Novel Access Control Approach for Inter-organizational Workflows

Asmaa El Kandoussi and Hanan El Bakkali
Information Security Research Team, ENSIAS, Mohammed V University, Rabat, Morocco

Keywords: Access Control Policy, Inter-organizational Workflows, Conflict Resolution.

Abstract: Inter-organizational workflows have become increasingly used by companies to improve their productivity by sharing resources and activities. These systems have proven their effectiveness in several areas. However, the sensitivity of the exchanged data, push participating organizations to set authorization rules in order to protect their data and processes. At this level, the cohabitation of different security policies arises as a problematic issue. In fact, how can we combine different or even conflicting policies with regard to privacy preserving and collaboration objectives?

In this paper, we propose a new Inter-Organizational Workflow Based Access Control (IOW-BAC) approach. Besides, we present a new algorithm to resolve potential detected conflicts occurring during the composition of the global Access Control policy. This algorithm is based on a set of important parameters which are organization's weight, object owner, task criticality and object sensitivity.

1 INTRODUCTION

Currently, Workflow Management Systems (WfMSs) (Specification, 1999) are increasingly used by companies to manage their activities through the creation of intra and inter-organizational workflows.In fact, the internet and business globalization greatly rise the creation of inter-organizational workflows. These collaborative workflows allow organization to share resources and complete common activities. However, this collaboration poses new security challenges and access control is the most crucial one. For that purpose, many access control models exist in the literature, the most common and used model is Role-based access control (RBAC)(Sandhu et al., 1996). By granting permissions to roles played by users rather than to users themselves, it has greatly facilitated the access control administration in companies. However, it was difficult for RBAC to satisfy the WfMSs security requirements . Thus, many works was raised to bridge this gap such as; Task Based Access Control (TBAC) (Thomas and Sandhu, 1998) where permissions are assigned to tasks and users can only get the permissions within the execution of tasks. Authors in (Atluri and Huang, 2000) added time constrains in their proposed solution Workflow Authorization Model (WAM) ; In Task-Role-Based Access Control (T-RBAC) (Oh and Park, 2003), authors add tasks into RBAC model, T-RBAC made permissions to be associated with tasks directly. Nevertheless, these models are more suitable for the centralized environment. On the other hand, many other researches ((Le et al., 2012),(Gouglidis and Mavridis, 2012),(Yang and Liu, 2012),(Wang et al., 2015)) were presented for distributed environment.

However, and to the best of our knowledge, none of the existing models propose an adequate model for Inter-Organizational Workflows, especially, the cohabitation of multiple access control policies of participating organization in the global workflow with the respect of organization autonomy and data security. In fact, each organization has local access control policy; the problem that arise is how to combine different or even conflicting access control policy rules. Yet, the challenge is to resolve potential conflicts and generate global access control policy . Few works devote the concern of conflict in distributed collaborative workflows such as ((Duan et al., 2015),(Ma et al., 2009),(Wang et al., 2010),(Hu et al., 2013)). However, they overlook how multiple access control policies can compose global access control policy . For that purpose, we propose a new approach named Inter-organizational Workflow Based Access Control model (IOW-BAC) that extends the RBAC model with the introduction of a new concepts and associations. Besides, we present a new algorithm to resolve potential detected conflicts occurring during the composition of the global Access Control policy. This algorithm is based on a set of important parameters which are organization weight, object owner, task

kandoussi, A. and bakkali, H.
Novel Access Control Approach for Inter-organizational Workflows.
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 345-352
ISBN: 978-989-758-282-0

criticality and object sensitivity.
The rest of the paper is organized as follows: Section 2 presents the main access control requirements in the inter-organizational workflows followed by related works in section 3. Section 4 details our proposed Inter-organizational Workflow Based Access Control (IOW-BAC) approach. The global access control policy composition was explored in section 5 . Section 6 presents un illustrative example. The last section concludes the paper with future works.

