Encoding a T-RBAC Model for E-Learning Platform on ORBAC Model

Kassid Asmaa
STIC Laboratory
Chouaib Doukkali University
El Jadida, Morocco

Elkamoun Najib
STIC Laboratory
ChouaibDoukkali University
El Jadida, Morocco

***Abstract*—with rapid development and increase in the amount of available resources in E-learning platforms, the need to design new architecture for such systems has become inevitable to improve the search quality and simplifying ways to take online courses. The integration of multi-agent systems has played a very important role in developing open, interactive and distributed learning systems. A lot of research in E-learning and multi-agent system have been put into developing infrastructure and providing content, security and trust issues have hardly ever been considered worth knowing that security issues may endanger the success of these platforms.**

The application of a control access policy, as one of the most important aspects of security, in E-learning platform based on multi agent systems , plays an important role to secure interaction with agents/users and reinforcing it with the integration of trust level .The work of this paper is to encode a new access control model developed in previous works based on '' role based access control model '' and trust level, on ''Organization based access control model'' to improve the security level in E-learning platforms based on multi-agent systems.

The encoded model is implemented and evaluated by "MotOrbac" tool, in order to define its validity context and limitations for a large and extended deployment.

Keywords—Security policies; Access control; Rbac model; Orbac model; e-learning platforms; trust; multi-agent systems

I. INTRODUCTION

The definition of E-Learning is understood simply as a means of teaching throughout the online internet technology , it is a convenient and inexpensive way to gain knowledge and learn ; It has become the need of the hour since more and more people are taking online courses; With the development of Information Technology, E-learning is developing rapidly; It is does not only support teaching and learning, but also some Intelligence interaction among the collaborative team members[1], to design such complex platform, designers use one of the emerging technologies in distributed Environment: Agent based technology ,

Multi agent system in E-learning system makes a great change in the society because the conventional education system need the presence of the student and the instructor at the same time, same place and at the same interval of time, which is somehow difficult to manage every time . This technology is helping in developing interactive and better E-learning system. In agent-based systems, agents try to get information from other or gain access to remote service provider agents in order to achieve their goals. We have seen considerable effort being put into development of the content and infrastructure for the e-learning system, yet there is hardly any effort being put into these system for making them secure, especially, in open environments where agents are able to freely move around, many activities would be unsafe and unreliable because it is hard to know which agents are trustworthy and which external accesses are not harmful. Worth knowing that the integration of security concerns could help towards the development of more secure multi agent systems.

A lot of models how are found in the literature consider the integration of trust in multi agent systems as the key to protect it, and as a basis for building a satisfactory model of security based on access control policies, one of the most developed security methods, it is expressed by identifying the restriction of access rights an entity has over system resources. Access controls are the concrete mechanisms that are put in place to assert whether or not the current user can perform a given action on a given resource.

As we know to achieve a satisfactory level of security, it is necessary to define a security policy that meets the needs of the application, several formalisms have been proposed and developed during last years to overcome the limitations of the models above depending on the nature of systems and their development witch make the management of the different levels of access rights to multiple types of resources by different and distributed users more complex : DAC [4], MAC[5], RBAC [6], TBAC[7] or TMAC[8] . In these models we find a lot of extensions of role based access control (RBAC) which make this one as the standard of access control models. The concept of RBAC had begun with multi-users and multi-applications on-line systems pioneered in the 1970s. The difference between RBAC and the other access control models is the ease of security administration which is manifested by linking permissions with roles, while the users are assigned to definite role. In spite of that Rbac model and its extensions, must take into consideration the new demands:

- Every organization has the opportunity to have their own policies.
- Rules in access policies, with the integration of context concept, become dynamic.
- Rules in access policies must be self-adaptive to the temporal conditions, the location of the user and the previous user behavior.

Hence the appearance of OrBAC model (Organisation-Based Access Control) who is more oriented security policy. It is a model allowing abstract notions of users, action and object, expressing rights context, obligations or recommendations not only the permission like tradional models. It contributes to define abstractions which allow us to relate managed objects to one another or which allow us to relate users, or groups of users, to groups of objects.

