International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-3, Issue-2 May 2013

Multi-Trust_Or BAC: Access Control Model for Multi-Organizational Critical Systems Migrated To the Cloud

Mustapha Ben Saidi, Abderrahim Marzouk

Abstract--Security of information systems is a problem chronic, the arrival of cloud computing as a new computing model, feeds the difficulty of implementing effective solutions. Thus more research is currently focused on data security in the cloud, and especially the issue of confidentiality. In this paper we propose a new protocol access control for complex, heterogeneous, interoperable, and distributed systems in the context of Cloud Computing : « Multi-TrustOrBAC » (Multi-Organization - Trust Based Access Control). This protocol allows a TTP «Trust Tierd Party [10] » to force users belonging to several organizations to cooperate to meet the security policies defined independently by them. The aim is to offer to organizations working together and having decided to migrate to the cloud, a means of real-time monitoring of their safety. Our solution is based on both the concept of trust assigned to users and to the definition of an order on the set of security policies. The logical formalism is used to specify and describe the rules of the security policies of different organizations.

Keywords: Policy security, interoperable system, heterogeneous and distributed systems, actions weighted, access control.

I. INTRODUCTION

Cloud computing is a new computing model that is attracting more and more, thanks to the benefits they advance [5]. But, like any other generation of computing platforms, it has many challenges to overcome. The big challenge is that data security will be in another third uncontrollable. Hence the issue of trust cloud operators and users with access to corporate data. [7]. Several research focuses therefore on new models of access control incorporating human character [8,9]. **TOrBAC** model [1,2] "***Trust Organization Based Access Control***" is a newly developed protocol. It is based on the concept of capital or confidence index and the notion of an order on the set of policies to control the actions of users in an organization.

In TOrBAC, UML models, safety rules (eg, permissions) are based on one organization where views, objects, activities and actions are defined uniquely and consistently. Therefore it is impossible to apply in the following two situations:

- On the one hand when it comes to an organization must have both documents in various formats to meet their own needs or the needs of its external collaborators. For example, it may have XML files (or Word, or other) for administrative files and text files (or databases, etc.) to supplier files.
- On the other hand, when it is also independent organizations to collaborate in an outsourcing to a cloud of their heterogeneous SI. A topic that has several of its organizations must be able to perform different actions on heterogeneous objects of different origins.

TOrBAC therefore does not meet the needs of distribution, collaboration and heterogeneity. It therefore seems necessary to extend T (rust) Or-BAC to suit these needs. Multi-OrBAC Trust model is an extension TOrBAC. It covers the wealth of collaborative systems, distributed and interoperable.

In this paper we recall in the first section the principle of Multi-model OrBAC, then in the second we introduce the concepts used in TOrBAC. The third section is to adapt the model to a Multi TOrBAC organizational lead for the fourth section the construction of the new protocol for TTP [10] to monitor security policies independent organizations and collaborators. Finally, we conclude in section 5.

II. MULTI-MODEL ORBAC

This model is an extension of OrBAC model [4] (relative to a single organization) to several organizations. It covers the needs of distribution, collaboration and heterogeneity that is lacking in OrBAC model. Multi-model OrBAC [3] takes into account the fact that each organization can define its views, its objects, activities and actions in several ways. So that action performed by a subject on an object becomes dependent on both an organization and a view of an activity and not only objects to which it applies.

A. Activité dans Organisation (AdO)

Organizations can perform the same activity differently, for example: if we consider the activity "reading", it can fit in the organization Org1, action "read ()", but can equally match action "select" in Org2. We model this situation by introducing the class AdO "activity organization" as an association class between activities and organizations (Figure 1).

