Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 11 (2016) pp. 302-310

Towards a new access control model based on Trust-level for E-learning platform

Kassid Asmaa[1], El kamoun Najib[2]

[1] STIC LaboratoryChouaib Doukkali University
El Jadida, Morocco
kassid.asmaa87@gmail.com

[2] STIC LaboratoryChouaib Doukkali University
El Jadida, Morocco
elkamoun.n@ucd.ac.ma

***Abstract*: Nowadays E-learning's popularity is increasing as more and more people are taking online courses. It becomes the need of the hour. The increase in the amount of resources available in E-learning systems will require the need for designing new architecture of such systems. The integration of multi-agent systems has played a very important role in improving the search quality, supplying new solutions and simplifying ways to very complex tasks.**

While a lot of efforts in the E-learning and multi-agent system domains has been put into delivering infrastructure and providing content, security and trust issues have hardly ever been considered. Worth knowing that in Multi-agent systems with the properties of agents (autonomous, social…), some activities will be dangerous and unreliable because it is difficult to know which agents are trustworthy and external accesses are safely.

In the present paper, the security aspects are directly related to the application of a control access policy, responsible for securing interaction with agents and reinforcing it with the integration of trust. The giving work will focus on combining two access models based on RBAC model :"TrustBAC",T-SR " Dynamic RBAC with Trust-Satisfaction and Reputation for multi-agent system" . The main goal here, is to develop a new model that incorporates the advantages of both models and improve the highest degree of security in the E-learning platforms based on multi-agent systems.

The proposed approach is implemented and evaluated by simulation using "MotOrbac" tool in order to define its validity context and limitations for a large and extended deployment.

***Keywords*:** Access control; Rbac model; Orbac model; security policies; e-learning platform; trust; multi-agent system

I. Introduction

Technology has changed the way people communicate and revolutionized education and training in the 21st century E- learning is one of the fastest growing markets in virtual world. E-learning is a flexible term used to describe the newest method of teaching throughout the online internet technology; this method incorporates self-motivation and communication. Although it has a relative fast growing, E-Learning becomes an important part the of learning system. To achieve its goals, it has gained most of its popularity in the recent years. It is a convenient and inexpensive way to gain knowledge and learn while living everydays' ordinary life.

With the development of Computer networking and Information Technology, E-learning is developing rapidly; It is does not only support teaching and learning, but some intelligence interaction among the collaborative team members[1],are designed for such complex system , one of the emerging technologies in distributed Environment is making it with less effort: *Agent based technology.*

Multi agent system in education field makes a great change in the society for the reason that the conventional education system required the presence of both the student and the instructor at the same time, same place and at the same interval of time, which is somewhat hard to manage every time [2].This technology is helping in developing interactive and better E-learning system.

While a lot of effort in the E-learning and multi-agent system domains have been put into delivering infrastructure and providing content, security and trust issues have hardly ever been considered. However that security is a growing concern in designing such systems that organizations can trust and use, one of the most developed security bases is "access control"; It is manifested by the selective restriction of access to a place or other resources . The act of accessing may mean consuming, entering, or using [3]. Also, by authentication and authorization that limits the actions for a user to perform in a system and control access to resources, several mechanisms how are found in the literature consider authorization as the key to protect a MAS, and as a basis for building a model of trust.

The management of the different levels of access rights to multiple types of resources by different and distributed users is one of the complex challenges that researchers of access control models confronted .Several access control models have been developed during last years : DAC [4], MAC[5], RBAC [6], TBAC[7] or TMAC[8] . Among these, role based access control (RBAC) is progressively becoming the standard for access control. The concept of this model had begun with multi-users and multi-applications on-line systems pioneered in the 1970s. The main advantage of RBAC on other access control models is the ease of security administration which appears on permissions that are associated with the roles while the users are assigned a certain role[9]. However this model becomes limited faced to the current network development specially the open and decentralized multi- centric system (E-learning systems), in terms of user population which is dynamic and identity of all users which are not known. For such systems, TrustBAC model [10] has been proposed to overcome the shortcomings of RBAC model by extending it with the notion of trust levels.

To highlight the dynamic changes of the environment and the roles assigned to users ,the authors propose a new access control approach to multi-agent systems based on the model RBAC with the notion of trust : " Dynamic RBAC with trust-satisfaction and reputation for multi-agent systems"[9] . In the present paper, the work is to develop a new model based on the two cited above models to incorporate the advantages of both and to improve the highest degree of security in E-learning platforms based on multi-agent systems.

Having given an initial introduction and motivation of the proposed work, the rest of this paper in structured as follows:

In Section 2 an overview of some of the related works on access control. There is a plethora of works in access control mechanisms. Here we present some of the works that are related to trust, e-learning platforms and multi-agent systems access control model.The architecture of TrustBAC model and dynamic RBAC model for multi-agent systems and a comparative study between them are presented in Section 3 including the trust evaluation method; Section 4 presents the proposed model and its components with an example of how our model works in E- learning platform. Section 5 is dedicated to present the basic concept of e-learning platform oriented spatial metaphor based on Multi-gent systems, with a use case of the model in a concrete e-learning scenario for educational purpose. Finally, we conclude the paper with some perspectives in section 6.

as the "corresponding author". This is the author to whom proofs of the paper will be sent. Proofs are sent to the corresponding author only.

II. RELATED WORKS

As we know e-learning covers a broad category of applications and processes, such as education via the Internet / Intranet (web based learning), education provided via computer (computer based learning), virtual classrooms and digital collaboration [14]. The e-learning platforms need to be secured, in this section we would briefly discuss the research works related of security requirements for e-learning and multi-agent platforms.

