; Mazzoleni *et al*., 2006). These studies do not involve complex rule comparison methods using patterns or semantic analysis. Previous study compromises between participating organizations and adopted weaker policy in order to improve the collaboration chance (Yau and Chen, 2008). This approach cannot compromise actual minimal damage because the collaborating organizations will take risk by relaxing their security policies to resolve the conflicts. Besides that, previous research study supported precedence concept in order to use for resolve possible conflicts between two policies (Rao *et al*., 2009). This approach allows one to specify the behavior of the integrated policy at the granularity of requests and effects. However, each organization is an autonomous entity and will specify its own security policies independently. It is unreasonable to choose an organization’s policies over the others when policy conflict happens during comparison process. To the best of our knowledge, only a few existing approaches investigated policy integration mechanisms to generate actual security policy as a result of policy integration.

In this study, we proposed an approach for integrating security XACML policies based on RBAC policy model considering both 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 using logical reasoning and similarity analysis. There is no universal method of resolution (Zidat and Djoudi, 2006). The existing conflict resolution technique is depends on the requirements that organizations necessary for collaboration. Thus, our work will resolve policy redundancies and conflicts based on the types of policy redundancy and conflicts. We believe our conflict resolution can laying good foundation to for security policy integration that is suitable for collaboration environments.

**Prior literature:** Lin *et al*. (2007) proposed a tool which acts as filter phase, before more expensive analysis tools are applied, such as logical reasoning and Boolean function comparison. This study does the comparison of each same policy targets and the same type of elements belonging to the rules with the same effect. According to the obtained similarity scores, dissimilar policies can be pruned so that the number of policies which need to be further examined is largely reduced. However, they will reject all possible collaborators when dissimilar policies are obtained during policy evaluation. Yau and Yin (2009) developed an approach that can collect only the required policies based on user's integration requirements and requests for collaboration, which is related to our study.

There are a few previous studies that use description logic reasoner to prove that two policies are suitable, or not suitable, for collaboration purposes. Description logic that is encoded in these studies can be used to determine the satisfiability of a concept. However, description logic used in these previous studies cannot deal with meta data information (He and Yang, 2009). Meta data information is required to specify which roles in organization A relate to which roles in organization B and what privileges are equivalent. Data profile that is proposed in Martino *et al*. (2008) is the mechanism provided in extended Privacy Role-Based Access Control (P-RBAC) to store and manages meta data information. Meta data information currently included in data profiles in this study are: data-category, creator-name, creator-affiliation, date-of creation or valid-to and privacy-sensitive (Y/N). Thus, it is important for us to investigate meta data information during policy comparison process.

A number of studies concentrated on the analysis to show that different types of collaboration impose different ways of integration (He and Yang, 2007; He and Yang, 2009). 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 studies 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. 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 studies is also intractable.

Chi *et al*. (2008) propose a security access control model based on role-based access control for integrating healthcare information systems of various organizations. This study only extended RBAC model with role hierarchy, may not encompass the overall context associated with collaboration environment. A case study among pharmacies, hospitals and clinics is presented in this study. However, their implementation is in a relatively small number of organizations. Huang *et al*. (2009) proposed a method using eXtensible Access Control Makeup Language (XACML) policies to Description Logics Knowledge Base and the conflict detection problem is transferred into a problem of consistency in Abox. Though this study used XACML to express role hierarchy and resource hierarchy, it is not sufficient enough to policy integration since Role-Based Access Control (RBAC) still has many properties, such as dynamic separation of duty, cardinality and context constraints. This study only considers the policies that have the same action attribute values and the environment attributes will always be fitted. However, in real world we should consider there have different action attribute values in policy comparison process. The previous study is not sufficient to guarantee that the privacy of patient information can be protected during data sharing in collaboration environment. Our study will consider how to extend XACML to express more constraint modeled by RBAC.

Park and 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 study presents an access control mechanism 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. Huang *et al*. (2009) identified the types of redundancy and inconsistency during the policy redundancy and inconsistency checking. The policy checking algorithm is studied 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, these studies 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.