In this paper, the work is to encode a new model that we developed in previous work [9] based on the two access control model'' TrustBAC model'' [10] and" Dynamic RBAC with trust- satisfaction and reputation for multi-agent systems" [11]; the main goal of this model is to incorporate the advantages of both 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 proposed model, its components and an example of how our new model works in E- learning platform are presented in Section 3 including the trust evaluation method; Section 4 presents the main concepts and components of orbac model Section 5 is dedicated to present the encoded model.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 will be presented in section 6. Finally, we conclude the paper with some perspectives in section 7.

II. Related Work

Since security has become an essential asset in numerous application areas such as e-learning platforms, the integration of security policies has become a major issue in the design of security architectures.

Much work has been done in the area of e-learning, since it covers a broad category of applications and processes, such as education via the Internet / computer (web based learning/ computer based learning), virtual classrooms and digital collaboration [14]. In this section we would briefly discuss the research works related of security requirements for e-learning and multi-agent platforms.

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.

Access control model 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. A lot of access control models have been developed ,a relevant work is provided by Xiao et al. – an authorization mechanism based in RBAC model [6], the authors consider that using policies based on roles is possible to build a security architecture that automatically adapts to system changes.. However it is still not enough for open and decentralized multi-centric systems in terms of dynamic and unknown users, to overcome the limitations of RBAC for this kind of systems, authors have proposed credential-based access control models [15, 16]. This model implement a concept of binary trust which mean that a user has to produce a predetermined set of credentials (proofs) to gain some determined access privileges. It's 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 combination between credential based access control and role-based access control make the security administration more flexible [17, 18]. even though the credential based models solve the problem of access control in open systems ,still not enough in terms of given information about the behavior or action of the user, the credential model shows its limits to achieve a satisfy level of security , 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.

To highlight the dynamic changes of the environment and the roles assigned to users , researchers develop a new access control model for multi-agent systems based on the RBAC model with the integration of trust concept : " Dynamic RBAC with trust-satisfaction and reputation for multi-agent systems"[9] because 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, this model updates dynamically 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.

The incorporation of the advantages of both latest models cited above gives birth to a more efficient new model that we developed in previous works and to improve the highest level of security in E-learning platforms based on multi-agent systems: The notion 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 , so,

if an agent wants to request a service, as first step , it needs to pass the permission test checking on whether it is authorized or not, then it must solve the problem of security.

As we know ORBAC model produce a rich and modular (the designer can define a policy security independently of the implementation), but with the integration of the concept of trust make it more dynamic (rules can be activated or deactivated based on trust levels of the user or the organization) and more interactive (the recent behaviors of the trustee are used to control the access of resources). In the literature two different model of TRUS T-ORBAC are proposed for two different platform the first is ''A Trust Access Control Model in Multi-Organization Environments ''[19] and ' A Trust-Orbac Control is a new model dedicated to the security of Cloud Computing Systems'' [2]. The difference between these two models is in the fact to evaluate the trust; knowing that this later change from one to another system.

III. The Proposed Model

This model allows to us an *access control management* more dynamic and precise, with the help of three modules that build the access control structure of our approach:

- The *"Trust Evaluation Module*" it's the principal; it receives access requests, analyzes, collection of context values and other parameters, and sends the trust value of the user to the Access Control System module.
- The *"Access Control System"* makes decisions for each application based on the value of trust of the user provided by the *trust 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.

A. Evaluation of a trust value

Before exploring the parameters to evaluate trust value, we first define trust in the context of this paper. Trust is defined in a variety of ways. Many authors examine the various definitions of trust and then provide a working definition of trust for internet applications: "Trust is the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context". However, in our model we adopt the definition of Mui et al. , because the definition of trust is based on reputation which both are strongly related to evaluate trust in Multi agent systems: "Trust is a subjective expectation an agent has about another's future behavior based on the history of their encounters".