Much work has been done in the area of e-learning, to achieve a good level of security, there are many important elements that must be taken into account, and this has been discussed in a good way and can be reached in [11]. In [12], proposals for Security of e-learning Systems and security requirements for Multi-agent systems have been discussed; Security case modeling has been taken into account with emphasis on use cases.

Security has already proved an important requirement for the success of MAS, so there are already some works in this research area cited in [13], showing the concern of multi-agent community with security.

One of the most developed security bases is "access control", it is an important method of grant the three security Principles of computing: confidentiality, integrity and availability, the control of how resources are accessed it is very important in the protection of the e-learning platforms based on Multi-agent technology, preventing unauthorized modification or disclosure of resources. Several access control models have been developed during last year's ,a relevant work is provided by Xiao et al. – an authorization mechanism based in RBAC model [6], the authors believe that using policies based on roles is possible to build a security architecture that automatically adapts to system changes. In part, this is true: Assigning access policies to groups of agents/users with the same capability makes the system independent of the input and output of individual agents/users. However it is still inadequate for open and decentralized multi-centric systems in terms of dynamic and unknown users, to overcome the shortcomings of RBAC for such systems, researchers have proposed credential-based access control models [15, 16]. Credentials implement a notion of binary trust: the user has to produce a predetermined set of credentials like credit card numbers or proof of membership to certain groups to gain specific access privileges. The credential provides information about the rights, qualifications, responsibilities and other characteristics attributable to its bearer by one or more trusted authorities also it provides trust information about the authorities themselves. The integration of credential based access control with role-based access control make the security administration easy [17, 18]. Although credential based models solve the problem of access control in open systems to a great extent, but it still not enough to achieve a satisfy level in terms of given information about the behavior or action of the user between the time the credential was issued and its use, such information may play crucial parts in access control decisions, that why a lot of research has been done to improve the evaluation of trust on integrating the mechanism of history and context information (context awareness takes an important part which identifies the user's needs by analyzing the context information of user environment) of the user [19, 20, 21] .

The TrustBAC model, enhance the binary trust paradigm with multi-level trust which make the model much richer : trust levels in the users can be determined not only by using the credentials presented by the user but also from the results of past interactions with the user, from recommendations about the user and/or knowledge about other characteristics of the user.

In multi agent systems the context information collected from diverse sensor agents needs to be protected from unauthorized access and properly shared by many agents depending on the types of information and roles of user agents. For efficient access control to these resources, [9] propose a model based on RBAC which dynamically updates the roles and permissions according to the continuously changing environment. The proposed model employs the notion of trust evaluated with the measure of satisfaction and reputation.

III. PRESENTATION OF TRUSTBAC AND T-SR MODELS

With the evaluation of systems and applications, access control models have seen a lot of extensions as system security requirements in order to achieve the highest degree of security. in this case, to secure an E-learning platform based on multi agent systems, the given case are presented in two significant models of access control (TrustBAC and T-SR), and a comparative study, in order to cooperate with the advantages of both. This cooperation will allow the birth of a new model suitable to the platform

A. *TrustBAC model*

1) Overview

The model extends the RBAC model by introducing the notion of trust levels: users are assigned to trust levels not to roles as in traditional RBAC model like the figure shows.

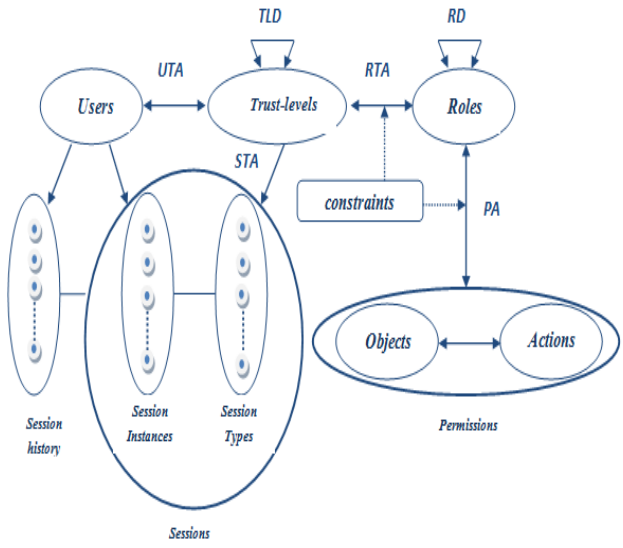

Figure 1. TrustBAC model

When using TrustBAC for access control, a user invokes a session instance of a particular type at an instant of time. The user has a trust level which allows him to use the roles associated with that trust level during this session, for each of these roles the user has a set of permissions to perform a set operations on a particular set of resources.

2) Elements and relations between them

The TrustBAC model is defined in terms of a set of elements and relations among those elements.

- The 12 elements with the corresponding sets are cited and defined in the following table.

Element	Set	Definition
User	USERS	Human entity, intelligent agents or system
user properties	USER PROPERTIES: Pu	-is a set of properties of the user
session instance	SESSION INSTANCES	- is a *login* instance of a user. -Session instance is identified by a system generated *id*
session-type	SESSION TYPES	- A set of properties manifested in a session instance, is an identifier of this session instance
session	SESSIONS	-Is identified by a session instance with a session type
session history	SESSIONHISTORY	-is a set of information regarding the user's behavior and trust level in a previous use of a session of that type.
trust level	TRUST LEVELS	-is a set of real number between -1 and +1.
role	ROLES	-Same concept in RBAC model: is a job function conferred to a user assigned to the role.
object	OBJECTS	-is a data resource as well as a system resource.
action	ACTIONS	-is an executable image of a program: read, write, execute....
permission	PERMISSIONS	-is an authorization to perform certain tasks within the system.
constraint	CONSTRAINTS	-is a predicate which applied to a relation between two elements returns a value of acceptable or not. -conditions imposed on the relationships and assignments.