Table 1: Analysis of characteristics of the approaches proposed by previous works

| Characteristics | Huang *et al.* (2009) | He and Yang (2009) | He *et al.* (2009) | Lin *et al.* (2007) | Huang *et al.* (2009) | Chi *et al.* (2008) | Martino *et al.* (2008) | Park and Lee (2007) | Mazzoleni *et al.* (2008) | Rao *et al.* (2009) | Yau and Yin (2009) | Yau and Chen (2008) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Security policy specifications | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Policy comparison | √ | √ | √ | √ | √ | | | | √ | √ | √ | √ |
| Policy inconsistencies reconciliation | √ | | √ | | | | | | | √ | | √ |
| Policy redundancy checking | | √ | | | | | | | | | | |
| New policy generation | | | | | | | | | √ | √ | | √ |
| Encryption & decryption | | | | | | | | | | | √ | |
| Types of policy redundancy | | √ | | | | | | | | | | |
| Type of collaboration patterns | √ | | √ | | | | | | | | | |
| Constraints information | | √ | | | √ | √ | √ | √ | | √ | | |
| Data flow between organizations | | | | | | √ | | | | | | |
| Critically aware | | | | | | | | | | | | |
| Types of policy inconsistencies | √ | √ | √ | | | | | | | | | |
| Role provisioning | | | | | | | √ | | | | | |
| Privacy preserving concerns | | | | | | | √ | | | | √ | |
| Data integration process | | | | | | | | | | | √ | |
| Query plan wrapper | | | | | | | | | | | √ | |
| Query plan executor | | | | | | | | | | | √ | |

Mazzoleni *et al*. (2006) proposed an extension to the XACML language, called policy integration preferences, which a party can specify the approach that must be adopted when its policies have to be integrated with policies by other parties. However, they do not discuss mechanisms to perform such integrations. Also, the integration preferences discussed in such study are very limited and do not support fine-grained integration requirements. They presented the method of computing policy similarity that is limited in identifying policy rules specifying the same attribute. This method simply adopts syntactical analysis to identify policies specifying the same attribute. The study does not involve complex rule comparison methods using patterns or semantic analysis. Furthermore, this study does not relax some constraints like obligations on XACML policies. Hung and Zheng (2007) were proposed privacy-based entities to the core RBAC which are purposes, recipients, obligations and retentions. Thus, it seems like obligations are necessary to consider include in RBAC policy model. Rao *et al.* (2009) discussed algebra for fine-grained integration of sophisticated policies from the collaborating parties. This work proposed a framework that uses the algebra for the fine-grained integration of policies expressed in XACML. A methodology for generating the actual integrated XACML policy, based on the notion of Multi-Terminal Binary Decisions Diagrams is similar to our study.

Yau and 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. There are no mechanisms to generate real policies as a result of policy integration. Negotiation-based conflict reconciliation proposed in this study 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 prefers to select 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.

Based on the above previous study, 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 study 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 study.

## MATERIALS AND METHODS

**Preliminaries:** The Security Policy (SPL) in our study is defined as follows:

SPL= (R, CR, PM, C)

Where:
R = Role
CR = Credential
PM = Permission and is defined as a pair <M, O>

where, M is an operation mode and O is an object of data (Park and 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 policy integration process worked through our proposed approach. This case study is a modified version of the case study given in Yau and 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 study draft, (09:00-18:00 ∪ Other_Time) ∈ Temporal, Inner_Office ∈ Spatial, Y ∈ Privacy-Sensitive}
Policy $U_2$ = {Graduate_Assistant, Assistant_ID, Access, Unpublished study draft,
(09:00-18:00) ∈ Temporal,
Inner_Office ∈ Spatial,
Y∈ Privacy-Sensitive}
Policy $U_3$ = {Professor, Professor _ID, Access, Patient information at collaborative medical center,
(09:00-18:00) ∈ 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,
(09:00-18:00) ∈ Temporal,
Inner_Office ∈ Spatial,
Y∈ Privacy-Sensitive}
Policy $P_2$ = {Director, Director_ID, Update,
Trial participants list,
(09:00-18:00) ∈ Temporal,
Inner_Office ∈ Spatial,
Y∈ Privacy-Sensitive}

**Organization C-medical center:**

Policy $M_1$ = {Senior_Doctor, Senior_Doctor_ID,
Forward, Patient information,
(09:00-18:00) ∈ 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,
(09:00-18:00) ∈ Temporal,
(Inner_Office ∈ Outer_Office) ∈
Spatial,
Y∈ Privacy-Sensitive}
Policy $M_3$ = {Professor_University at collaborative
university, Professor _ID, Access,
Patient Information,
(09:00-18:00) ∈ 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 study. In this study, the terms conflicts and inconsistencies are used interchangeably.