2 THE MAIN ACCESS CONTROL REQUIREMENTS

Many access control requirements have to be considered in Inter-organizational workflows. Among the main needs are policy cohabitation, privacy preserving and role mapping. Other specific requirements are presented in our previous works(Elkandoussi and Elbakkali, 2014),(Elkandoussi et al., 2015) :

1. Policies cohabitation: Policies cohabitation aim to conciliate different or even conflicting access control policies, and resolve detected conflicts. In fact, each organization must be able to protect its own data while respecting the global security policy of the global workflow.
2. Privacy preserving: Privacy arises as a major concern in todays collaboration. In fact, how to use suitable control to preserve privacy and perform cooperation needs.
3. Role mapping: role equivalence among different domains by mapping a local role to its equivalent global role.
4. Inter-organizational security contracts: To govern collaborations, security contracts are established. They aim to detail the objectives and tasks to be achieved, to attribute responsibilities to each party and to specify penalties in case of abuses.
5. Workflow Satisfiability: When different policies are combined potential conflicts may occur. Such situation may cause the workflow incompleteness. The challenge is to guarantee the workflow completeness with the respect of the global access control policy.

In order to guarantee a secured environment for participating organizations in the global workflow, the above-mentioned requirements should be considered.

3 RELATED WORKS

There are several models that have been proposed for distributed envirementents. Among these models we highlight the following.
An enhanced RBAC was proposed in (Le et al., 2012) to facilitate information access management in the context of team collaboration and workflows. Authors in (Gouglidis and Mavridis, 2012) present a new access control model for collaborative applications capable to support collaboration under secure interoperation and cardinality constraints. In (Yang and Liu, 2012), an extented model GT-RBAC (Group-Task-Role-Based Access Control) was explored. GT-RBAC introduces organization unit and hierarchies into T-RBAC model. Also, the authors present a new algorithm to meet the requirement of dynamic rights constraints of workflow. In (Wang et al., 2015), the proposed model combines Task and Role-based Access Control with multi-constraint. In the model, workflow is broken down into tasks, which are divided into public tasks and private tasks. It defines the mutually exclusive roles and binding tasks and formulates dynamic users allocation policies by establishing a users execution history table to improving the efficiency.
As mentioned before, the policies cohabitation is one of the main security requirements that should be respected. Yet, in the litterature few works devote the concern of conflict in distributed collaborative workflows. Authors in (Duan et al., 2015) present an automated policy combination for data sharing across multiple organizations. They made it possible by adopting bottom-top approach in the decomposition of the policy rules into different classes based on the subject constraints; each rule in a class that has the same subjects is combined by the condition-based attribute combination based algebraic operations. Their proposed approach makes the combined policy more restrictive, that is, the combined policy permits a request when all the policies permit it, denies a request when any one of policies denies it. Unlike our solution that take into account multiple parameters to prioritize rules. In (Ma et al., 2009), authors propose conflict detection and resolution in WFMSs. In this work, authors define a set of rules to detect and resolve static and dynamic conflict. Furthermore, they classify conflicts into two categories (i) policy-policy conflicts which occur when two or more authorization policies are considered incompatible, (ii) policy constraint conflicts which occur when the performance of two or more authorization policies will lead to situations that are prohibited by other constraints in the system. The proposed solution is based on prece-

dence rule priority which defines the order of priority to resolve conflict. In (Hu et al., 2013), a purpose-based access control model was presented in orderto preserve privacy, also a new algorithm was described to resolve conflicting policies based on purpose.The key component is purpose involved in access control models for expressing privacy-related policies. Nevertheless, authors did not present how to resolve inter-organizational policies conflict. In the context of Online Social Networks, authors in (Hu et al., 2013) , present a multiparty access control model to capture the essence of multiparty authorization requirements, also they propose Multiparty Policy Evaluation Process that include two steps and propose systematic conflict resolution mechanism to resolve conflicts during multiparty policy evaluation. Several solutions were proposed to resolve potential conflict such Threshold-based conflict resolution, Strategy-based conflict resolution with privacy and Decision Voting.