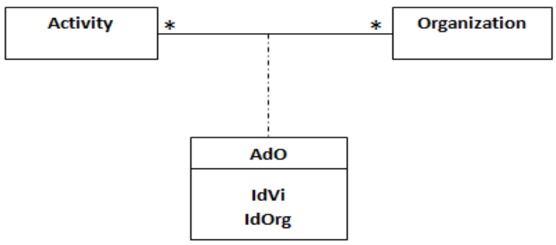


Fig 1 : Activity in the Organization

Manuscript received on May, 2013.
Mustapha Ben Saidi. FST Settat University Hassan 1 Settat Department of Mathematics and computers sciences Lab. MAI; Morocco.
Abderrahim Marzouk. FST University Hassan 1er Settat Department of Mathematics and computers sciences; Lab MAI Morocco.

B. View in Organization (VdO)

A view shows how objects are used in an organization. Note here that the same view can be defined differently depending on the organization: A view V can be set in Org1 as a set of XML documents, while at the same Org2 view corresponds to a table in one or more database. We introduce the class-association "View in Organization" (VdO), and we associate objects to VdO (Figure 2).

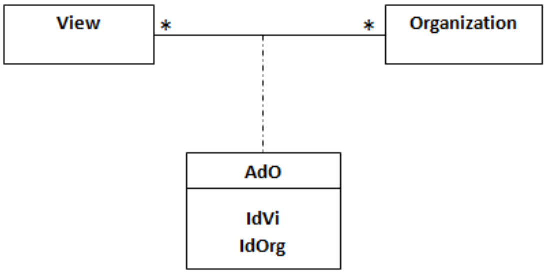


Fig 2 : View in an Organization

Note that in Multi-OrBAC, the action depends not only on the activity and organization, but also of the view. It may therefore well have- in the same organization-heterogeneous views (that is to say, on which you can perform different actions).

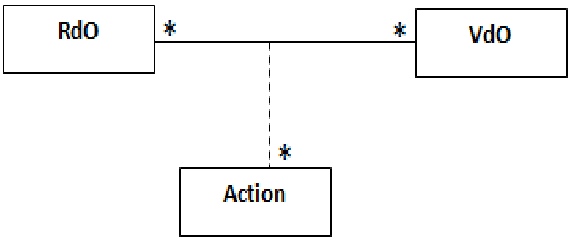


Fig 3 : Role in an Organization

C. Actions Weighted [1,2]

Actions performed within an organization are weighted by a weight between 0 and 1. They are then five types :

- Prohibitions are actions zero weight.
- Obligations are actions of weight 1.
- Permissions are actions of weight 0.5.
- Pre- Prohibitions are actions of weight between 0 and 0.5.
- Pre-obligations are actions of weight between 0.5 and 1.

A pre-interdictions (resp pre-obligations) become prohibitions (resp obligations) after a certain number of times violations.

D. User Account in an Organization

In a multi-organizational same subject can be linked to several organizations. It can then perform different actions on objects belonging to different organizations. We can attribute in this case to a subject a user account in an organization. This account has then an identifier of the organization, and identifying the subject of trust. Account user therefore has the characteristics of a class and an association and as such can be described by a class of association in UML notation [Figure 4]. We consider in this paper a subject can have only one account in an organization to enable it to perform actions on the objects of the organization.

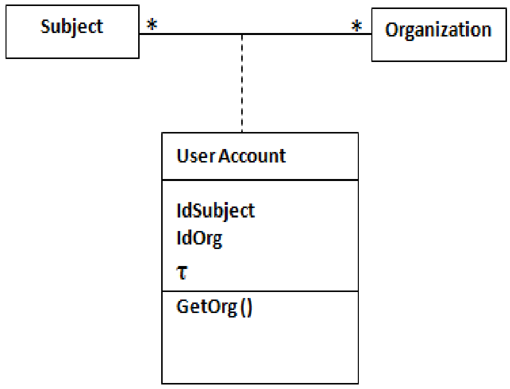
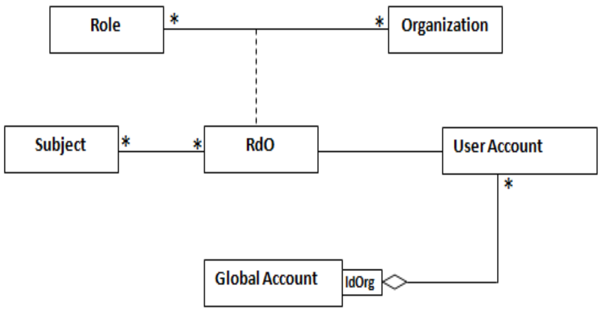


