Trust Levels Definition on Virtual Learning Platforms Through Semantic Languages

Paulo A. Gaona-Garcia[1], Jesús Soto-Carrión[2], Carlos E. Montenegro-Marin[3]
[1]*Engineering Faculty, Distrital University, Bogotá, Colombia.*
[2]*Artificial Intelligence Department, Pontifical University of Salamanca, Madrid Campus, Spain*
[3]*Engineering Faculty, Distrital University, Bogotá, Colombia.*

***Abstract* — Trust level concept is a topic that has opened a knowledge area about the profile evaluation and the people participation in Social Networks. These have presented a high knowledge profit, but at the same time it is necessary to analyze a group of variables to determine the trust participants' degree.**

In addition, this is a topic that from some years ago has been presenting a big expectation to settle some alternatives to generate confidence in an activer community on internet. To establish these parameters it is important to define a model to abstract some variables that are involved in this process. For this, it is relevant to take into account the semantic languages as one of the alternatives that allow these kinds of activities. The purpose of this article is to analyze the Trust Levels definition in the contents that are shared on Open Source Virtual learning Platforms through the use of a model of representation of semantic languages. The last ones allow determining the trust in the use of learning objects that are shared in this kind of platforms.

***Key Words* — Trust-Levels, FOAF, Web Service Security. WS-Trust, Ontology's**

Manuscript received October 1, 2010 This article is part of the thesis research project mentored Ph.D. program in Computer Engineering from the Pontificial University of Salamanca.

Author 1 is with the Distrital University, Bogotá, Colombia. The area of knowledge is Networks and communications. Is principal investigator of GIIRA group. (E-mail: pagaonag@udistrital.edu.co).

Author 2 –Jesús Soto Carrión, Artificial Intelligence Department, Pontifical University of Salamanca, Madrid Campus, Spain

Author 3 is with the Distrital University, Bogotá, Colombia. The area of Computer Science. Is investigator of GIIRA group. (E-mail: cmontenegro@udistrital.edu.co).

I. Introduction

The gradually growing of services about Open Source virtual learning platforms has permitted a dynamic access to a huge range of contents represented through learning objects. At the same time this demands a lot of time consuming for the creation and the definition of strategies about the validation of contents that are not plagiarized by a user. This implies first, that in academic terms there is not any contribution to the learning student's process and second that there is not any possibility to validate the contents authenticity presented by an author.

In some educative entities this kind of activities are carried out by an external authority through manual processes before the publication of the content. In this case it is done by the formation of an academic committee that checks and validates the content that is going to be published on these platforms. In the function of the academic committees, it is necessary to settle a group of policies to manage each one of the activities which involve a lot of time consuming for the checking and the publication.

To avoid this kind of delays, this document settles a strategy from the semantic point of view so as to identify the variables needed to highlight the trust levels of the contents that are published and shared on a LCMS platform (Learning Content Management System). This creates the possibility to check the contents before they are published on a virtual site.

II. LCMS Platforms Security

One of the most important information technology contributions, in educational terms, is the development of e-learning environment. With this it is possible to carry out the creation of strategies for all the educative entities, for the knowledge and for training through computer tools that are used on the communicative networks.

These learning environments are supported by different platforms that are invented with the purpose of giving access to educative contents that are part of the managing learning systems.

Nevertheless, the necessity of having the same kind of production, socializing and communication of contents allows an evolution from this kind of systems to others that are focused on the managing of contents. These are known as LCMS learning systems. However, the three processes mentioned before imply an additional task that is in relation to the authenticity of them through the possibility of acknowledging some theories of contents. It is possible to do this from the different computer techniques and the specifications that allow the creation of didactic material through the concept of learning objects.

The outlook that is worked on LCMS platforms in terms of computer security of content levels and their authenticity is not an explored area[3]. It is true that there are some security devices that are managed with certain data trust degree, but this is one of the weak points in most of the Open Source platforms. This means an unknown factor in order to try to identify the academic contents origin and its creation[3]. This kind of problems has not been controlled yet by the computer

DOI: 10.9781/ijimai.2010.134

devices. For the academic institutions this represents an important topic in the previously mentioned formation processes and their evaluation strategies.