In the literature, there are many works that enhance the existing models and propose a new extended approach to support the distributed access control need. Yet, to my knowledge, none of them presents how to conciliate multiple access control policies and create global one free of conflicts in the context of distributed workflow. Furthermore, our proposed approach define a new associations and entities to meed inter-organizational workflows requirements.

4 PROPOSED INTER-ORGANIZATIONAL WORKFLOW ACCESS CONTROL APPROACH

From the security point of view, the creation of new global security policy that respects organizations security concerns is a critical requirement. Nevertheless, the enforcement of access control policy in inter-organizational workflows may cause the incompleteness of the workflow. In fact, many tasks could not be executed due to a lack of permission or policy rule conflict. In this paper, we propose new approach to conciliate different or even conflicting access control policies in whole one.

Hereafter we set out assumptions concerning this study

4.1 Preliminaries and Assumptions

In conducting this study the following assumptions were made. It was assumed that:

- We have persistent inter-organizational workflow: Cooperation between partners within inter-organizational workflows can be dynamic or persistent. When collaboration is based on permanent relation between known partners to satisfy a pre-established global workflow, the cooperation is called persistent. On the other side, the cooperation is dynamic, when organizations could join or leave the coalition based on the business needs.
- Local policies are coherent: we assume that local policies are free of conflicts.
- The initiator of the collaboration is considered as the mean participating organization in the global workflow.
- Organization weight can be calculated based on specific values (trust, importance for the collaboration), or predefined by the collaborating enterprise as agreement. For example, the organization who initiates the global workflow can set different weights values to other participating entities based on their activities dependency and organization strength in the global workflow.
- Role mapping is established between different originations, in order to map local roles into global roles that have the adequate permission to execute specific global task.

4.2 Main Steps for the Proposed Appraoch

Our approach is basically based on the definition of cooperative tasks and global access control policy. Different steps to create new global access control policy are presented in our previous work (Elkandoussi et al., 2015), we summarize the most important steps:

1. Workflow collaboration: In this step we identify the participating organizations, their weights and the global tasks assigned to each partner. We consider that global tasks are atomic tasks.
2. Public access control policy: Each partner defines how to access to his resource and under which condition.In this step the organizations can define the criticality parameters of their tasks and also the sensibility levels of their shared data (defined hereafter).
3. Security policy mapping: The security manager must control the role mapping and policy rules mapping in order to respect the local security policies.

4. Access control policies cohabitation and conflict resolution: this step aims to check different access control policy rules issued by participating organizations and resolve detected conflict. At the end of this step new global access control policy is created. Our main contribution is in this step.
5. E-contract: in order to govern the collaboration between different organization, contact is established.It contains the objective of the collaboration, the organizations responsibilities and the global access control policy.

At the end of the predefined phases, the policy of global access control of the inter-organizational workflow will be established.

4.3 The Proposed IOW-AC Model

Each participating organization in the global workflow may already have adopted an access control model. As RBAC is the most popular access control model, we assume that participating enterprises use RBAC or TRBAC as an extension of RBAC. In the IOW-BAC, a set of organizations participate to a global workflow which is composed of multiple global tasks. Each global task is assigned to global role; global roles are mapped to local roles.

As shown in figure 1 , IOW-BAC model includes many entity sets, as well as the relations and functions between them, we will give the formalized definition of IOW-BAC, only increased or changing definitions, the local access control models deployed in participating enterprises will not be detailed.