**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 study are redundancy between roles, redundancy between credentials, redundancy between permissions, redundancy between temporal and spatial constraints and redundancy between meta data information.

**Types of conflict:** The types of inconsistencies considered in our study 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 permissions to comparable roles. Such an inconsistency means that 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.

**Temporal and spatial constraint inconsistencies:** Temporal and spatial constraint inconsistencies occur when the location and time of the user to access information do 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 09:00-18:00 whenever 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 09:00-18:00.

**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.

**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: Filtration 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.

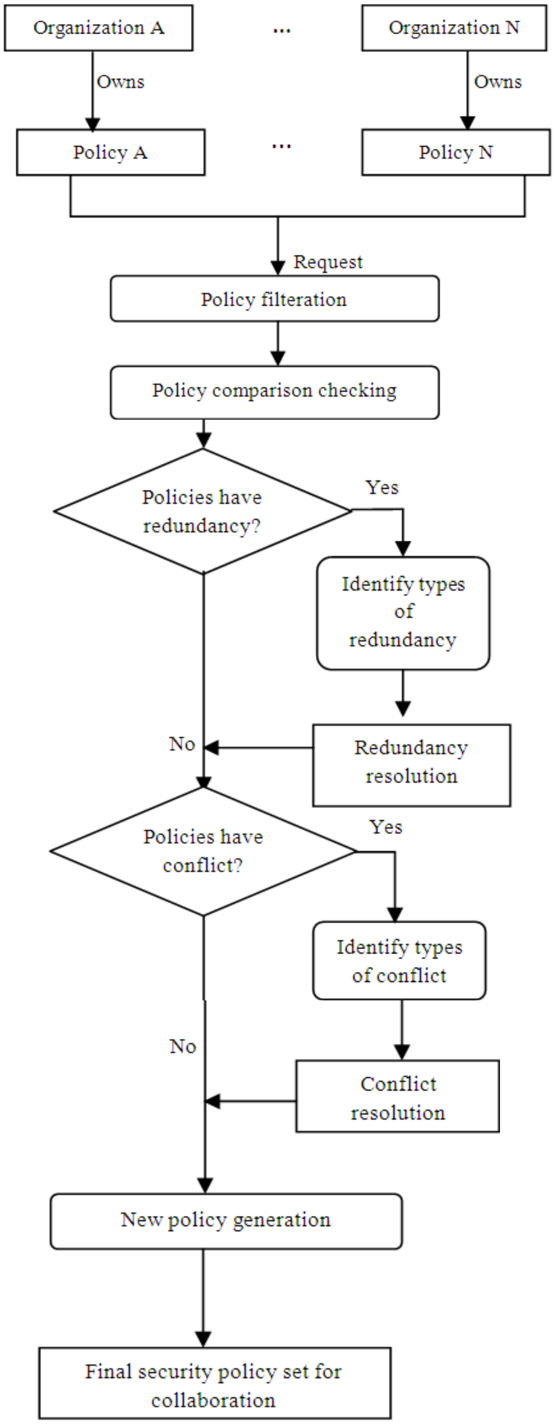

Fig. 1: Overall approach for policy integration, redundancy resolution and conflict resolution based on RBAC model

**Filtration phase:** Each organization may specify its own security policies independently. Policy filtration filters the policies from those organizations that are related and required based on organization's collaboration before the organizations engage in collaboration. For example, referring to the case above, the filtration 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 filtration phase. Specifically, we compute the element matching function $M_{policy}$ between two policies $P_a$ and $P_b$ as follows:

$$M_{policy}(P_a, P_b) = M(R_a, R_b) * M(CR_a, CR_b) * M(PM_a, PM_b) * M(C_a, C_b)$$

Where:

R = Roles<br>
C = Credential<br>
PM = Permission<br>
C = Constraints

**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.

For example, policy $U_3$ states that a professor is allowed to access patient information at collaborated medical center from 09:00-18:00 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 09:00-18:00 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 09:00-18:00. 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.