So as to create strategies to carry out this kind of activities from the technological point of view it is better to work it from the same platform. This avoid the checking times, validation and authenticity of the contents and the formation of external academic committees that are in charge of the previous activities on a platform.

In order to do this activity in a virtual learning platform it is necessary to define a deeper language so as to associate and represent these activities. Ontology's models and semantic languages will allow creating a pertinent representation of the variables involved in this process. This implies and evaluation of the current platforms to identify if they are able to bear this kind of representations and at the same time the confidence in terms of computer science for the validation of contents and the authors possession to determine trust levels.

The new challenge is to determine the way in which learning objects, resources and digital contents are valid according to a group of parameters such as: profiles, trust levels and other kind of activities that are in relation to getting in touch with the following topics. Taking all this into account, it is necessary to define some processes related with these users' activities on a virtual platform so as to identify these groups of characteristics and to begging the identification of this kind of characteristics start with the definition of a strategy for its development.

III. IDENTIFICATION OF TRUST LEVELS ON A VIRTUAL LEARNING PLATFORM

To locate the processes which permit the definition of activities and the identification of trust levels about contents created by an author on a virtual learning platform; it is necessary to adapt the workflow definition proposed by WFMC (Workflow Management Coalition) [4], [5], [6] to the platform characteristics in relation to a user on the same platform.

On figure 1 there are some processes that are carried out for the definition of trust levels. These are represented by ontology's model according to the user's profile and content published by him. These characteristics are going to take into account the following items.

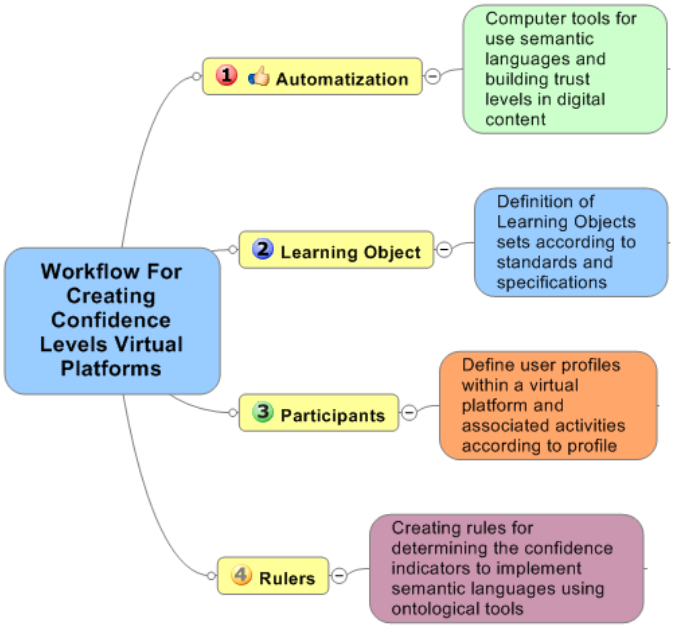

Fig 1.process for the definition of trust levels on a virtual platform. (Author)

A. Definition of Automation Processes

In this stage it is carried out the selection of technological tools for the creation and definition of ontology's rules; that allows the definition of a language representation outline for the definition of trust levels on LCMS platforms. These processes represent the simplicity and optimization of the complex processes that are going to be taken into account:

- Contents Quality: To improve the contents quality to have all the important information available and reducing the time to consult.
- Reduction of checking time content: The reduction of time processes by an academic committee and an external inspector. This process will be carried out by the platform through the ontology's representation of trust level about content.
- Profiles definition: According to the content reliability published on a LCMS.
- Definition of languages and tools: Next there are presented some alternatives to work on the representation of processes on a LCMS platform:

  In language ontology's selection we use the ontology's definition language OWL and the graphic representation through Protége. This information is expanded whit more details in the Rules Process Definition.

B. Learning Objectives Definition Processes

Learning objectives concept is in relation to a key element for the definition of contents that is represented through a group of SCORM specifications (Sharable Content Object Reference Model) defined by [7]. This allows the relation with the user's characteristics.