- Entities:
  Users, Roles, Global Roles, Permissions, Global Workflow, Organizations and Global Tasks are:
  1. $U = \{u_i | i = 1,2,\ldots,n\}$ is a set of users, each user belongs to an organization
  2. $R = \{r_i | i = 1,2,\ldots,n\}$ is a set of roles, each role belongs to an organization
  3. $P = \{p_i | i = 1,2,\ldots,n\}$ is a set of permissions, The permission $P_i = (Op_i, Obj_i)$ denotes the set of operations on objects
  4. $Op = \{Op_i | i = 1,2,\ldots,n\}$ is a set of atomic operations on objects
  5. $Obj = \{Obj_i | i = 1,2,\ldots,n\}$is a set of objects $GW = \{GW_i | i = 1,2,\ldots,n\}$ is a set of global workflows
  6. $O = \{O_i | i = 1,2,\ldots,n\}$is a set of organizations
  7. $GR = \{GR_i | i = 1,2,\ldots,n\}$ is a set of global roles
  8. $GT = \{GT_i | i = 1,2,\ldots,n\}$is a set of global tasks
  9. $GW = \{O, GR, GT\}$ is a global workflow
     We define a global task GT as $GT = \{O_t, GT_{name}, GR_t, P_t\}$ where: O_t is a set of all organizations that can perform the task T
     GT_{name} is the name of the task
     GR_t is a set of all global roles can perform the task T
     P_t is a set of all necessary permissions to perform the global task GT , $P_t = \{Op_t, Obj_i\}$ a set of operations actions on objects
- Associations
  In addition to the existing association in the RBAC model, we define new association for IOW-BAC ,
  1. U-O-A $\subseteq U \times R$ is User Organization Assignement, $(u,o) \in$ U-O-A shows that user u is the member of organization O
  2. U-R-A $\subseteq U \times R$ is User Role Assignement
  3. O-R-A $\subseteq O \times R$ is Organization Role Assignement , $(r,o) \in$ O-R-A shows that role r is belonged to user Organization O
  4. O-GW-A $\subseteq O \times GW$ is Organization Global Workflow Assignement, $(o,gw) \in$ O-GW-A shows that organization o is participating in the global workflow gw
  5. GR-GT-A $\subseteq GR\times$ GT is the Global Role Global Task Assignement
  6. GT-O-A $\subseteq GT \times O$ is the Global Task Organization Assignement,$(t,o) \in$ GT-O-A shows that global task GT is executed by o
  7. Obj-O-A $\subseteq Obj \times O$ is Object Organization Assignement
  8. GT-GW-A $\subseteq GT \times GW$ Global Workflow Global Task Assignement
  9. GT-P-A $\subseteq GT \times P$ is Task Permission Assignement $RM\,(R_i, GR_i)$ define Global Roles that can execute Global Tasks. Role mapping provides a decentralized access control. $RM\,(R_i, GR_i)$ means that the Role R_i is mapped to Global Role GR_i. That means that R_i can execute GT_i with permission assigned to GT_i, in order to respect least privilege.
- Functions
  1. Roles functions: $GT \cup R \cup GR \to 2^R$
     $f_r(T_i) = \{r \in R | ((T_i, GR) \in$ RG-GT-A $\wedge RM\,(R, GR))\}$ this function relies the Role R to the global tasks T.
  2. Global Tasks functions: $O \to 2^{GT}$
     $f_t(O_i) = \{t \in GT | (O_i, t) \in$ O-GT-A $\}$
  3. User functions: $GT \cup GR \cup R \to 2^U$
     $f_u(GR) = \{u \in U | ((u,r) \in$ U-R-A $\wedge RM\,(R, GR))\}$

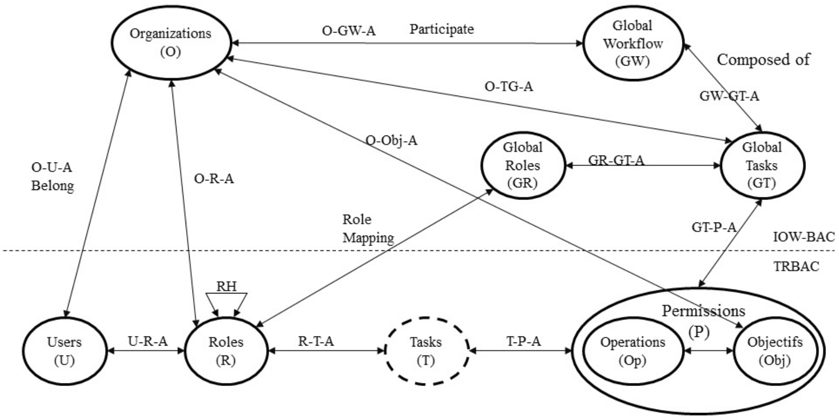

Figure 1: Proposed IOW-AC model.