Fig 4: Account of the Subject in an Organization

This way of modeling is used to associate a user account a series of policies rather than as a subject in the case of a single organization [1,2]. So an individual can be assigned as many suites political organizations to which it belongs.

Remark: Can be considered a subject can be to play several roles in one or more organizations and each role has a user account. In this way an individual can have so many accounts in the same organization. In the following section, we assume that subject has one and only one user account that includes previous accounts whatever roles. This is illustrated in the following diagram:



For a user account ***cu***, an action ***α*** and object ***o***, we define the following predicates:

- *Obligation* ***(cu, α, o)*** *<u>if and only if</u>* ***cu*** *is obliged to perform* ***α*** *on* ***o***.
- *Interdiction* ***(cu, α, o)*** *<u>if and only if</u>* ***cu*** *is forbidden to perform* ***α*** *on* ***o***.
- *Permission* ***(cu, α, o)*** *<u>if and only if</u>* ***cu*** *has permission to perform* ***α*** *on* ***o.***
- *Pre- Prohibition* ***(cu, α, o, w)*** *<u>if and only if</u> weight(**α**)=**w and cu*** is forbidden to perform ***α*** on ***o***.
- *Pre-Obligation* ***(cu, α, o, w)*** *<u>if and only if</u> weight(**α**)=**w and cu** is obliged to perform **α** on **o.***

III. SECURITY POLICIES ASSOCIATED WITH A USER ACCOUNT

A. Définition :

A security policy in an organization is a set of actions weighted objects belonging to the organization and assigned a user account. In the following, we denote by **w (α, P)** the weight of the Action α belonging to the policy P.

We assume that each organization has the autonomy to define its own security policies.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

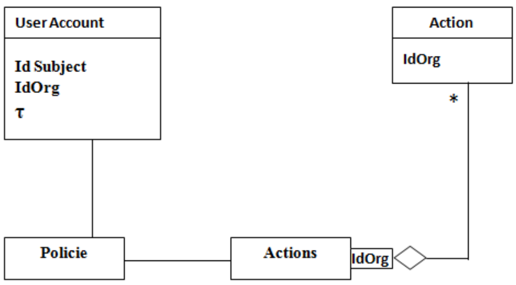


Fig 5: Diagram linking policies to user accounts.

The term "**IdOrg**" is used to reflect the fact that each instance "Actions" is comprised of multiple instances "Action" that are associated with the same organization.

B. *Order on security policies:*

P1 and P2 are two security policies in an organization. Then P2 is stricter than P1 (and there P2 <P1) ***if and only if***:

- *P1 and P2 contain the same actions weighted.*
- *Either there is a pre-requirement α belonging to P1 (thus P2) such that w (α, P1) <w (α, P2), or there is a Pre- Prohibition that α belonging to P1 (thus P2) such that w (α, P1)> w (α, P2).*

C. *Switching security policies*

We say that a user accounts ***cu*** rocking a policy ***P*** to a policy ***P*** ', and there *Switches (cu, P, P')*, ***if***:

- *P and P' contain the same actions weighted.*
- *Account **cu** violates a Pre-Obligation or violates a Pre-Prohibition **α** belonging to **P***
- *The policy **P'** is obtained from **P** by changing the weight of action **α**.*
- *Policies **P** and **P'** are successively affected to **cu** by the TTP.*

Corollary:

Let ***cu*** a user account and **P** and **P'** two security policies defined in the same organization. Then we have:

Switches (cu, P, P') ➔ P'<P.