**Matching score between rules and effects:** 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. We will classify all types of possible matching between policies based on comparing the same fields in the elements. There are 5 types of possible comparisons between these fields: Exactly matching ($\equiv$), subset ($\subseteq$), superset ($\supset$), disjoint ($\neq$) and intersect ($\cap$). Assume that:

$$P_a = \{elem_{as}, elemt_{ar}, elemt_{aa}, elem_{act}, elemt_{acs}, elem_{am}, elemt_{af}\}$$

$P_b$ = {$elem_{bs}$, $elemt_{br}$, $elemt_{ba}$, $elem_{bct}$, $elemt_{bcs}$, $elem_{bm}$, $elemt_{bf}$}}

Where:

| | | |
|---|---|---|
| s | = | Subject |
| r | = | Resource |
| a | = | Action |
| ct | = | Time constraint |
| cs | = | Spatial constraint |
| m | = | Meta data information |
| f | = | Effect |

**Matching 1: Exactly matching policies:** Elements of $P_a$ and $P_b$ are exactly matched if every field in $P_a$ is equal to the same filed in $P_b$. Formally, the exactly matching policies are stated as follows:

if ($R_{a \equiv} R_b$) && ($CR_a \equiv CR_b$) && ($PM_a \equiv PM_b$) && ($C_a \equiv C_b$), then $P_a \equiv P_b$

**Matching 2: Completely disjoint matching policies:** $P_a$ is completely disjoint with $P_b$ if every field in $P_a$ does not have any common part with the corresponding field in $P_b$. We can assume that $P_a$ and $P_b$ do not represent the same thing or value:

if ($R_a \neq R_b$) && ($CR_a \neq CR_b$) && ($PM_a \neq PM_b$) && ($C_a \neq C_b$), then $P_a \neq P_b$

**Matching 3: Inclusively matching policies:** $P_a$ is subset of $P_b$ every field of $P_a$ is also an element of in $P_b$. Thus, $P_b$ is a superset of $P_a$. When $S_1$ from $P_1$ is subset of $S_2$ from $P_2$ if the $S_1$ inherit $S_2$. In other words is $S_1$is a subclass of the $S_2$:

if ($elem_{ai} \subseteq elem_{bi}$) where i = (r, cr, p, c), then $P_a \subseteq P_b$

**Matching 4: Intersect matching policies:** $P_a$ and $P_b$ is intersect matching when some elements in $P_a$ has a common part with the corresponding elements in $P_b$ but some other field in $P_a$ does not has common part with the corresponding elements in $P_b$.

if ($elem_{ai} \cap elem_{bi}$) where i = (r, cr, p, c), then $P_a \cap P_b$

The inconsistencies between policies are raised when $P_a$ and $P_b$ are inclusively matching. The redundancy between policies are raised when $P_a$and $P_b$ is intersect matching or exactly matching. The complately disjoint policies rules will be directly pruned after policy comparison process.

**Redundancy resolution:** The redundancy between policies are raised when $P_a$ and $P_b$ is intersect matching or exactly matching. When the policies evaluation is exactly matching, we will choose to remove one of the policies and retain another policy. While the policy evaluation is intersect matching, we will choose to remove subset of the policy and retain superset of the policy.

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 $U_3$. We will remove the redundant part and retain the subset of the policies. For example, policy $U_3$ allows the professor to access patient information at inner and outer office. However, policy $M_3$ only allows professor to access patient information at collaborative university in inner office only. This is redundancy between spatial constraints. Based on the least of privilege principle, we will only allow professor to access patient information at inner office.

**Inconsistencies resolution:** Permit decision will be in precedence to choose if any permit rule wins its matches against every deny rule and otherwise issues a deny decision.

**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, (09:00-18:00)$\in$Temporal, Inner_Office $\in$ Spatial, Y$\in$Privacy-Sensitive}

**Algorithm for policy integration process:**

Input: Policy $P_a$ = ($R_a$, $CR_a$, $PM_a$, $C_a$)
Policy $P_b$= ($R_b$, $CR_b$, $PM_b$, $C_b$)

Table 2: Comparison between the Proposed Approach and Yau and Chen (2008)

| | Domain | No. of Organization | No. of Policy | Conflict Resolution |
|---|---|---|---|---|
| Proposed Approach | Health-care | N | N | More restrict policy |
| Yau and Chen (2008) | Health-care | 2 | 6 | Weaker policy |