Table2. Elements of TrustBAC model

- Association between any two of the above elements is specified by mathematical relations. TrustBAC has the following relation:

Relation	definition
Sua: USERS × SESSION INSTANCES × SESSION T-YPES → SESSIONS	defines the user-session assignment relation
UTA ⊆ USERS × TRUST LEVELS	defines the user trust level assignment relation
STA ⊆ SESSIONS × TRUST LEVELS	defines the session trust level assignment
RTA ⊆ ROLES × TRUST LEVELS	defines the role trust level assignment relation
PA ⊆ PERMISSIONS × ROLES	Define permission to role assignment relation
RD⊆ ROLES × ROLES	defines a dominance relation between two roles in terms of permissions
TLD ⊆ TRUST LEV ELS × TRUST LEV ELS	Defines a partial order relation on trust levels

TABLE 3. Relations between Elements

3) Evaluation of a trust value

TrustBac model adopts the vector model of trust that we had introduced earlier [22] for purpose of evaluating trust values of users with some changes:

- Trust and distrust are separately defined in the model,
- The possibility of a neutral position where there is neither trust nor distrust is discussed in the model.

Given first the definition of both trust/distrust:

Definition1. **Trust** is defined to be the firm belief in the competence of an entity to act dependably and securely within a specific context.

Definition 2. **Distrust** is defined as the firm belief in the incompetence of an entity to act dependably and securely within a specified context.

The simple trust relationship between **A** (Truster) and **B** (Trustee) is a vector with three components: Experience, Knowledge, and Recommendation.

$$\left[A \xrightarrow{C} B \right]_t = [AEB, AKB, \psi RB] \quad (1)$$

Where ${}_AE^C{}_B$ represents the magnitude of A's Experience about B in Context c (user's past behavior), ${}_AK^C{}_B$ represents knowledge about the user (credentials presented by the user) ${}_\psi R^C{}_B$ represents the cumulative effect of all B's recommendations to A from different sources (recommendation provided by others about the user). Each of these three factors is expressed in terms of a numeric value in the range $[-1, 1] \cup \{\perp\}$: ***The negative value*** is used to indicate the trust-negative type for the component, while ***the positive value*** is used to indicate the trust-positive type of the component., the ***0 (zero) value*** indicates trust-neutral and ***the special symbol*** $\perp$ indicates a lack of value due to insufficient information for any component.

The value for a normalized trust relationship allows us to revise the terms trust and distrust as follows:

$$V\left(A \xrightarrow{c} B\right)_t^N = \begin{cases} [-1, 0) \rightarrow \text{Distrust} \\ 0 \rightarrow \text{Neutral} \\ (0, 1] \rightarrow \text{Trust} \\ \perp \rightarrow \text{Undefined} \end{cases}$$

B. Dynamic RBAC with Trust-Tatisfaction and Reputation for multi-agent system model

With the rapid development of ubiquitous computing technology, the context information collected from various sensors has been increased fastly and need to be protected from unauthorized access and properly shared by many agents depending on the types of information and roles of user agents. For efficient access control to these resources, the authors propose a new model for multi-agent systems based on the RBAC with the notion of trust which dynamically updates the roles and permissions according to the continuously changing environment.

1) Overview

The model extends Rbac with the notion of trust and flexibility of using context: if the trust value of the requester is not smaller than the trust threshold defined by the system and the user's context information satisfies the context constraints, the user is assigned some roles, and may check the corresponding permissions associated with the roles.

In multi-agent system every component can be treated as an agent. The structure of the proposed model with trust is shown in Figure 2.

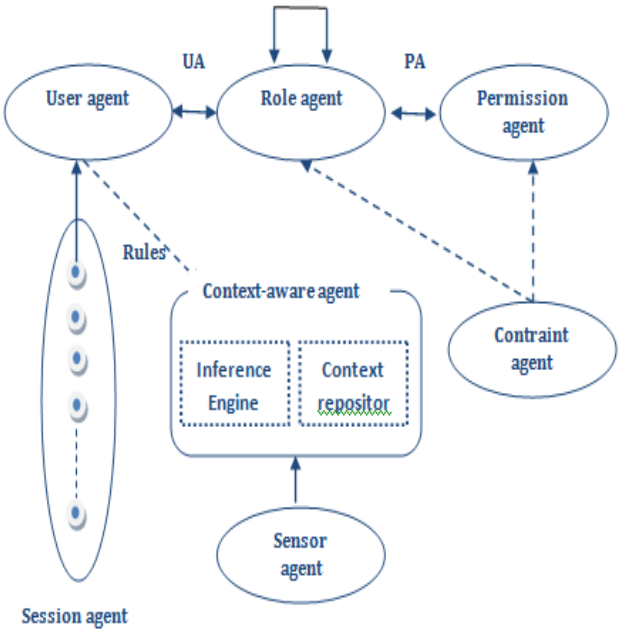

Figure 2. RBAC model for multi agent system

2) Elements and relations between them

The model is defined in terms of a set of elements and relations among those elements which are cited and defined in the following table.