$f_u(T_i) = \{u \in U \,|\, \exists r \in R \,, (u,r) \in$ U-R-A $\wedge (R,GR) \wedge (GR,GT) \in$ GR-GT-A $\}$
$f_u(T_i)$ denotes eligible users set that can execute Global Task T.

4. Organization functions: $Obj \rightarrow 2^O$
$f_{obj}(o_i) = \{obj \in Obj | (obj_i, o) \in$ Obj-O-A $\}$

5 GLOBAL ACCESS CONTROL POLICY COMPOSITION

In this paper, we aim to compose global policy P_g based on multiple public policies. A proposed approach is based on organization weight, task criticality and object sensitivity.

5.1 Access Control Policy

We define access control rules in our model as $AR = \{O, GT, GR, Op, Obj\}$Where O is organization, GT is global task, GR is global role, in our example role includes staffs of hospitals such as doctor and nurse, Op is operation, Obj is an object. The $AR = \{O, GT, GR, Op, Obj\}$ indicates that any user in organization O with global role GR is authorized to exercise operation Op on object Obj when he/she performs global task GT .

5.2 Criteria Specification

In our approach we define new essential criteria that are used to resolve potential policy conflicts; organization weight, Object sensitivity level and Task criticality level. We chose the main requirements in workflows system in order to compose coherent global access control policy, hereafter their definition.

1. Organization weight: this parameter can be calculated based on specific values (trust, importance for the collaboration), or predefined by the collaborating enterprise as agreement. In our case study, we assume that the organization who initiates the global workflow can set different weights values to other participating entities based on their contribution in the global workflow. each organization has a specific value α_i , we have $\sum_{i=1}^{n} \alpha_i = 1$

2. Object Sensitivity Level: each organization should specify the object sensitivity level of his data that refers to her privacy concern. The OSL has range between [0,1] based on the object confidentiality level.
For example if the confidentiality is: High → OSL=1 , Medium → OSL=0.5, Low → OSL= 0
The Global Object Sensitivity Level GOSL is defined as the sum of each organization O_i for a specific data. The global Object sensitivity level should take into account the organization weight. Organization weights are represented as α_i and n is the number of participating organization in the collaboration. A GOSL is calculated as follows:

$$GOSL(Obj, O_i) = \frac{\sum_{i=1}^{n} (\alpha_i \times OSL_i)}{\sum_{i=1}^{n} \alpha_i}, i = 1, \ldots, n \quad (1)$$

3. Task Criticality Level (TCL): TCL is based on the importance of the task. Each organization should define this parameter for a set of tasts that will execute.
For example if importance of the task is High → OSL=1, Medium→ OSL=0.5, Low → OSL= 0.
Organizations weight is introduced in the Global Task Criticality Level (GTCL) .A GTCL is calcu-

lated as follows:

$$GTCL(T,O_i) = \frac{\sum_{i=1}^{n} (\alpha_i \times TCL_i)}{\sum_{i=1}^{n} \alpha_i}, i = 1,\ldots,n \quad (2)$$

If the task is urgent, the policy should be permissive especially in health domain

5.3 Our Proposed Conflict Resolution Algorithm

As we defined previously, Access Control Policy Rule in organization O_i is $AR_{ih} = \{O_i, GT_{ih}, GR_{ih}, Op_{ih}, Obj_{ih}\}$, AR_{ih} indicates that any user in organization O_i with global role GR_{ih} is authorized to exercise operations Op_{ih} on object Obj_{ih} when he/she performs the global task GT_{ih} . Also in organization O_k , we define $AR_{km} = \{O_k, GT_{km}, GR_{km}, Op_{km}, Obj_{km}\}$, AR_{km} indicates that any user in organization O_k with global role $GR_{km}$is authorized to exercise operations Op_{km} on object $Obj_{km}$when he/she performs task T_{km}.
The algorithm 1 hereafter describes the conflict rule detection between two different access control rules.