Table 3: Results of the security policy integration

| | Final actual security policy integration |
|---|---|
| Proposed Approach | {Professor, Professor_ID, Access,<br>Trial participants list,<br>(09:00-18:00)$\in$Temporal,<br>Inner_Office $\in$ Spatial,<br>Y$\in$Privacy-Sensitive} |
| Yau and Chen (2008) | {(Scientists $\cup$ Directors) ,<br>(Scientists _ID $\cup$ Directors_ID, Access,<br>Trial participants list,<br>(09:00-18:00)$\in$Temporal,<br>Inner_Office $\in$ Spatial,<br>Y$\in$Privacy-Sensitive} |

Output: New Integration Policy
For each attribute in $P_a$ and $P_b$

Check whether elements of $P_a$ and $P_b$ are exactly matched, completely disjoint, partially disjoint, inclusively matching, or intersect matching:

If ($R_a \equiv R_b$) && ($CR_a \equiv CR_b$) && ($PM_a \equiv PM_b$) && ($C_a \equiv C_b$), Then $P_a \equiv P_b$, Redundancy Resolution.
else If ($R_a \neq R_b$) && ($CR_a \neq CR_b$) && ($PM_a \neq PM_b$) && ($C_a \neq C_b$), Then $P_a \neq P_b$, Policy Pruned
else If ($elem_{ai} \subseteq elem_{bi}$) where i = (r, cr, p, c), then $P_a \subseteq P_b$, Inconsistencies Resolution.
else If ($elem_{ai} \cap elem_{bi}$) where i = (r, cr, p, c), then $P_a \subseteq P_b$, Inconsistencies Resolution.

## RESULTS

Table 2 and table 3 compare our proposed approach to Yau and Chen (2008).

## DISCUSSION

Our result show that the present approach can carried out actual security XACML policies integration based on RBAC policy model by considering both constraints and meta data information. Compares to the method by Yau and Chen (2008), our approach is different in several ways: Firstly, our approach can work in a wide variety of collaboration environments ranging from small to large healthcare organization, within a few to a large number of policies and comprising of access control constraints. From the above result evaluation, we can see that our algorithm can work in more policy comparison and integration compared to with previous works. Secondly, our approach is the first attempt to take similarity and logical reasoning analysis in consideration for policy comparison. Thus, this approach could provide the maximum confidence for pre-compile a large amount of policies and only return the most similar policies for policy integration. Thirdly, our approach applies the least privilege principle. Thus, the weakest policy will not be taking during the conflict resolution. The principle of least privilege, which restricting by denied the access when inconsistencies occur during policy integration, described as important for meeting integrity. According to the case study, we get the actual security policy integration based on our approach is more restricted and secure than Yau and Chen (2008). As a future work, we plan to consider the dynamic constraints such as dynamic Separation Of Duty (SOD).

## CONCLUSION

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. There is no universal method of resolution. It is important for us to resolve policy redundancies and conflicts based on the types of policy redundancy and conflict.

## ACKNOWLEGEMENT

Our thanks to the University Putra Malaysia (UPM) for supporting this study under grant number 05/01/07/0162RU.

## REFERENCES

Ahamed, S.I., N. Talukder and A.D. Kameas, 2007. Towards privacy protection in pervasive healthcare. Proceedings of the 3rd IET International Conference on Intelligent Environments (IE 07), Sep. 24-25, Ulm, Germany, pp: 296-303. ISBN: 978 0 86341 853 2

Chi, H., E.L. Jones and Zhao, 2008. Implementation of a security access control model for inter-organizational healthcare information systems. Proceedings of the Asia-Pacific Services Computing Conference, Dec. 09-12, IEEE Computer Society Washington, DC, USA., pp: 692-696. DOI: 10.1109/APSCC.2008.256

El-Sofany, H.F., 2008. Extending the concepts of normalization from relational databases to extensible-markup-language databases model. J. Comput. Sci., 4: 729-740.

Fahad, T.B.M., 2010. Dominant factors in national information security policies. J. Comput. Sci., 6: 808-812.

Frezza, E.E. and M. Chiriva-Internati, 2005. The evolution of today’s health care economy. J. Soc. Sci., 1: 39-40.

Frezza, E.E., 2005. The Six stages of the healthcare economy-is socialized medicine at the door? A historical review. J. Soc. Sci., 1: 197-198.