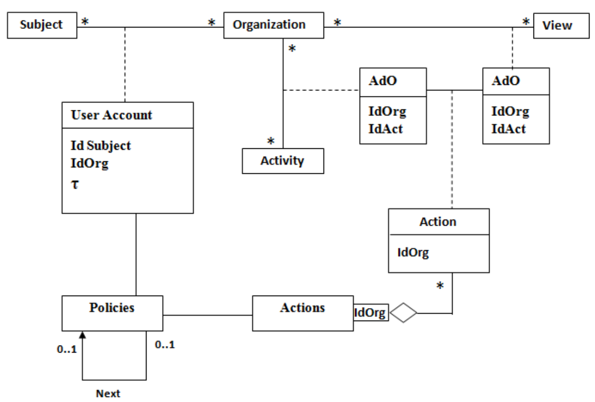


Fig 6: Diagram for switch policies.

Proposition:

Let 𝒫 be the set of policies assigned to a <u>user account</u> for its various connections to the cloud. If P contains a security policy 𝒫 containing only permissions, obligations and prohibitions then P is minimal in 𝒫 with respect to the order < defined on the set of security policies.

Proof: see [1]

We note later in this article:

- **PMIN(cu,Org)** a minimal policies assigned by an organization Org, a user account cu;
- **PMAX(cu,Org)** a policies maximum is given to cu at its first connection to the cloud;
- **PPUB(Org)** a public policies granted to a user account that does not contain any of the permissions set by the Administrator SI organization Org.

IV. BUILD A PROTOCOL FOR MONITORING A SECURITY POLICIES

A. *Principle of the monitoring protocol:*

To force a subject to comply with the rules of its policies, a TTP must ensure compliance with the security policy assigned to each user account activity on the Cloud. It monitors their actions and rape her confidence index is then lowered and/or its current switches to a more stringent policy.

Note first that only the actions of different weights of 0.5 could be violated.

Signalons d'abord que seules les actions de poids différents de 0,5 pourraient être violées. To switch a user account to a minimum political organization after a series of violations, we propose a monitoring protocol based on the following four rules regardless of the organization:

Rule 1: For any violation of a prohibition or obligation, their weight remains constant for all connections unlike index declining confidence of a fixed amount in advance by the CIO organization.

Rule 2: For each violation of a pre-prohibition, its weight and the confidence index falling by user account amounts set by the system administrator information (DSI) of the organization. Therefore such actions are transformed into prohibitions after a finite number of violations because their weight will eventually become zero.

Rule 3: For any breach of a pre-requirement, weight and undergoes an increase in the confidence index of the user account undergoes a decrease amounts set by the DSI. Therefore such actions are transformed into bonds after a finite number of violations because their weight will eventually become equal to 1.

Rule 4: If a user account reaches a minimum policy or if its confidence index reached a threshold set by the DSI organization, then automatically switch to public policy PPUB (Org) on the organization Org.

The development of this protocol is shown in the following algorithm:

<u>**Algorithm:**</u>

initialization:

*Assigned to each user account cu its capital and political trust initial maximum **PMAX(cu,Org).***

*P ← **PMAX(cu,Org).***

Procedure :

While (P≠PPUB(Org)) Do

{

For any violation of a prohibition or obligation to apply the "Rule 1".

For any violation of a pre- prohibition

apply the "Rule 2".
For any violation of a pre-obligation to apply the "Rule 3".

If cu attained a minimal policy or if its confidence index attained a level set by the DSI organization Org, then
apply **"Rule 4":** P←PPUB(Org).
}

B. *Role of TTP in the context of Cloud:*

TTP must ensure compliance with security policies granted to each subject (so its different user accounts). It applies the monitoring protocol described above to each user account. For each violation, a subject sees its security policies switch to a new stricter policy or one of its lower confidence indices. Each subject s can then pass on his connections suites strictly decreasing security policies. Each suite is of the form ***(P1, P2, ... Pk)*** where ***P1, P2, ... Pk*** are defined security policies in an organization Org, assigned to the same user account cu s and contains the same actions weighted with ***P1 = PMAX(cu, Org)>P2>……..> Pk =PMIN(Org) and Switches(cu, Pi, Pi+1).***

At the limit, an individual may end up with only user accounts associated with public policies in each of its organizations.