Algorithm 1: Conflict rule detection.

```
    Input:
$n$ is the number of organizations in the collaboration
$AR_{ih}$ is pol Access Control Policy Rule h in organization $O_i$
where $AR_{ih} = \{O_i, GT_ih, GR_ih, Op_ih, Obj_ih\}$
$AR_{km}$ is Access Control Policy Rule m in organization$O_k$
where $AR_{km} = \{O_k, GT_km, GR_km, Op_km, Obj_km\}$
$nb_{AR}(O_i)$is the number of Access Control Policy Rule in organization $O_i$
$nb_{AR}(O_k)$ is the number of Access Control Policy Rule in organization $O_k$
    Output :ConfRule is a list of conflicting rules
for $i \leftarrow 1$ to $n-1$
    for $k \leftarrow i+1$ to $n$
        for $h \leftarrow h$ to $nb_{AR}(O_i)$
            for $k \leftarrow m$ to $nb_{AR}(O_k)$
                if $(GT_{ih} = GT_{km}) \wedge (GR_{ih} = GR_{km}) \wedge (Obj_{ih} = Obj_{km}) \wedge (Op_{ih} \cap Op_{km} \neq \varnothing)$ then
                    $ConfRule \leftarrow (AR_{ih}, AR_{km})$
                else
                    $m \leftarrow m+1$
                end if
            end for
            $h \leftarrow h+1$
        end for
        $k \leftarrow k+1$
    end for
    $i \leftarrow i+1$
end for
return $ConfRule \leftarrow (AR_{ih}, AR_{km})$
```

In our algorithm 1, we compare the Access Control Policy Rule two by two for all participating organizations in the collaboration. In our case the conflict is detected if we have different set of operations for the same global task executed by the same global role on the same object.

Algorithm 2: Global Access Control Policy Composition.

```
    Input:
$\alpha$ is the organization weight,we have $\alpha_i > \alpha_j$
$f_{obj}(O_i) = \{obj \in Obj | (obj, O_i) \in Obj - O - A\}$ fonction that return a set of objects that belong to organization $O_i$
$f_{obj}(O_j) = \{obj \in Obj | (obj, O_j) \in Obj - O - A\}$ fonction that return a set of objects that belong to organization $O_j$
$GTCL(GT, O_i, O_j)$ is Global Task Criticality Level || GTCL is define in section X, $GTCL(GT, O_i, O_j) = \frac{(\alpha_i TCL_i(GT) + \alpha_j TCL_j(GT))}{\alpha_i + \alpha_j}$
$GOSL(Obj, O_i, O_j)$ is Global Object Sensitivity Level || GOSL is define in section XX, $GOSL(Obj, O_i, O_j) = \frac{(\alpha_i OSL_i(Obj) + \alpha_j OSL_j(Obj))}{\alpha_i + \alpha_j}$

    Output :
$AR_g$ is Global Access Control Policy Rule , $AR_g = \{GT, GR, Op_g, Obj\}$
$list \leftarrow ConfRule(AR_i, AR_j)$
if $list \neq \varnothing$ then
    for each $(AR_i, AR_j) \in list$
        if $Obj \in f_{obj}(O_i)$ then
            $AR_g \leftarrow AR_i$ || if the organization with higher weight is the object owner then we prioritize its rule and put it in the global policy
        else
            if $Obj \in f_{obj}(O_j)$ then || if the Obj belong to the organization with lower weight, we have two case

                if $Op_i \subset Op_j$ then $AR_g \leftarrow AR_i$
                end if
                if $Op_j \subset Op_i$ then
                    if $GTCL(GT, O_i, O_j) \geqslant GOSL(Obj, O_i, O_j)$ then
                        $AR_g \leftarrow AR_i$ || if the task is critical and must be executed, we prioritize the permissive rule.
                    else $GTCL(GT, O_i, O_j) < GOSL(Obj, O_i, O_j)$
                        $AR_g \leftarrow AR_j$ || if the object is more sensitive and confidential we prioritize the restrictive rule to preserve privacy.
                    end if
                end if
            end if
        end if
    end for
end if
```

Our proposed algorithm 2, if the organization with higher weight is the owner of the object , we prioritize

Table 1: Global Inter-Organizational Workflow specifications.