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

$$Trust = \alpha_1 * SD + \alpha_2 * R \quad (1)$$

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

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* reputation. Local reputation is the quotient of number of honest transactions and the sum of honest and malicious transactions between agent-i and agent-j. The global reputation is the average value of the local reputation values of an agent evaluated by other agents; more details are explained in [9]).

B. Basic concept of the new model

The components of this model can be treated as an agent ; they are cited as follow:

- ***User agent*** : is the user how carries to access the resources according to the user's role(same as user in RBAC model)
- ***Trust-levels agent*** : responsible for checking the trust value of the agents and classifying it in different levels
- ***Role Agent***: responsible for keeping the list of the roles and managing the their hierarchy.
- ***Permission Agent*** : its role is keep the list of permissions
- ***Sensor Agents***: its role is collects the context information and sends it to the 'Context-Aware Agent'.
- ***Session Agent***: its role is register 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***: its role is infers the context using diverse context information and reports the result when the rule is fired.

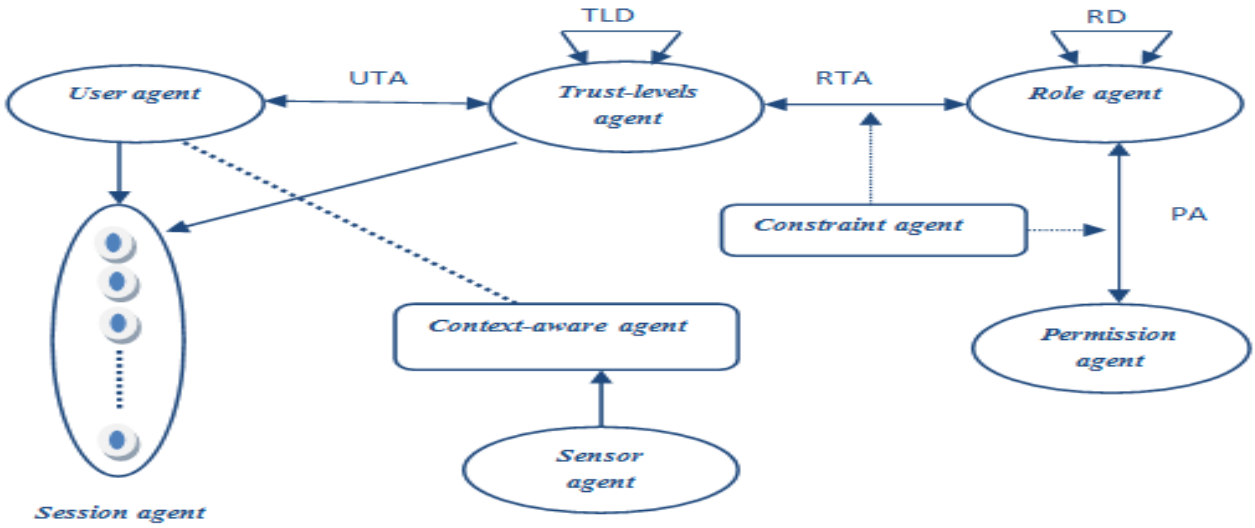

Fig. 1. The new model

The structure of the new model is presented in Figure 1.

The difference between trust-role-based dynamic access control mechanisms and the other access control models is that the user's role can control policy by its trust level.

C. The process of access authorization

The access authorization process is illustrated in the Figure 2 as following:

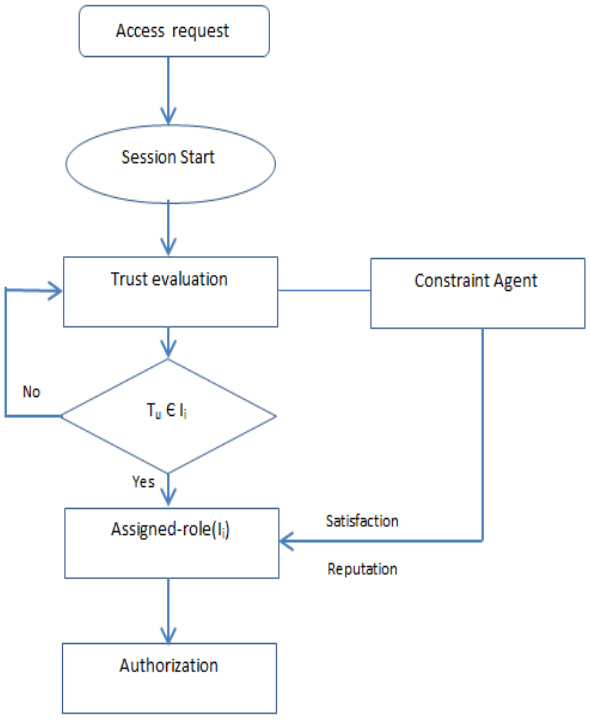

Fig. 2. access authorization process

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.

IV. Presentation of OrBAC Model

Organisation Base Access Control, is an access model that took over the cited above models by adding the concept of abstract entities. In the beginning, OrBAC was proposed in [10] to meet security policy requirements in the health care fields.

The application of OrBAC model in different platforms confirms it's expressive power ,adding to these, OrBAC includes contextual rules based not only on permissions but also prohibitions, obligations and recommendation which make the security policy rich ,modular and dynamic.

A. Basic concepts of OrBAC model

The central entity in Or-BAC is the Organization. An organization can be seen as an organized group of subjects playing a role or another. Worth knowing a group of subjects does not necessarily correspond to an organization. More specifically, the fact that each object plays a role in the organization is an agreement between the materials to form an organization.

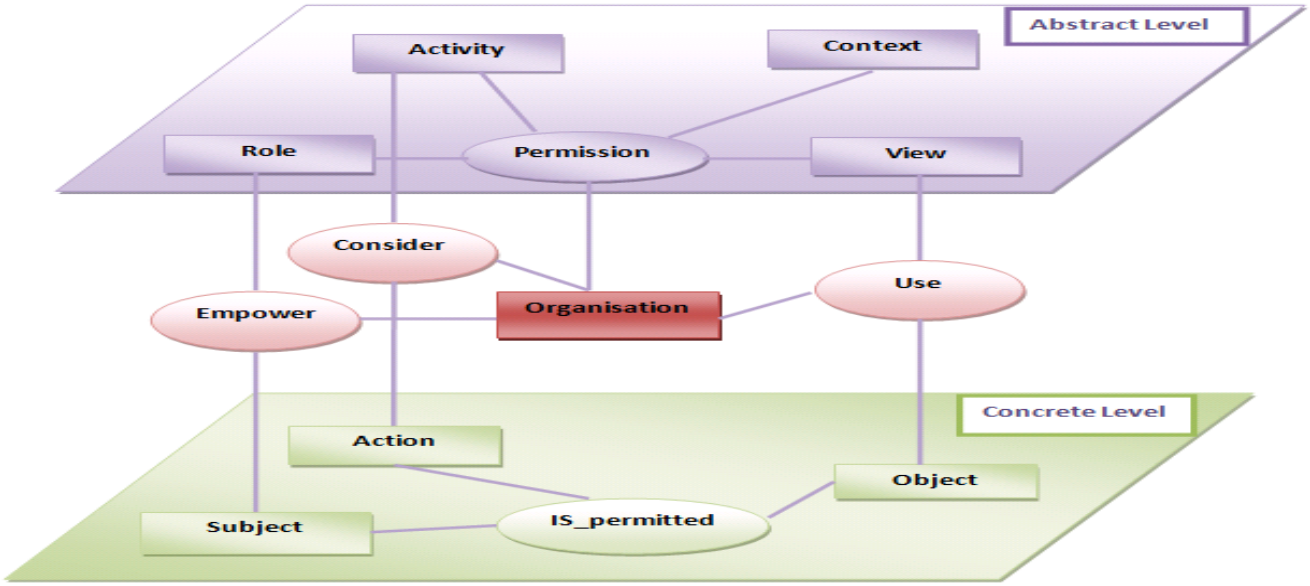

Fig. 3. The ORBAC model

As the Figure 3, the introduction of an abstract level where the role, activity and view concepts abstract the subject, action and object concepts [8] allow to the designer the possibility to define a policy security policy independently of the implementation .A view is a set of objects that satisfy a common property. An activity includes actions involved the same principles and privileges apply only in the specific *context.*