Relation/function	definition
user: USERS × SESSION	function mapping each session Si to a single user
UA ⊆ USERS × ROLES	defines the user role assignment relation
RTA ⊆ ROLES × TRUST LEVELS	defines the role trust level assignment relation
PA ⊆ PERMISSIONS × ROLES	Define permission to role assignment relation
RR ⊆ RULE × SESSION	defines relation between permission and role assignment
Rule Register : SESSION x RULE	function registering each rule in a single session Si

TABLE 4. Elements and relations

3) Evaluation of a trust value

The trust value in a practical system is calculated ***Satisfaction*** which represents the confidence of the services and resources the agents provide, and ***Reputation*** which represents the recent behavior and past history of requesting agent.

We compute the trust value of an agent as

$$Trust = \alpha_1 * SD + \alpha_2 * R \quad (2)$$

$$\alpha_1 + \alpha_2 = 1 \text{ and } \alpha_1, \alpha_2 > 0$$

Where α_1 and α_2 are the weight coefficients defined by the System according to the application

- ***Satisfaction degree SDi is*** between 0 and 1. If it is close to 0, it means that agent-i is untrustworthy. On the contrary, if it is close to 1, agent-i is trustworthy.

- ***Reputation is*** evaluated by calculating local and *global* reputations, the first is computed as the quotient of number of honest transactions and the sum of honest and malicious transactions between agent-i and agent-j, the method of obtaining the global reputation value is to compute the average value of the local reputation values of an agent evaluated by other agents.(for more detail refer to [9]).

C. A comparative study between T-SR and TrustBac models .

As we have seen in previous sections, both models are an extension of RBAC satisfying the aspects of security for the complex and open systems bringing with them the notion of trust which is evaluated differently, depending the system, for example , in open systems like internet the TrustBAC is more adequate, it's mechanism is based on assignment of users to trust levels which is determined by three factors: users past behavior, knowledge about the user and recommendation provided by others about the user.Which means that the user can have many profiles depending on the value of trust (basic user, privilege user ..), making it possible to manage several policies associated with the dynamic level of the trust value which is absent in T-SR model : the user based on his confidence level is either refused or accepted .

Model / Factors	Rbac	TrustBac	T-SR
Open system		x	x
Complexity		xx	xxx
Context	x	x	xx
Trust evaluation		xx	x
MAS			x

IV. THE PROPOSED MODEL

A. overview.

The concept of trust in multi-agent system which can be used is to put the relationship into the dynamic multi-agent system to control the access to the resources and services. If an agent wants to request a service, firstly, it needs to pass the permission test checking on whether it is authorized or not, then it must solve the issue of security. Even for authorized agent, some chance still exists that the service is abused. Since there is no central certification authority in the multi-agent system, a new agent has to verify the trust value of the agents and classify it in levels using the satisfaction and reputation information. Where a user can have multiple trust levels since he can invoke many sessions at the same time (each session has a unique trust level).

Like the T-SR model every component can be treated as an agent. The structure of the proposed model is shown in Figure 3.

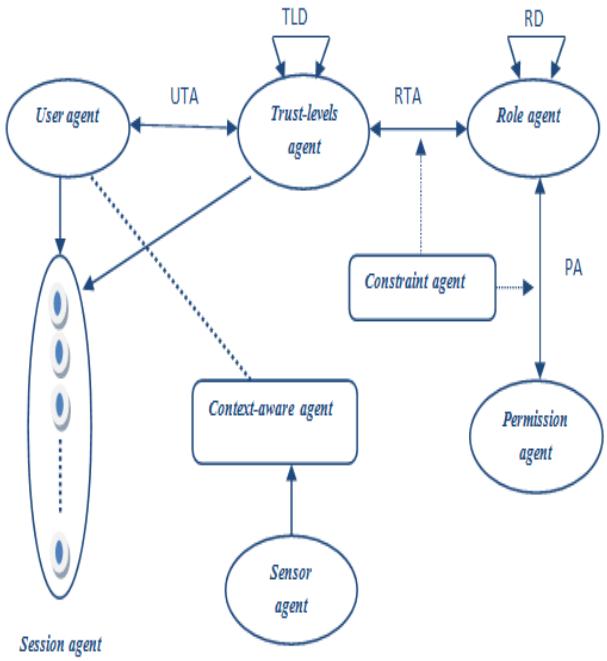

Figure 3. the proposed model

Here are the components of the model:

User agent is the same as user of the original RBAC model which can be a device the user carries to access the resources according to the user's role.
Trust-levels agent verifies the trust value of the agents and classifies it in levels
Role Agent keeps the list of the roles and manages the role hierarchy
Permission Agent keeps the list of permissions
Sensor Agents collects the context information and sends it to the 'Context-Aware Agent'
Session Agent registers the rules in 'Context-Aware Agent' besides connecting 'User Agent' and 'Permission Agent. It is dynamically updates the user's role according to the context

Context-Aware Agent infers the context using diverse context information and reports the result when the rule is fired.

The proposed model allows an access control management more dynamic and precise, with the help of his access control structure which is composed of three modules as shown in the figure4.