Learning object and representation of contents

So as to identify functional parts it is important to highlight the concept: Learning Objectives from the programming point of view. In its works [8] it is relevant the idea of the representation of contents reflected through the creation of contents. In this way, the current concept has changed to work with RLO (Reusable Learning Object). This topics were developed under advices given by [9] and by [10] on the definition metadata and valid elements for the definition of contents. The last ones are adapted to E-learning to offer a program focused on objects to about components for the definition of most of the specifications.

C. Participants definition processes

For the definition of the user's actions it is necessary to take into account the concept of trust levels. In general, this concept is related to the user's participation on Social Networks. In this way, we are going to present a lot of proposals that have been showed for the definition of the concept already mentioned according to the necessities of our proposal.

Standard WS- Trust

This rule is a standard proposed by OASIS (Organization for the Advancement of Structured Information Standards). This is an organization that with other computer companies are devoted to define access standards for Web Services on Internet; known as WS-Trust 1.4 [11].

This initiative was created by IBM, Microsoft, and VeriSign. These present a communication infrastructure to make easier Web security applications. Now it is developed, on internet, by an interdisciplinary group known as OASIS. In this group there are more than 700 organizations that are supporting this initiative in order to try to standardize all the communication processes in a secure way on the Web. This representation has a group of standards that describe basic security devices in relation to Web services through extensions like SOAP (Simple Object Access Protocol) [12]. These extensions give some characteristics of integrity and reliability to the message.

Another characteristic of this standard is the one in relation to extensions. These consist on the expansions of the security devices capacity. This is important for the application, tokens security swap and the definition of the trust relations.

Security tokens interchange allows the emission and the spread of documents in different trust controls. This could be valid from the definition of PKI (Public Key Infrastructure) [13] and CA (Certificate Authority) that allows the digital certifications through digital signs in contents. In Figure 2 shows the group of security specification.

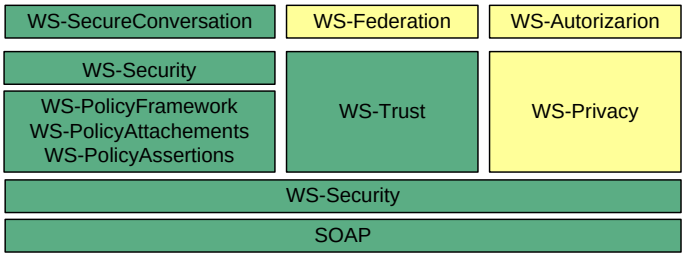

Fig. 2 Group of security specifications WS [2].

The trust level defined by this standard presents one important characteristic. One authority is willing to trust in another one so as to carry out a group of actions and set some statements. This standard defines three kind of trust:

- *Direct Trust*: it is when one piece of trust accepts all or one piece of request as true. This is in the token sent by the addresser.
- *Direct Negotiated Trust*: it is when one part trusts in a second part that at the same time trusts in a third part.
- *Indirect Negotiated Trust*: It is a variation of the direct negotiated trust. A second part negotiates with a third part or additional parts to evaluate their trust.

This is not the only proposal about trust levels. The proposal developed by [14] defines the following kinds of trust:

- *Certified trust*: It is the user's trust in a user as notary. The code is shared in a personal and confidential way.
- *Hierarchical* trust: It is the confidence in certified authorities.

This Project shows one way to guaranty the user's authenticity without the need of certified authorities. Trust levels appears with PGP (Pretty Good Privacy) [1] device. This is used for the communication via e-mail. This device defines 4 trust levels presented in the figure number 3.

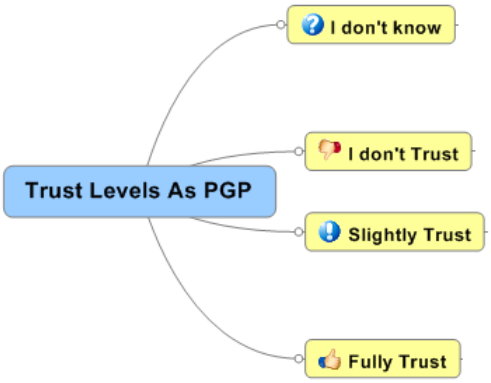

Fig. 3 Group of security specifications WS

One limitation factor of this model is that it is based on a direct trust and, in this way; there is no connection whit the needs of LCMS platforms. One answer to this problem is through the definition of nine trust levels. Table I.