Each organization ***org*** specifies its own security rules, some ***role*** may have the *permission, prohibition, and obligation* or *recommendation* to do some ***activity*** on some ***view*** given an associated ***context*** is true:

permission(org, *role, activity, view, context).*
prohibition (org, *role, activity, view, context).*
obligation (org, *role, activity, view, context).*
recommendation (org, *role, activity, view, context).*

B. The new Concepts characterizing the model

In ORBAC model, new concepts have been added in a developed way, and which have characterized as the most developed access control model, in the following table you found these concepts with their explanation.

Notion Of hierarchy	In ORBAC model an organization can be divided in sub-organization, a role in sub-role, activity in sub-activity, and a view in sub-view. These decompositions generate hierarchical relationships between the parent entity (generalization) and the Child entity (specialization). In order to express this hierarchy OrBAC introduces the predicates ***sub_role (org, R1, R2)*** which means that in organization org, role R1 is a sub-role of the role R2, same thing with ***sub-activity(org, A1, A2)*** and **sub-view(org, V1, V2**).
Notion of Context	Express different types of constraints that control the activation of the rules expressed in the access control policy. OrBAC model represents the contextual constraints allocation rights, brings together the different contexts by type, to acceptance a request an evaluation of the context must be done , this evaluation is based on some information in order to test the activation of the context.
Notion Of Conflict	Since Or-BAC model specifies at the same time permissions and prohibitions the appearance of conflict became remarkable, especially when a user is permitted and prohibited to perform an action on object a conflicts can occur. To model such a situation, we introduce a predicate called ***conflict()*** used in rules as follow: *Is -permitted(s, α, o) ∧Is-prohibited(s, α, o) →**conflict** ()*

V. ENCODING THE PROPOSED MODEL ON ORBAC MODEL

This section provide an encoding of the proposed model, which is based on RBAC model with trust level, on OrBAC organizational model. For each concept (role, type, context ...) used in the model, we provide its counterpart in the OrBAC model to confirm the expressive power of this later.

Two concepts of ORBAC model are not directly used in the proposed model:

- ***The concept context*** which is not exploited in a larger and varied manner, so with the use of context OrBAC model, we can express different types of extra conditions or constraints that control activation of rules.
- ***The concept of organization***: in this case the OrBAC model is supposed to have a fixed value, we assume here that we have only one organization we simply call " **learn-organization** ".

A. Subject / role

As we said in the previous section, in the ORBAC model, a subject may be either an active entity: a user / agent, an organization STIC laboratory or department of IT …. . In our platform, the ***entity subject*** lists the UID (User Identifier) of this system, each UID is related to specific username. The ***entity Role*** is used to structure the relationship between subjects and organizations. In our case, like the table show, the roles «*Privilege-student* », «*administrator*», are played by users specially students.

TABLE I. SUBJECTS / ROLE

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

B. objects / view

In our model, the entity subject primarily represents non-active entities such as files, emails, printed forms …, in e-leaning platform, we consider objects as courses, exams, practical work.... The **entity views** like role is used to structure the relationship between objects and organizations. The following table summarize some of view/object used in e-leaning platform.

TABLE II. OBJECTS / VIEW

View	Objects
course	Course-X.doc/html/pdf/ppt
Resource-sup	- video/-shéma.jpg / …
Resource-Test	-Quiz.doc/-Exam-modul-x.doc
Doc-team	- Doc-team 1/2/3 ….
training	-Training-BD

C. Activities / Action

Security policies specify allowed access to passive entities by active entities and regulate the actions performed on the system. In ORBAC model, the Action entity includes IT actions like "read", "write", "send", etc. The activities will be "consult", "edit", "transmit", etc. Each organization may consider the same action used in the realization of different activities. You find in the following table some Activity/Actions used in E-learning.