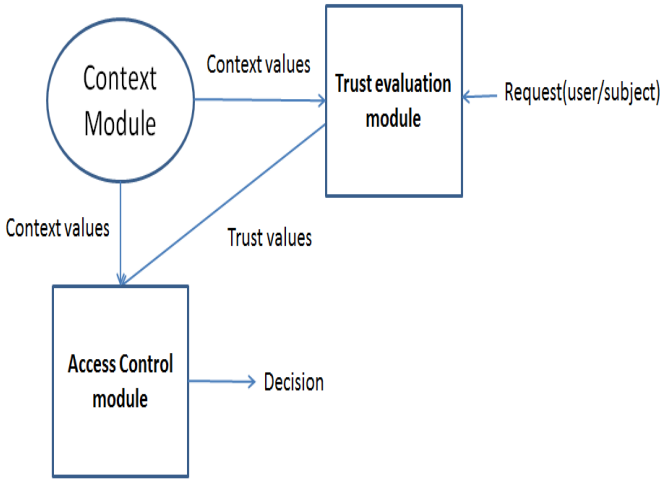

Figure.4 The Access Control Structure

In this system, the "*Confidence Evaluation Module*" is the principal module; it receives access requests, analyzes, collection of context values and other parameters such as reputation and satisfaction , and sends the trust value of the user to the "Access Control System" module. After that the access control system makes decisions for each application based on the value of trust of the user provided by the *confidence evaluation* module.

The *Trust evaluation module* plays a key role in the proposed model. It calculates the values of trust based on the reputation, satisfaction and context values. The context module is responsible for collecting user and environment information's.

B. Mapping algorithm for roles

In the proposed model , the administrator will associate to each trust value some specifics roles on defining the function R such TV →R(roles) TV (Trust Value) , this mapping depends on the control access requirement .Here we present the algorithm that compute dynamically the roles :

Data:request
Result: set of roles where the request entity is mapped
u ← Subject (request);
T_0 ← Trust-value (u);
Roles= Φ ;
Foreach T_0 DO
Roles ← Roles ∪ R(T_0);
End
Return Roles ;

role-based dynamic access control mechanisms and *traditional access control mechanisms* is that the user' s role can control policy by its respective trust level.

C. The process of access authorization

The access authorization process is illustrated in the Figure 5 as following:

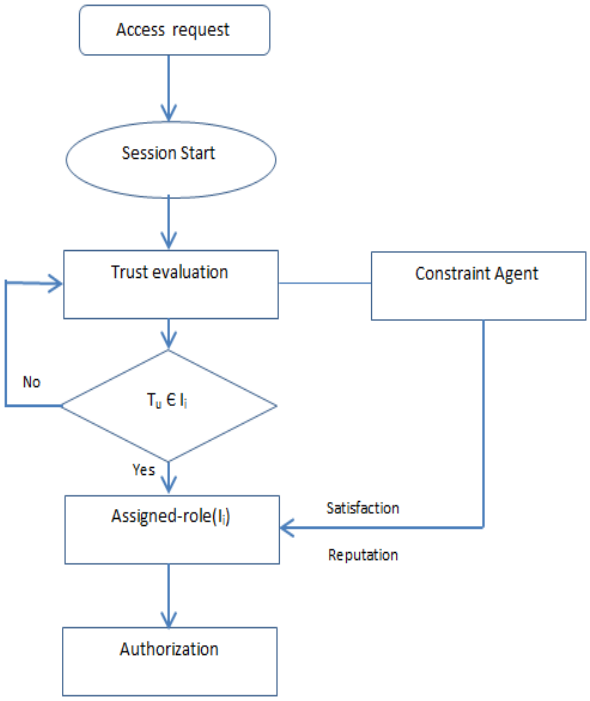

Figure.5. access authorization process

The access authorization process is summarized:

Step 1: After a request for access is made, a session is started.

Step 2: Once the session is establishes, the trust evaluation module which is based on reputation and trust gives a value of the requester (user) .

Step 3: If the user confidence value T_u, belongs to the interval defined by the administrator, specific roles are assigned to the user depending this interval and constraint agent, after that the authorization is granted. Alternatively, we recalculate the confidence value if there is an unexpected error.

D. Example of access authorization process

Let us consider an example to show how the present approach works:

Let *public student*, *basic student* and *privilege student* be three roles in the ROLES set of the platform. We specify the following: Assigned Roles ([0.05, 0.2]) = public student, Assigned Roles ([0.15, 0.4]) = basic student and Assigned Roles ([0.35, 0.6]) = privilege student. A Student log in to the system, the credentials are verified and evaluated and the corresponding value the trust is evaluated as 0.45, therefore, according to Assigned Roles the user at this stage is allowed to act as a *privilege student* as well as a *basic* and *public student.* Let the privilege users of the platform be allowed to write comment about the courses presented in the database of the E-learning platform as well as the uploading copies of courses that are not presented in the database. We consider that:

- Abusive/irrelevant comments as negative events and
- Upload of a corrupted or inauthentic file as negative event.

We consider that the student during the session writes several bad comments and upload a few inauthentic files. Each of these activities get reported in the session , Let T evaluates trust periodically within a session. Let at some evaluation point v=0.345.This shows that the student is no longer 'trustworthy' to the system as a *privilege student* . That is why the system automatically refuses the role of privilege student for the student. During the remaining time in this session, he can no longer acts as a privilege student. So if there is a section of articles in the database which is only available to privilege student then he cannot access those articles anymore. However, he can continue to act as a basic/public student who will keep it for its next login, except if the confidence level increases with the good actions and is reached to 0.35. It can again act as a privilege student.

V. THE EVALUATION OF SECURITY POLICY OF THE PROPOSED MODEL

A. *Presentation of the platform*

For this purpose we assume that the E-learning platform is manipulated by different actors: tutors, learners, and teachers where each actor plays a specific role in the learning process.