Organization O_i	Global Tasks GT	Global Roles GR	Operations Op	Objects Obj
$O_1 = HospitalA$	$GT_1 =$ radio exam	$GR_1 =$ doctor	$Op_1 =$ read	$Obj_1 = F_1$
$O_2 = HospitalB$	$GT_2 =$ blood test	$GR_2 =$ nurse	$Op_2 =$write	$Obj_2 = F_2$
$O_3 = Lab_1$	$GT_3 =$ ask other opinion			

Table 2: Access Control Policy Rules.

Organization O_i	Access Rule
O_1	$AR_{11} = O_1, GT_1, GR_1, (Op_1 \cup Op_2),$
	$AR_{12} = O_1, GT_2, GR_2, Op_1, F_1$
	$AR_{13} = O_1, GT_3, GR_1, (Op_1 \cup Op_2), F_1$
O_2	$AR_{21} = O_2, GT_1, GR_1, Op_1, F_1$
	$AR_{22} = O_2, GT_3, GR_1, (Op_1 \cup Op_2), (F_1 \cup F_2)$
O_3	$AR_{31} = O_3, GT_1, GR_1, (Op_1 \cup Op_2), (F_1 \cup F_2)$
	$AR_{32} = O_3, GT_2, GR_1, (Op_1 \cup Op_2), (F_1 \cup F_2)$

its access policy rule. However, if the object belongs to the organization with lower weight, we compare GTCL and GOSL in order to decide which policy is privileged. In fact, if the task is critical and must be executed, we prioritize the permissive rule.Otherwise , the object is more sensitive and confidential we prioritize, then we prioritize restrictive rule to preserve privacy.

6 ILLUSTRATIVE EXAMPLE

Healthcare organizations are currently facing pressure to improve productivity and to reduce costs while at the same time the demand for more hospital services is increasing. In order to provide optimal care for patients, Healthcare organizations decide to use WFMSs to establish inter-organizational collaboration. However, these systems are facing security threads and are requiring a security mechanism, particularly access control.

6.1 E-health Inter-organizational Workflow Example

Hospital A would like to create an inter-organizational workflow with other hospitals and health centers to execute specific tasks. In fact, Hospital A would like to create collaboration with hospital B for the task Radio Exam and specialist opinion, and with lab_1 for radio exam task and blood test task (in emergency case, overloaded work or specific radio not covered by the hospital). On the example mentioned before, we have the flowing AR defined by each organization. Potential conflicts can be detected. For example, for the task radio exam, the doctor in O_2 can read and write in the object F_1 based on the AR_{11}, but he cannot write in F_1 based on A_{21}.

6.2 Global Access Control Policy Composition

Based on the information given by O_1 and O_2, we have to calculate $GTCL(GT_1, O_1, O_2)$ and $GOSL(F_1, O_1, O_2)$.
we assume that $TCL(GT_1, O_1) = 0.5$, $TCL(GT_1, O_2) = 0.5$, $OSL(F_1, O_1) = 1$, $OSL(F_1, O_2) = 0.5$, $\alpha_1 = 0.5$, $\alpha_2 = 0.3$.
we calculate the GTCL and GOSL based on equation (1) and (2) we have:
$GTCL(GT_1, O_1, O_2) = 0.875, GOSL(F_1, O_1, O_2) = 0.812$.
Based on Global Access Control Policy Composition algorithm, we have :

1. If $F_1 \in f_{obj}(O_1) then AR_g \leftarrow AR_{11}$
2. If $F_1 \in f_{obj}(O_2) and Op_2 \subset Op_1$ then we compare GTCL and GOSL
   In our case $GTCL(GT_1, O_1, O_2) > GOSL(F_1, O_1, O_2)$ Then $AR_g \leftarrow AR_{11}$

The proposed algorithm helps as to combine multiple access control policy rules in order to compose global access control policy free of conflicts. However, potential conflict may persist if the participating organization did not accept the proposed solution to resolve it. In this case, we can go to the negotiation step where other specific criteria should be considered.