TABLE III. ACTIVITY / ACTIONS

Activity	Actions
Creation	- writing courses / exercises -filed courses / exercises
Update	-Modification /Suppression(courses / exercises)
Follow	-Explain-course/project – Answer-questions
download	-Download (course/Exam)
Answer	-Answer (questions/exam)
Register	-Registration

D. Trust context

We recall that a context is a condition over the environment, to control the activation context, the systems has to give some information to check if the condition is satisfied or not worth knowing that there is many type of context in ORBAC model, the following figure resume and presents the taxonomy of contexts and describes all the information necessary that the system should be able to provide for their evaluating [25].

Fig. 4. Context taxonomy and required data

In this model we need to add a novel type of context *(TRUST-CONTEXT)*, the role of this latest is to check if the trust levels of the user/agent respect the administrator levels or not .

As you can see n figure 4, our encoded model TRUST-ORBAC model for E-leaning platform based on multi agent system, give birth of a new level witch named ***trust level***, adding to abstract and concert levels.

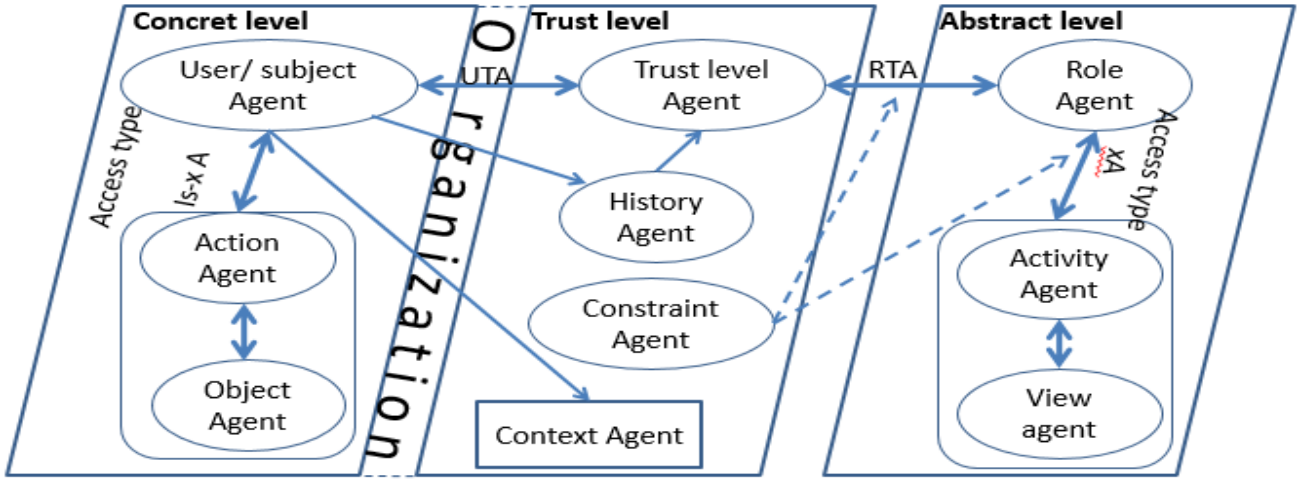

Fig. 5. New Trust-ORBAC model for e-learning platform based on multi-agent systems

VI. 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 its pedagogical scenario through the learning platform, using some tools and resources offered by the platform.
- The tutor supports the students in their learning activity, in order to help them, and evaluate their progress.
- The student use the pedagogical scenario proposed by the teacher, in order to achieve some educational goals like understanding the course content.

So each actors in the platform has a specific security levels associated with a level of his trust for example we have here some levels which identify the nature of student: *privilege, basic, public*. This concept keep to the user/agent possibility to enter with *public* policy which is the lower limit applied to the platform.

B. Example of access authorization process

Here we present an example to explain how the present model 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 ([0.38, 0.7]) = privilege student, Assigned Roles ([0.06, 0.3]) = public student and Assigned Roles ([0.16, 0.5]) = basic student. In general as first step a student must log in to the system by its credentials. Then the system verify and evaluate its trust value for example 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 platform as well as the uploading copies of courses that are not presented in the database we consider that Abusive/irrelevant comments and upload of an inauthentic file as negatives events.