- The teacher sets through the learning platform its pedagogical scenario, and uses a set of tools and resources offered by the platform.
- The tutor supports the students in their learning activity, in order to answer questions, raise interactions, and evaluate progress.
- The student on his side use the pedagogical scenario defined by the teacher, looking for example at the solution of an exercise and trying to understand the course content.

The pedagogical activity fits into the context of database training for the student of the 2nd year specialty networks and telecommunications at the University . It includes 22 learners to find a model Entity / Association and implement it on a computer software 'rational rose'. This training takes 3 sessions of 2 days each. At the end of each session the learner must pass a test that should validate the access to the resources of the 2nd. Figure 4 summarizes the scenario in accordance with the constraint of time. The distribution of groups and teams is done by the ticket of teacher-tutor.

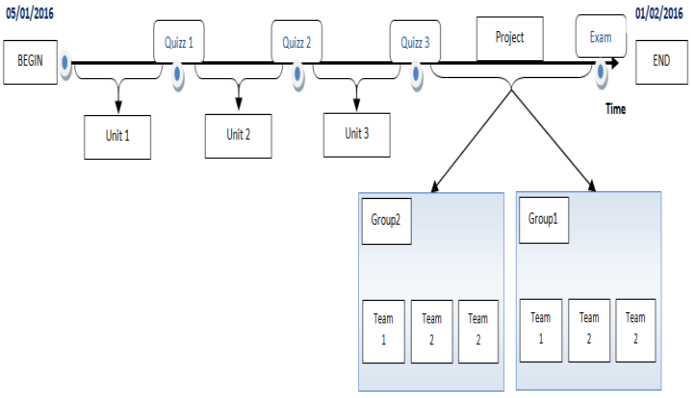

Figure.6. An example of a pedagogical scenario

B. *Managing Subjects /roles, Objects And Actions*

We define some Subjects /roles, Objects And Actions entities of our pedagogical scenario, considering that the following tables resume some of needed entities to model our approach based on the example cited in previous section :

Role	Subject
Privilege-student	{Mr Najib}
basic-student	{Mlle Fatima , Mr Khalid}
Public-Student	{Asmaa,zahira,hind...}
administrator	9 students per group

TABLE 5. MANAGING SUBJECTS /ROLES

Actions	Objects
-Writing coments / exercises **-Filed courses / exercises**	**Course-X.doc/html/pdf/ppt** **- video/-shema.jpg / …**
Modification courses / exercises	**-Quiz.doc/-Exam-module-x.doc**
Download course/TD/Quiz/Exam	

TABLE 6. MANAGING ACTIONS AND OBJECTS

C. *Simulation with motorbac tool*

Designers of the Or-BAC model have developed MotOrBAC [23][24] a security policy tool which can be used to specify, simulate, evaluate and administrate the security policies not only based OR-BAC model but also RBAC model, This is partly due to the fact that its GUI is independent of its API and RBAC has common entities of the OrBAC model.

Security policies expressed by MotOrBAC have a declaration section which provides useful information on security policy like: the date of the last version of the policy, creation date, version, ... We can also use this declaration part to inform the access control model used to express in this tool, In fact, when the security policy is expressed from RBAC, certain parts of MotOrBAC will be disabled: views, activities, prohibitions, obligations.

In this simulation we considered that the trust value is an attribut of the subject, its already calculated with an independent program.