TABLE I
TRUST LEVELS DEFINE BY [10]

Trust Level	Worth	Trust Level	Worth
Absolute distrust	1	Slightly trust	6
High Slightly trust	2	Moderate trust	7
Slightly distrust	3	High trust	8
Slightly distrust	4	Absolute trust	9
Neutral	5		

FOAF Project

Based on the vocabulary given by (Friend of a Friend) defined in [15] we have one description of the vocabulary used on the Semantic Web through RDF languages (Resource Description Framework) and OWL (Ontology Web Language) and the case of the ontology's WOT (Web of Trust) [16]. Next there is s set of characteristics that give an adequate vocabulary to use a set of computer tools with cryptographic public code. This has the purpose of defining some rules to get the user's trust level on a virtual platform according to the given signs by the certificated trust or the certificated trust if there are a lot of developed activities.

D.Processes Definition about Rules Level

After the identification of security models devices based on trust levels applied to the current platforms we see that they do not cope with the virtual platform necessities because they do not have a vocabulary to express the different kind of users, relations, resources (Learning Objects), etc., What is more, they are not able express anything about the environments where the other elements are.

It is not possible to measure the trust level by the number of signs, the certifier trust level and the kind of sings on a virtual platform. It is because each user has a specific role that changes according to the environment where he is. For example: one user is a teacher on a virtual site and a student in another. If there is a user in the same conditions and his trust relation with the first user is student-teacher on a site this relation could not be generalized to the entire platform because other site could be for student-student. Here there is a clear necessity for the creation of ontology's model based on trust levels with a vocabulary that allows:

a. The implementation of a security device based on trust levels.
b. The permission to do activities according to the trust level.
c. The quality measure of the learning objects on the platform.
d. Making decisions based on the users' actions and their development on the LCMS platform. The system makes autonomous decisions.
e. The measure personalization of trust levels that are in agreement with the one who implements LCMS organizational rules.

Next a proposal is presented to establish trust levels on virtual platforms presenting the term *Trust Indicator* to measure the user's trust level in a certain environment.

a. Confidence users' indicators

So as to define these characteristics some variables were cleared taking into account, trust levels, profiles, user's abilities and moods on a virtual platform.

In figure number 4 there are some trust indicators for a user depending on his role, student or teacher on a virtual platform.

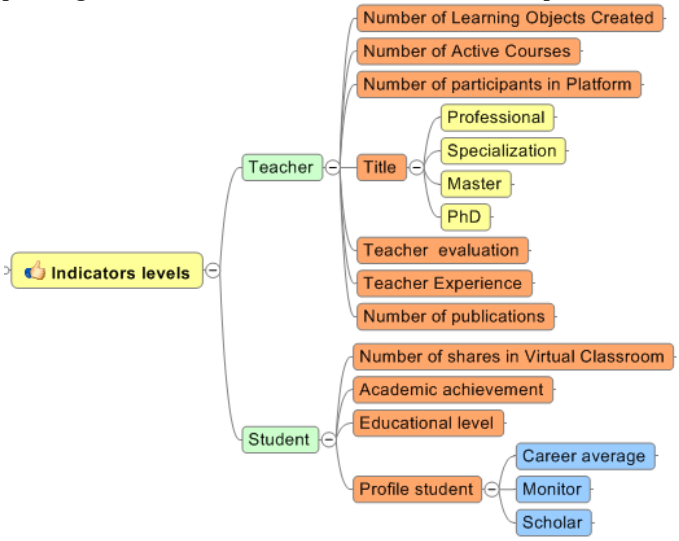

Fig. 4 Indicators Levels of a User

In figure number 5, a user is able to have different profiles on a virtual platform. Also, it is possible to measure some abilities to create a course out the curriculum of a career or a project. For example:

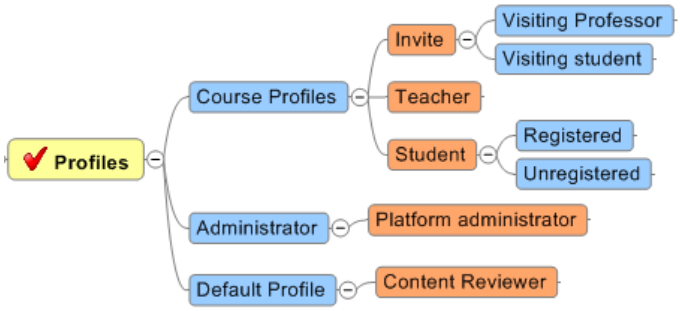

Fig. 5 Profiles Levels of a User

In Figure 6 shows the profiles of abilities of a user within a virtual platform:

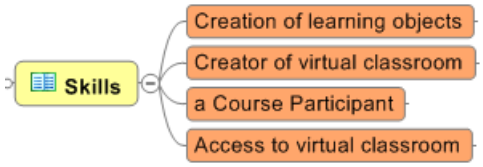

Fig.6 Skills profiles of a user

A user with a general teacher role and the necessary trust

level to create courses wants to create an elective course to present a new topic or create a new subject.

At the same time some kind of guests were defined because they can come from another institution platform and there are some trust indicators defined. These may help to measure the user's trust level depending on his profile on the virtual platform.

Once the user's variables were identified, it is necessary to identify the variables to define trust indicators to courses.

In figure 7 shows the indicators of the characteristics and status of a user within a virtual platform

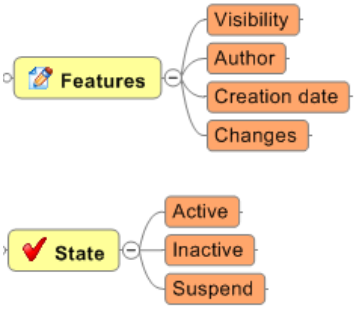

Fig.7 Skills profiles of a user

b. Trust Indicators for Courses

The variables are defined so as to measure the trust level for a course from the point of view of the use so as to give to a user ability or condition on a platform depending on his profile.

Finally, some trust indicators are defined for the contents presented through learning objectives.

c. Trust Indicators to Learning Objectives

For the variables it is important to define associated characteristics for the creation of these contents form a group of specifications or standards to define rules. In Figure 8 arise trust indicators defined for the creation of an online course:

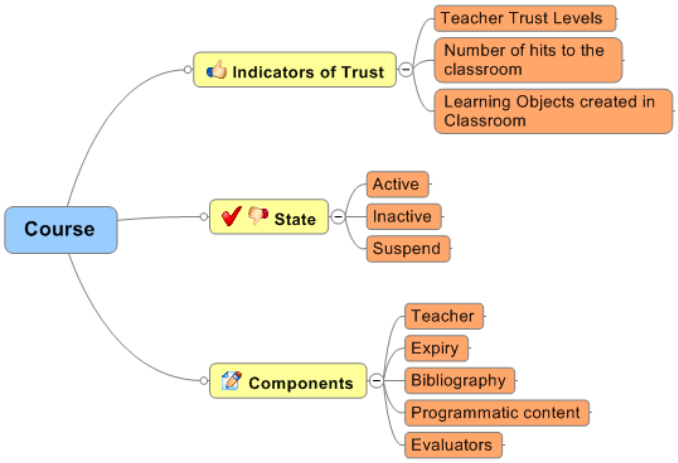

Fig. 8 Courses elements and components on a virtual classroom

Under the previous schemes we can mention the well known trust indicators and learning objects. These indictors work as tools to measure trust levels and their settlement. In Figure 9 shows the trust indicators defined for the creation of learning objects.

Any kind of indicators might have the following characteristics:

- They have to be registered in a theoretical framework
- Specific
- Explicit
- Relevant and appropriate