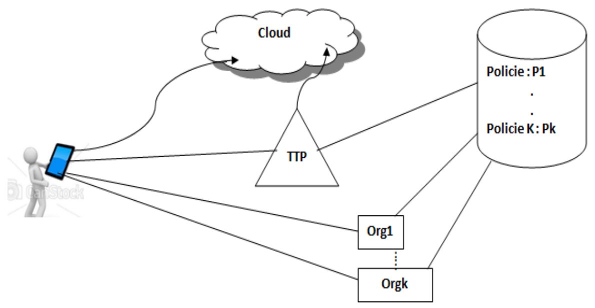


Fig 7 : Illustration of connection to the global count Cloud, monitored by the TTP

C. *UML Modeling*

Note here is that UML perfectly suited to represent several aspects related to security policies and violations thereof[1].

We denote by Violation entity can represent attempts violations weighted by the share user accounts. This entity is of type (user_account, Action, Object) and defined by:

Violation (cu, α, o) **means:**

The user account cu violates action α using the object o, i.e. ***if and only if*** *the action **α** is an obligation to object **o** and **cu** has not met, or action **α** is a prohibition for the object **o** and **cu** account tried to make or action **α** is a pre-prohibition or pre-obligation and **cu** tried to its negation (or its inverse).*

D. *Axioms:*

We give her some logical rules that formally express the notion of breach and its consequences.

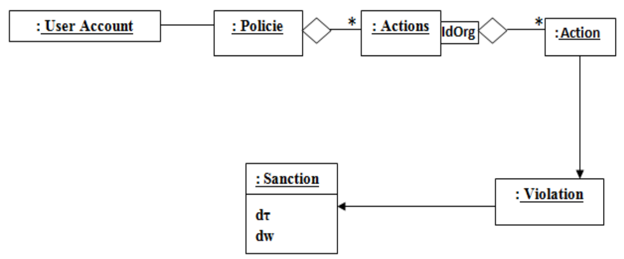
1. ∀cu ∀α∀o
   Violation(cu, α, o) <==>
   ¬*Obligation (cu, α, o)* ∨
   Prohibition (cu, α, o) ∨
   ¬*Pre-Prohibition (cu, α, o)* ∧
   ¬*Pre-Obligation (cu, α, o).*
2. ∀cu ∀α∀o
   Violation(cu, α, o) ===>
   confidence index "Account cu" down ∨
   the weight of α is modified.
3. ∀cu ∀α∀o
   ¬*Obligation (cu , α, o)* ===>
   Violation(cu, α, o) ∧
   confidence index "Account cu" down.
4. ∀cu ∀α∀o
   Prohibition (cu, α, o) ===>
   Violation(cu, α, o) ∧
   confidence index "Account cu" down.
5. ∀cu∀α∀o∀w
   ¬ *Pre-Prohibition (c, α, o)* ===>
   Violation(cu, α, o) ∧
   confidence index "Account cu" down ∧
   diminishes the weight of α.
6. ∀cu ∀α∀o∀w
   ¬ *Pre-Obligation (cu , α, o)* ===>
   Violation(cu, α, o) ∧
   confidence index "Account cu" down ∧
   increases the weight of α.

Associations: *Assigns, Control and Modify* keep the same meaning as in [1, 2] even if we replace a subject ***s*** by one of his accounts ***cu***. By cons, we are redefining the association *Modify* taking into account the organization is the account ***cu*** by:

Modify (TTP, P, cu) <==>
Control(TTP,cu)∧
cu.indextrust() down ∧

if ∃ P' such as P'≠ PMIN(cu.getOrg())∧
Switches (cu, P,P') ∧
Assigns(TTP,cu,P').