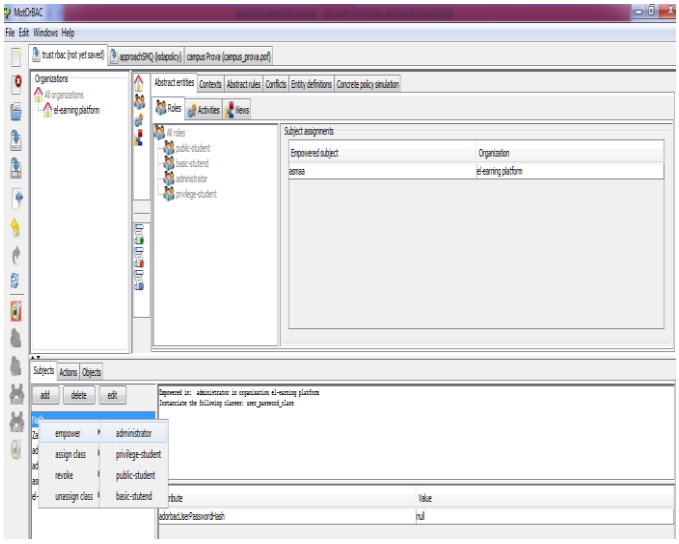

Figure.7 The creation of the role/subjects entities

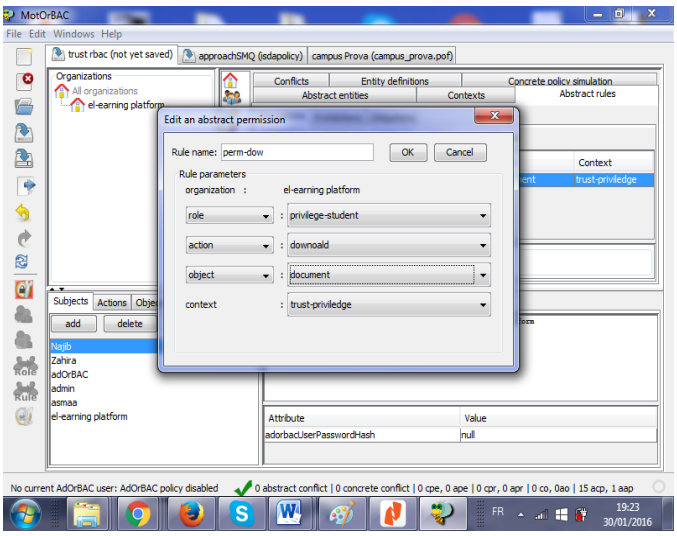

Figure.8. The creation of the rules

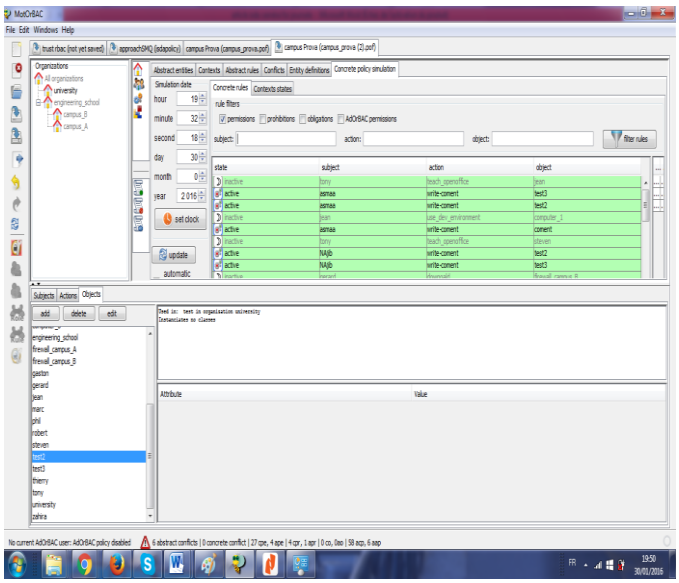

Figure11. Simulation of the policy

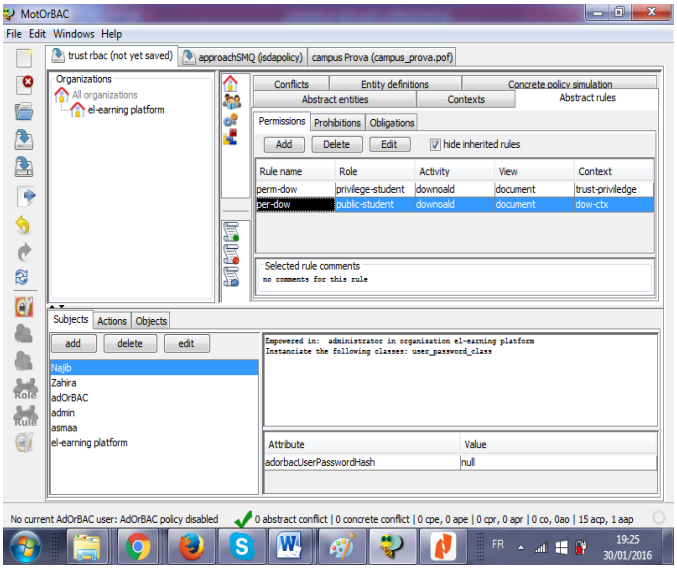

Figure9. Set of permission rules

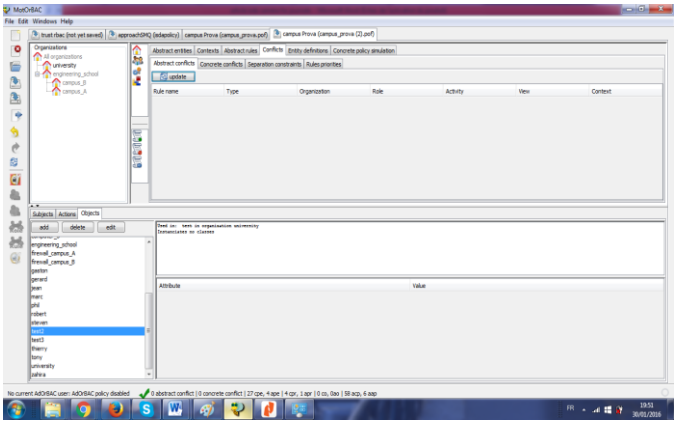

Figure10. Absence of conflicts

VI. CONCLUSION AND PERSPECTIVES

In addition to access control, trust and reputation are also key issues to provide secure and trustworthy services for modern systems, especially E-learning platforms based on multi agent systems

the main goal in this paper, is to provide a new model adapted to e-learning platform based on multi agent systems to improve the level of its security, taking into account the different interactions of these actors/agents and the notion of context, because it is one of an important factors. It allows to set certain conditions for the application of safety rules. This improvement may reside on combining the advantages of TrustBAC / T-SR models, as well as, the simplicity of evaluating the trust value.

A system is not safe if a model is developed but never managed afterwards. Policies handled by such a model need continuous maintenance to ensure the security model that remains useful . Bearing this in mind, we are working on many axes to implement and evaluate this model:

The proposed approach is implemented and evaluated by simulation using “MotOrbac” tool in a concert e-learning scenario for educational purpose, in order to define its validity context and limitations for a large and extended deployment. But still not enough so encode it on Orbac model, one of the most developed access controls, to prove how the expressive power and flexibility of this model work and profiting of all new concept added to orbac model make our approach more rich and modular

References

[1] S. Ahmad, & M.U. Bokhari, "A New Approach to Multi Agent Based Architecture for Secure and Effective E-learning" International Journal of Computer Applications, 46. 2012

[2] Bokhari, M.U., Ahmad, S. and Alam, S. 2011. Modern Tools and Technologies for Interactive Learning. In Proceedings of the Computing For

Nation Development, Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi

[3] Asmaa.K, Najib E,' A Comparative approach of different Or-BAC extensions: Application and limits'.In Proceedings of the 5thWorkshop on Codes, Cryptography and Communication Systems (WCCCS), El Jadida ,Morocco, 2014,pp. 67 – 72.