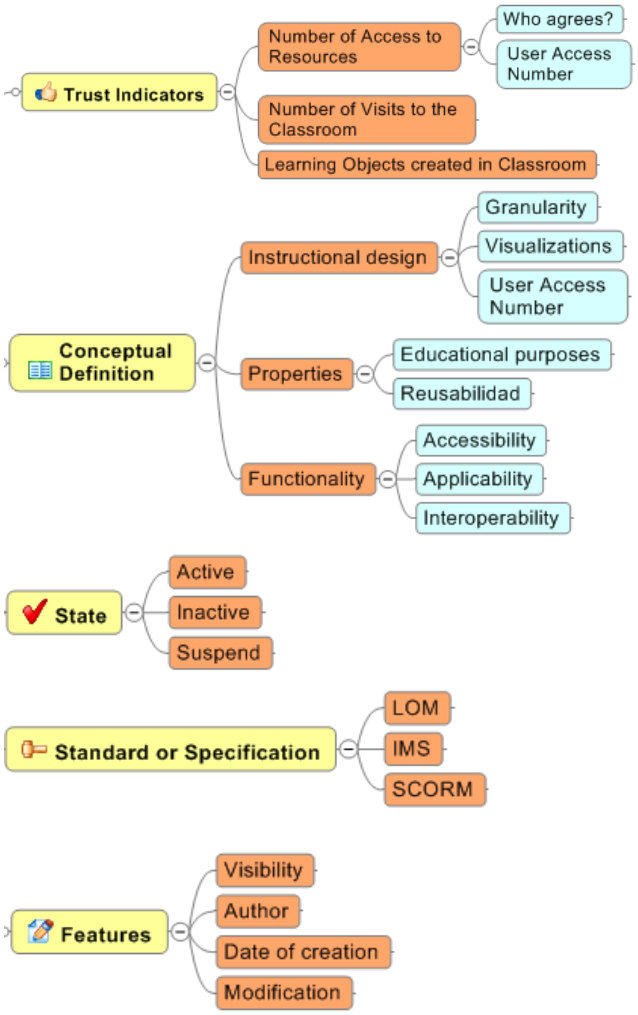

Fig. 9 Trust indicators for Learning Objects

- The indicators are not only for one specific action
- They are clear and easy to comprehend

Taking into account all the previous aspects, trust levels are not only devices for a secure communication with platform tools such as: forums, internal e-mail, blogs, etc. Also, they

work as support for the learning objects quality management, courses, frums, etc.

Trust indicators give us a measurement to give a trust level to a user in a specific context. After the announcement we give a value to the indictor to evaluate the impact on the trust level. This is according to the organizational rules implemented by a LCMS.

IV. Development of LCMS Platform Ontology's Model Based on Trust Levels.

Because of the difficulty of the trust levels and indictors introduced on a platform it is necessary the creation of an ontology's model based on trust levels in order to have a vocabulary of terms and the semantic expressiveness to make easier:

- The implementation of a security device based on trust levels.
- The automation to give permissions so as to do activities according to the trust level.
- The learning objects quality measurement on a learning platform
- To make autonomous decisions by the system
- To personalize the trust levels measurement so that they can be in agreement with the organizational rules implemented by a LCMS

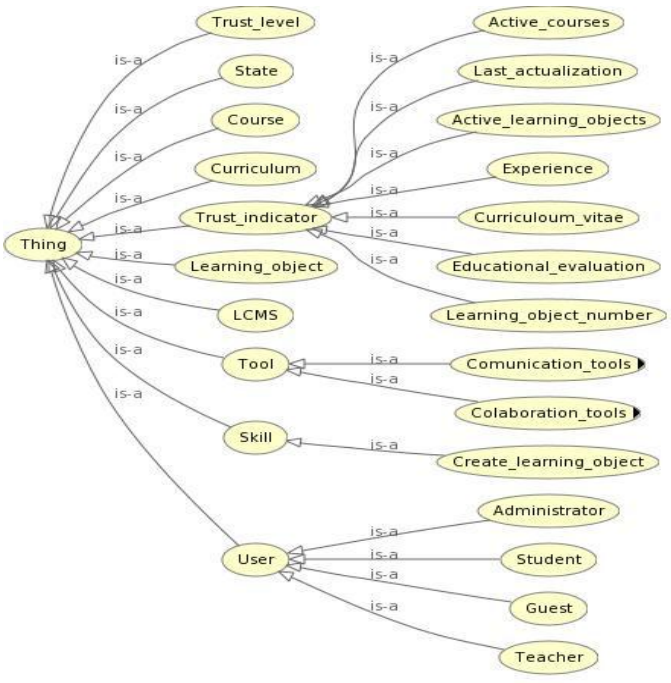

Fig. 10 Class Hierarchy Ontological Model

Taking into account the previous rules it is necessary to settle an ontology's model for the representation of trust levels that are planned to work in a virtual platform using OWL-DL language [17] created by W3C Web Ontology (WebOnt) Working Group.