7 CONCLUSION AND FUTURE WORK

In this paper, we propose a new Inter-Organizational Workflow Based Access Control (IOW-BAC) approach. The new approach extends RBAC model with a new entities and associations in order to support the main requirements of distributed workflow systems. Besides, we present a new algorithm to resolve potential detected conflicts occurring during the composition of the global Access Control policy. This algorithm is based on a set of important parameters. The organization weight, the object owner, object sensitivity level and the task criticality level to evaluate the importance of the executed task.
The next stage of our work is the implementation of our approach using the eXtensible Access Control Markup Language (XACML) standard. Moreover, we look to propose a new approach based on automated negotiation.

REFERENCES

Atluri, V. and Huang, W.-K. (2000). A petri net based safety analysis of workflow authorization models1. *Journal of Computer Security*, 8(2-3):209–240.

Duan, L., Chen, S., Zhang, Y., Liu, C., Liu, D., Liu, R. P., and Chen, J. (2015). Automated policy combination for data sharing across multiple organizations. In *Services Computing (SCC), 2015 IEEE International Conference on*, pages 226–233. IEEE.

Elkandoussi, A. and Elbakkali, H. (2014). On access control requirements for inter-organizational workflow. In *Security Days (JNS4), Proceedings of the 4th Edition of National*, pages 1–6. IEEE.

Elkandoussi, A., Elbakkali, H., and Elhilali, N. (2015). Toward resolving access control policy conflict in inter-organizational workflows. In *Computer Systems and Applications (AICCSA), 2015 IEEE/ACS 12th International Conference of*, pages 1–4. IEEE.

Gouglidis, A. and Mavridis, I. (2012). domrbac: An access control model for modern collaborative systems. *computers & security*, 31(4):540–556.

Hu, H., Ahn, G.-J., and Jorgensen, J. (2013). Multiparty access control for online social networks: model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, 25(7):1614–1627.

Le, X. H., Doll, T., Barbosu, M., Luque, A., and Wang, D. (2012). An enhancement of the role-based access control model to facilitate information access management in context of team collaboration and workflow. *Journal of biomedical informatics*, 45(6):1084–1107.

Ma, C.-h., Lu, G.-d., and Qiu, J. (2009). Conflict detection and resolution for authorization policies in workflow systems. *Journal of Zhejiang University-Science A*, 10(8):1082–1092.

Oh, S. and Park, S. (2003). Task–role-based access control model. *Information systems*, 28(6):533–562.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2):38–47.

Specification, W. (1999). Workflow management coalition terminology & glossary (document no. wfmc-tc-1011). *Workflow Management Coalition Specification*.

Thomas, R. K. and Sandhu, R. S. (1998). Task-based authorization controls (tbac): A family of models for active and enterprise-oriented authorization management. In *Database Security XI*, pages 166–181. Springer.

Wang, B. Y., Zhang, W. X., and Zhang, S. M. (2015). An improved task and role-based access control model with multi-constraint. In *Applied Mechanics and Materials*, volume 713, pages 2532–2535. Trans Tech Publ.

Wang, H., Sun, L., and Varadharajan, V. (2010). Purpose-based access control policies and conflicting analysis. In *SEC*, pages 217–228. Springer.

Yang, W. and Liu, Y. (2012). An organization-based access control model for workflow and dynamic constraints implementation. *I JACT: International Journa lof Adv ancements in Computing Technology*, 4(1):477–484.