[4]] B. Lampson. "Protection", 5th Princeton Symposium on Information Sciences and Systems, pp. 437-443, Mars 1971.

[5] D. Bell et L. LaPadula. "Secure computer systems:Unified exposition and multics interpretation", Technical Report ESD TR73-306, The MITRE Corporation, Mars 1976.

[6] R. Sandhu, E. Coyne, H. Feinstein et C.E.Youman. "Role-based access control models". IEEE Computer, 29(2), pp. 38-47, 1996.

[7] R. Thomas et R. Sandhu. "Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management". 11th IFIP WorkingConference on Database Security, Lake Tahoe, California, USA, pp. 166-181, 1997.

[8] R. Thomas. "TMAC: A primitive for Applying RBAC in collaborative environment". 2nd ACM, Workshop on RBAC, Fairfax, Virginia, USA, pp . 13-19, Novembre 1997.

[9] J. W.Woo, M. J. Hwang, C. G. Lee, and H. Y. Youn. Dynamic role-based access control with trust-satisfaction and reputation for multi-agent system. International Conference on Advanced Information Networking and Applications Workshops, 0:1121-1126, 2010.

[10] S. Chakraborty, I. Ray, "TrustBAC: Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems," In Proc. of the 11th ACM Symposium on Access Control Models and Technologies, Lake Tahoe, California, USA, 2006, pp. 49-58.

[11] Kambourakis G, Security and Privacy in m-Learning and Beyond: Challenges and stae-of-the-art. International Journal of u- and e-Service, Science and Technology, Vol. 6, No. 3, June 2013.

[12] S. H. Hasan, D. M. Alghazzawi, and A. Zafar "E-Learning systems and their Security" BRIS Journal of Adv. S & T (ISSN. 0971-9563) vol.2, no 3, pp. 83-92, 2014

[13] Rodolfo Carneiro Cavalcante , Ig Ibert Bittencourt , Alan Pedro da Silva , Marlos Silva , Evandro Costa , Rob ério Santos, A survey of security in multi-agent systems, Expert Systems with Applications: An International Journal, v.39 n.5, p.4835-4846, April, 2012 [doi>10.1016/j.eswa.2011.09.130]

[14] T. Kuhlmann. "Why E-Learning is So Effective," 19 April, 2013].

[15] M. Blaze, J. Feigenbaum, and J. Ioannidis. The KeyNote Trust Management System Version 2. Internet Society, Network Working Group. RFC 2704,1999.

[16] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In Proceedings of 17th IEEE Symposium on Security and Privacy, pages 164–173, Oakland, California, USA, May 1996.

[17] N. Li and J. Mitchell. Datalog with Constraints: A Foundation for Trust-management Languages. In Proceedings of the 5th International Symposium on Practical Aspects of Declarative Languages, New Orleans, Louisiana, January 2003.

[18] N. Li and J. Mitchell. RT: A Role-based Trust Management Framework. In Proceedings of the 3rd DARPA Information Survivability Conference and Exposition, Washington D.C., April 2003.

[19] M. Abadi and C. Fournet. History-based Access Control for Mobile Code. In Proceedings of the 10th Annual Network and Distributed System Security Symposium, pages 107–121, San Diego, California, USA, February 2003.

[20] G. Edjlali, A. Acharya, and V. Chaudhary. History-based Access Control for Mobile Code. In Proceedings of the 5th ACM Conference on Computer and Communication Security (CCS'98), pages 38–48, San Francisco, California, USA, November 1998.

[21] F. Feng, C. Lin, D. Peng et J. Li, «A Trust and Context Based Access Control Model for Distributed Systems, » Proc. of the 2008 10th IEEE International Conference on High Performance Computing and Communications, pp. 629-634, 2008

[22] I. Ray and S. Chakraborty. A Vector Model of Trust for Developing Trustworthy Systems. In Proceedings of the 9th European Symposium of Research in Computer Security (ESORICS 2004), volume 3193 of Lecture Notes in Computer Science, pages 260–275, Sophia Antipolis, France, September 2004

[23] Autrel, F., Cuppens, F., Cuppens-Boulahia, N., Coma, C.: MotOrBAC 2: a security policytool. In: 3rd Conference on Security in Network Architectures and Information Systems (SAR-SSI 2008), Loctudy, France, pp. 273–288 (2008).

[24] http://motorbac.sourceforge.net/index.php?page=home&lang=en

Author Biographies

Kassid Asmaa was born in El Jadida, Morocco, in 1987 , a Phd Student computer Science, in STIC laboratory at Chouaib Doukkali University (UCD) - MOROCCO. Her research interest is to develops access control policies in e-learning platform.

El kamoun Najib Professor Researcher at ICT laboratory Faculty of Science University Choaib Doukkali El Jadida Morocco. With over 20 years of expertise in distance education, he has conducted several thesis and overseas missions in e-learning. His current research interests focus on mobility management and QoS in emerging networks (MANET, VANET and WSN) and security .