It follows the following UML diagram:



For each violation committed by a user account, a penalty is characterized by two attributes dτ and dw respectively which represents the amount set by the DSI to be subtracted from the confidence index current user account and the amount to add or subtract weight to action violated.

V. CONCLUSIONS AND PERSPECTIVES

In this article, we presented a new protocol for monitoring and controlling access to information systems constituted by several organizations, and must cooperate by moving their SI to a Cloud. This protocol takes into account the characteristics of complex systems, heterogeneous and distributed. It allows organizations to delegate control of their security policy to a third party TTP. This allows them to apply security policies to user accounts based on their membership organizations.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

So we extended the control protocol violation of article [1] to one that takes into account belonging to several organizations. This protocol is also true for organizations wishing to integrate and cooperate in a cloud environment. Seen that the InterCloud promises to be a federation of Cloud, we note that our new protocol remains valid for such an environment. It remains to implement and validate our protocol and then apply it to a real case. For example, the case of academic medical centers, including such a solution will be significantly beneficial to push the advantage degree of cooperation academic medical centers in many areas of research and medical treatment.

REFERENCES

[1] Mustapha Ben Saidi – Abderrahim Marzouk Journal : International Journal of Soft Computing & Engineering ISSN: 22312307 Year: 2012 Volume: 2 Issue: 5 Pages: 134-138 Provider: DOAJ Publisher: International Journal of Soft Computing & Engineering

[2] Mustapha Ben Saidi - Anas Abou Elkalam - Abderrahim Marzouk Journal: International Journal of Soft Computing & Engineering ISSN: 22312307 Year: 2012 Volume: 2 Issue: 4 Pages: 122-130 Provider: DOAJ Publisher: International Journal of Soft Computing & Engineering

[3] Anas Abou Elkalam Yves Deswarte Multi-OrBAC :un modèle de contrôle d'accès pour les systèmes multi-organisationnels Anas Abou El Kalam LIFO-ENSI de Bourges ;LAAS - CNRS ;

[4] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel et G. Trouessin. Organization Based Access Control. IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003), Lake Come, Italy, June 4-6, 2003.

[5] Ouvrage : « Cloud Computing, une rupture décisive pour l'informatique d'entreprise ». Guillaume Plouin 2ème édition-2011.

[6] Anas Abou ElKalam, Philippe BalbianiEmerging :Policy Language for Modelling Recommendations - Challenges for Security, Privacy and Trust IFIP Advances in Information and Communication Technology Volume 297, 2009, pp 176-189

[7] Effective Ways of Secure, Private and Trusted Cloud Computing Article Authors: Kumar Pardeep --- Sehgal VivekKumar --- Chauhan Durg Singh --- Gupta P. K. Diwakar ManojYear: 2011 Provider: arXiv

[8] Dimitrios Zissis and Dimitrios Lekkas Addressing cloud computing security issues Journal : Future Generation Computer Systems Volume 28, Issue 3, March 2012, Pages 583–592

[9] P.G. Dorey, A. Leite Commentary: Cloud computing a security problem or solution? University of London, UK KPMG LLP, UK.

[10] Renaud Francou Daniel Kaplan : Nouvelles Approches De La Confiance Numérique, Conclusions de l'expédition, Février 2011 confiance numérique, Une "expédition" commune de la Fing et la Fondation Télécom,

Mustapha Ben Saidi Checheur security of information. In University Hassan I Morocco. Holds a degree in higher education and telecommunications networks. Member of the association AMAN Morocco. His current research interests are Software Engineering, Software Security and Software Process Modeling adapted to Cloud computing.

Dr. Abderrahim Marzouk received his PhD (Computer Science) from University of Cean (France) in 1995. He has more than 15 years of experience in teaching Computer Science, JEE Technology and Web Applications. His current research interests are Software Engineering, Software Security and Software Process Modeling.