He, D.D. and J. Yang, 2007. Security policy specification and integration in business collaboration. Proceedings of the IEEE International Conference on Services Computing (SCC 2007), July 9-13, Salt Lake City, USA., pp: 20-27. DOI: 10.1109/SCC.2007.96

He, D.D. and J. Yang, 2009. Authorization control in collaborative healthcare systems. J. Theoretical Applied Elect. Commerce Res., 2: 88-109. DOI: 10.4067/S0718-18762009000200008

Huang, C., J. Sun, X. Wang and Y. Si, 2009. Security policy management for systems employing role based access control model. Inform. Technol. J., Asian Network Sci. Inform. Pak., 8: 726-734. DOI: 10.3923/itj.2009.726.734

Huang, F. Z., Huang and L. Liu, 2009. A DL-based method for access control policy conflict detecting. Proceedings of the First Asia-Pacific Symposium on Internetware, Beijing, China, Oct. 17-18, ACM New York, NY, USA., pp: 1-150. http://portal.acm.org/citation.cfm?id=1640206

Hung, P.C.K. and Y. Zheng, 2007. Privacy access control model for aggregated e-health services. Proceedings of the 11th International IEEE EDOC Conference Workshop (EDOCW'07), Oct. 15-16, EEE Computer Society Washington, DC, USA., pp: 12-19. DOI: 10.1109/EDOCW.2007.24

Jurczyk, P. and L. Xiong, 2008. Towards privacy-preserving integration of distributed heterogeneous data. Proceedings of the 2nd PhD Workshop on Information and Knowledge Management, Oct. 30, ACM New York, NY, USA., pp: 65-72. DOI: 10.1145/1458550.1458562

Lin, D., P. Rao, E. Bertino and J. Lobo, 2007. An approach to evaluate policy similarity. Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, Sophia Antipolis, France, June 20-22, ACM New York, NY, USA., pp: 1-10. DOI: 10.1145/1266840.1266842

Martino, L.D., Q. Ni, D. Lin and E. Bertino, 2008. Multi-domain and privacy-aware role based access control in ehealth. Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare, Jan. 30-1 Feb, Pervasive Health, Tampere, pp: 131-134. DOI: 10.1109/PCTHEALTH.2008.4571050

Mazzoleni, P., B. Crispo, E. Bertino and S. Sivasubramanian, 2006. XACML policy integration algorithms (not to be confused with XACML policy combination algorithms!). Proceeding of the 11th ACM Symposium on Access Control Models and Technologies, June 07-09, ACM New York, NY, USA., pp: 219-227. DOI: 10.1145/1133058.1133089

Meingast, M., T. Roosta and S. Sastry, 2006. Security and privacy issues with health care information technology. Proceedings of the 28th IEEE EMBS Annual International Conference, Aug. 30-3 Sep., New York City, USA., pp: 5453-5458. DOI: 10.1109/IEMBS.2006.260060

Park, J.H. and D.G. Lee, 2007. PIS-CC RBAC: Patient information service based on CC_RBAC in next generation hospital considering ubiquitous intelligent environment. Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07), April 26-28, IEEE CS, Seoul, Korea, pp: 196-200. DOI: 10.1109/MUE.2007.171

Rao, P., D. Lin, E. Bertino, N. Li and J. Lobo, 2009. An algebra for fine-grained integration of XACML policies. Proceedings of the 14th ACM Symposium on Access Control Models and Technologies, June 3-5, ACM New York, NY, USA., pp: 63-72. DOI: 10.1145/1542207.1542218

Wahsheh, L.A. and Alves-Foss, J., 2008. Security policy development: Towards a life-cycle and logic-based verification model. Am. J. Applied Sci., 5: 1117-1126.

Wahyudi, A.W. and S. Mohamed, 2007. Intelligent voice-based door access control system using Adaptive-Network-based Fuzzy Inference Systems (ANFIS) for building security. J. Comput. Sci., 3: 274-280.

Yau, S.S. and Y. Yin, 2009. A privacy preserving repository for data integration across data sharing services. IEEE Trans. Services Comput., 1: 130-140. DOI: 10.1109/TSC.2008.14

Yau, S.S. and Z. Chen, 2008. Security policy integration and conflict reconciliation for collaboration among organizations in ubiquitous computing environments. Proceedings of the 5th International Conference on Ubiquitous Intelligence and Computing, Oslo, June 23-25, Springer-Verlag Berlin, Norway, pp: 3-19. DOI: 10.1007/978-3-540-69293-5_3

Zidat, S. and Djoudi, M., 2006. Task collaborative resolution tool for elearning environment. J. Comput. Sci., 2: 558-564.