During the session, we consider that the student writes some bad comments and upload a several inauthentic documents. Each of these activities get reported in the session, Let T evaluates trust periodically within a session. At some evaluation point we have v=0.345.This means that the student is not 'trustworthy' to the platform 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.

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[25].

In this simulation we considered that the trust value is an attribute of the subject, it's already calculated with an independent program.

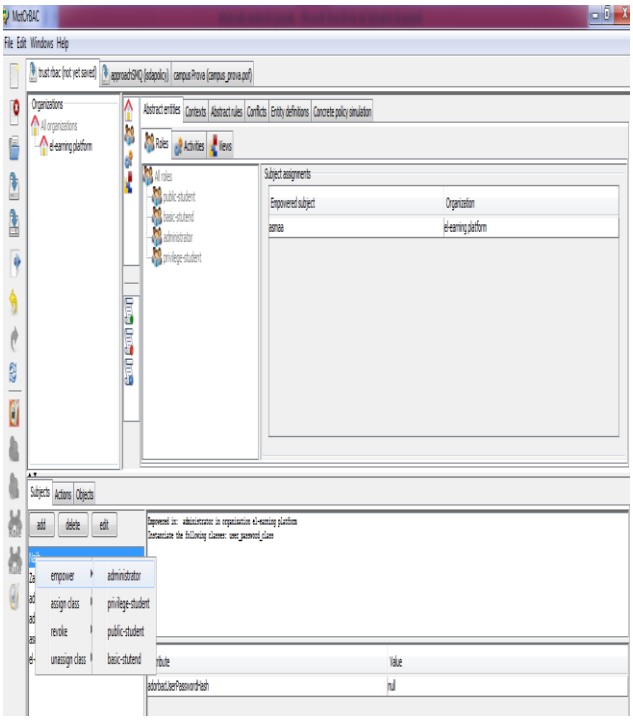

Fig. 6. role/subjects entities

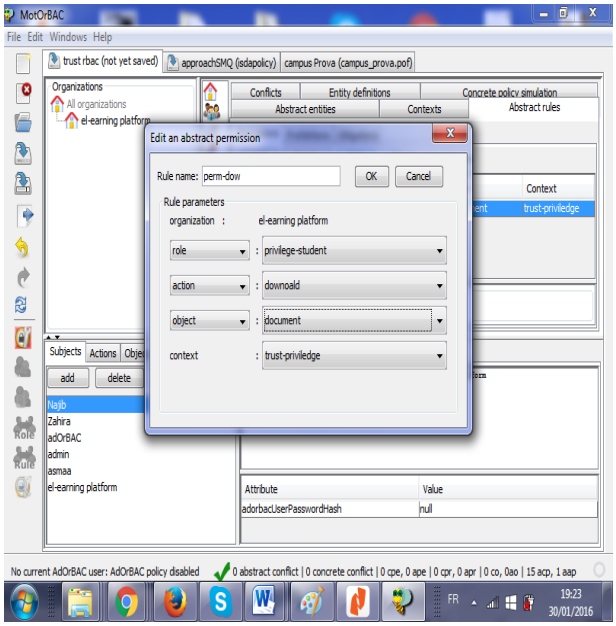

Fig. 7. The creation of the rules

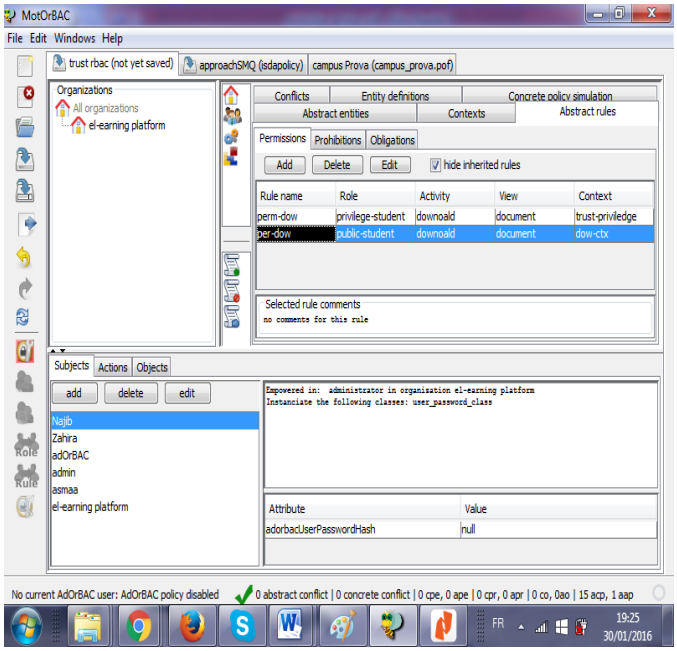

Fig. 8. Set of permission rules

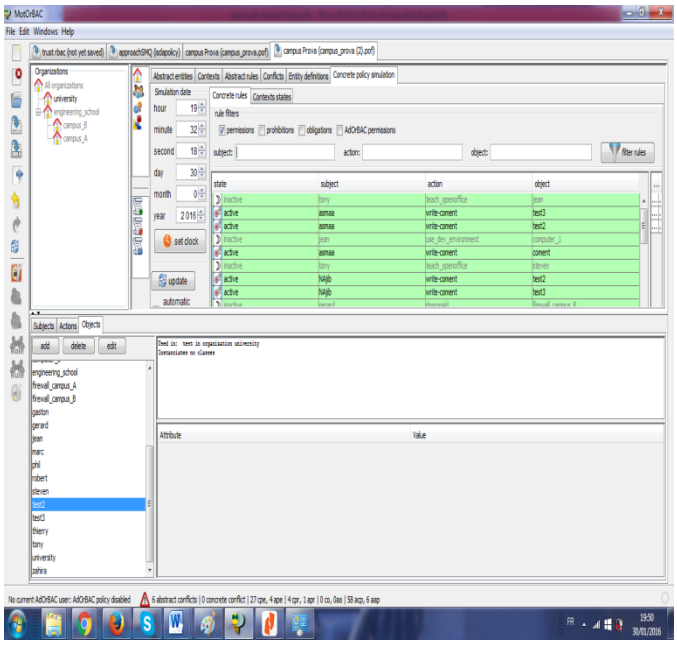

Fig. 9. Simulation of the policy

VII. Conclusion and Perspectives

The main goal of this paper, is to provide a new model based on ORBAC model , adapted to e-learning platform based on multi agent systems in order to have a satisfactory level of its security, taking into consideration the different interactions of these actors/agents and the integration of context and trust level. It allows to set certain conditions for the application of safety rules. This improvement may reside on richness as modularity of ORBAC model

This new model is implemented and evaluated by "MotOrbac": a simulation tool, to define its validity context

and limitations for an extended deployment .how ever this approach still not enough and rich so as future work , we encode the proposed model on Orbac model, in order to make it more rich and modular, and to prove how the expressive power and flexibility of ORBAC model work.

This work can be extended to a new TRUST-ORBAC model that analyzes the risks before making a decision to accept or deny access while taking account of the context information to determine trust levels of the subjects, the level of trust required by each role and the environmental risk threshold: The evaluation of risk should be done dynamically and in real time.

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] A.Kassid,N.El kamoun "Towards a new access control model based on Trust-level for E-learning platform" international journal of information assurance and security.

[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] 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.

[12] 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.

[13] 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

[14] Rodolfo Carneiro Cavalcante , Ig Ibert Bittencourt , Alan Pedro da Silva , Marlos Silva , Evandro Costa , Robério 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]

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

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

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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

[22] 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

[23] 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

[24] 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).

[25] A.kassid, N.El kamoun "Evaluation of a Security Policy Based on OrBAC Model Using MotOrBAC: Application E-learning' on Advances in Ubiquitous Networking: Proceedings of the UNet'15,PP.129-139.