In order to develop its methodologist part it was based on Metontology proposed by the Ontology group of Universidad Politécnica de Madrid. This allows the creation of ontology's about knowledge. This was proposed by Foundation for Intelligent Physical Agents (FIPA). It promotes the inner-operability through some applications based on agents and clear work proposed by [18].

In figure number 10 it is presented one approximation to the model that it is good to develop. This is showed by a Frames model (classifying it according to its internal richness).

In Figure 11 can display the properties of ontology model classes created.

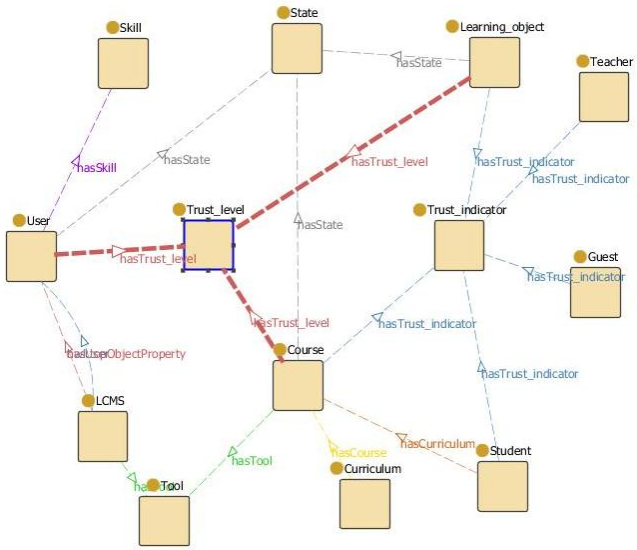

Fig. 11 Properties of Class Model

Finally we represent in Figure 12 at the properties of the relations of ontological model created

V. Conclusion

So as to define a trust level on virtual platforms, it was taken into account processes through Workflow. This is an alternative to identify activities and to define actions developed by a user on a virtual platform. So, workflow on the platform was identified through a Workflow Management System (WMS). This system is able to interpret the definition of the process, interact with the workflow participants, and if it is necessary, to call the use of technology information tools and computer applications to define the business nature to work on virtual platforms.

The identification through workflow processes allows the identification of the actions carried out by the users. These were permissions, actions and routes to follow for the representation of the trust levels on the virtual platform. This is one of the alternatives for the creation of rules that are that are with trust levels and to define the processes in relation to the users' activities and behavior on a virtual platform according to the definition of each one of the profiles.

The previous proposal points at the definition of a "Semantic Web Security Learning Content Management

System" SWS LCMS in which it is possible to manage the knowledge from the definition of trust levels through some variables such as: trust levels through content specification, users' profiles and courses characteristics. These create the development of a virtual learning platform based on intelligent agents to give value to this kind of contents based on a set of rules defined on ontology's model with learning objects based on a group of specifications.

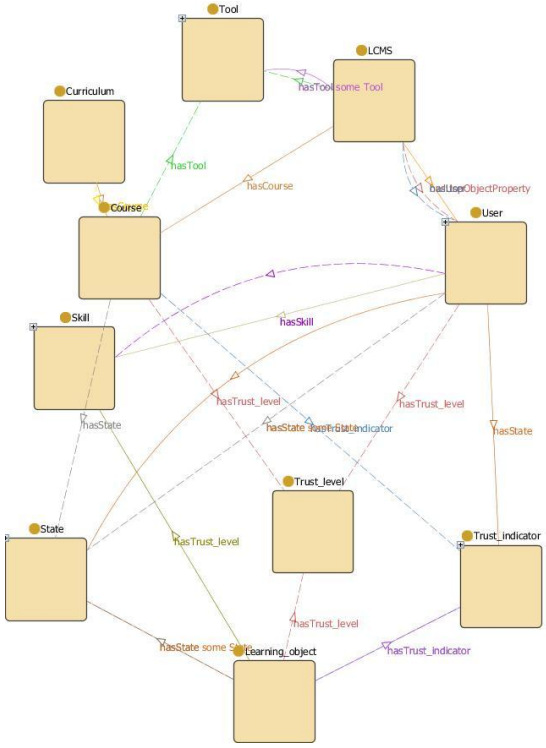

Fig. 12 Model and Property Relations

The rules for the semantic vocabulary were defined under FOAF and a combination of Trust Levels on Social Networks, but at the same time it is necessary to identify the activities that were carried out on a virtual platform what makes difficult to create connections because of the difficult activities that a user is able to do on a virtual platform.

REFERENCES

[1] [1] P. Zimmermann, "The official PGP user's guide," 1995.

[2] [2] D. Fensel and C. Bussler, "The web service modeling framework WSMF," Electronic Commerce Research and Applications, vol. 1, pp. 113-137, 2002.

[3] [3] P. Gaona, et al., "Modelo informático para autenticidad de contenidos mediante el concepto de Web of Trust sobre plataformas virtuales LCMS. LACCEI," p. 10, 2010.

[4] [4] R. Allen, "Open Image Systems Inc., United Kingdom Chair, WfMC External Relations Committee;"The Workflow Handbook 2001"; Workflow Management Coalition," ed: October, 2001.

[5] [5] C. Prior, "Workflow Handbook," Maestro BPE Pty Limited, Australia, 2005.

[6] [6] D. Hollingsworth, "Workflow management coalition: The workflow reference model," Workflow Management Coalition, 1993.

[7] [7] A. SCORM, "Documentation 2005," ed, 2004.

[8] [8] G. Santos, "Secuenciamiento de actividades educativas orientado a la reutilización y la auto-organización en tutoría inteligente," 2007.

[9] [9] R. McGreal, "Learning objects: A practical definition," INSTRUCTIONAL TECHNOLOGY, p. 21, 2004.

[10] [10] D. Wiley and E. Edwards, "Online Self-Organizing Social Systems: The Decentralized Future of Online Learning," Quarterly Review of Distance Education, vol. 3, pp. 33-46, 2002.

[11] [11] A. Nadalin, et al., "WS-Trust 1.3," OASIS Standard, March, 2007.

[12] [12] E. Cerami and S. Laurent, Web services essentials: O'Reilly & Associates, Inc. Sebastopol, CA, USA, 2002.

[13] [13] W. Ford, et al., "Xml key management specification (xkms)," Retrieved from: http://www.w3.org/TR/2001/NOTE-xkms-20010330, 2001.

[14] [14] E. Gordo and J. Soto, "Autenticidad basada en la Web Semántica de confianza," IJIMAI, 2007.

[15] [15] D. Brickley and L. Miller, "FOAF vocabulary specification 0.91," Namespace document, FOAF Project (November 2007) http://xmlns. com/foaf/0.1, 2007.

[16] [16] N. Noy, et al., "User ratings of ontologies: Who will rate the raters," 2005.

[17] [17] D. McGuinness and F. Van Harmelen, "OWL web ontology language overview," W3C recommendation, vol. 10, pp. 2004-03, 2004.

[18] [18] A. Gómez-Pérez, et al., Ontological Engineering: with examples from the areas of Knowledge Management, e-Commerce and the Semantic Web: Springer Verlag, 2004.

Paulo Alonso Gaona García. He´s Systems Engineer of Distrital University., Bogota-Colombia. Master of Information Science and Communications with emphasis in teleinformatics of the same university. Is a Ph.D. candidate in Computer Engineering University of Salamanca in Madrid - Spain. Is professor of plant of Distrital University, is an instructor participates in Cisco CCNA and Networking Research Areas, E-Lerning platforms and IT security. Is Director of the Investigation Group GIIRA of Distrital University.

Jesus Soto Carrión. Artificial Intelligence Department, Pontifical University of Salamanca, Madrid Campus, Spain.

Carlos Enrique Montenegro Marin. He's Systems Engineer of Distrital University., Bogota-Colombia. Master of Information Science and Communications with emphasis in teleinformatics of the same university. Is a Ph.D. candidate in Computer Engineering University of Salamanca in Madrid - Spain. Is professor of plant of Distrital University. Is member of the Investigation Group GIIRA of Distrital University.