Article publicat / Published article:

Miguel, J., Caballé, Santi, Xhafa, F., Prieto, J. (2015) Security in online web learning assessment: providing an effective trustworthiness approach to support e-learning teams. "World wide web: internet and web information systems". Vol. 18, num. 6. p.1655-1676. Doi: 10.1007/s11280-014-0320-2

WWWJ manuscript No.
(will be inserted by the editor)

Security in Online Web Learning Assessment

Providing an Effective Trustworthiness Approach to Support e-Learning Teams

Jorge Miguel · Santi Caballé · Fatos Xhafa · Josep Prieto

Received: date / Accepted: date

Abstract This paper proposes a trustworthiness model for the design of secure learning assessment in on-line web collaborative learning groups. Although computer supported collaborative learning has been widely adopted in many educational institutions over the last decade, there exist still drawbacks which limit their potential in collaborative learning activities. Among these limitations, we investigate information security requirements in on-line assessment, (e-assessment), which can be developed in collaborative learning contexts. Despite information security enhancements have been developed in recent years, to the best of our knowledge, integrated and holistic security models have not been completely carried out yet. Even when security advanced methodologies and technologies are deployed in learning management systems, too many types of vulnerabilities still remain opened and unsolved. Therefore, new models such as trustworthiness approaches can overcome these lacks and support e-assessment requirements for e-Learning. To this end, a holistic security model is designed, implemented and evaluated in a real context of e-Learning. Implications of this study are remarked for secure assessment in on-line collaborative learning through effective trustworthiness approaches.

Keywords trustworthiness · e-assessment · information security · collaborative learning

Jorge Miguel · Santi Caballé · Josep Prieto
Department of Computer Science, Multimedia, and Telecommunication
Open University of Catalonia, Barcelona, Spain
E-mail: jmmoneo,scaballe,jprieto@uoc.edu

Fatos Xhafa
Department of Languages and Informatic Systems
Technical University of Catalonia, Barcelona, Spain
E-mail: fatos@lsi.upc.edu

1 Introduction

Computer-Supported Collaborative Learning (CSCL) has been widely adopted in many educational institutions over the last decade. Among these institutions, the Open University of Catalonia[1] (UOC) develops on-line education based on continuous evaluation and collaborative activities.

Although on-line assessments (e-assessments) in both continuous evaluation and collaborative learning have been widely adopted in many educational institutions over the last years, there exist still drawbacks which limit their potential. Among these limitations, we investigate information security requirements in assessments which may be developed in on-line collaborative learning contexts.

Despite information security technological enhances have also been developed in recent years, to the best of our knowledge, integrated and holistic security models have not been completely carried out yet. Even when security advanced methodologies and technologies are deployed in Learning Management Systems (LMS), too many lacks still remain opened and unsolved. Therefore, as new models are needed, in this paper we propose a trustworthiness approach based on hybrid evaluation which can complete these lacks and support e-assessments requirements.

The paper is organized as follows. Section 2 shows the background about security in e-Learning as well as our research already done with respect to trustworthiness and security in e-assessment. Section 3 reviews the main factors, classification and security issues involved in security in e-assessments and we discussed that security improvements in e-assessments cannot be reached with technology alone; to fill this drawback, in Section 4, we extend our security model with the study of the trustworthiness dimension. Once studied trustworthiness factors and rules and presented our previous work, in Section 5 we describe a model based on trustworthiness applied to e-assessments. In Section 6, we conduct our research to peer-to-peer e-assessment developed in a real on-line course and by developing a statistical and evaluation analysis for the course collected data. Finally, Section 7 concludes the paper highlighting the main ideas discussed and outlining ongoing and future work.

2 Security in e-Learning Background

Since 1998, information security in e-Learning has been considered as an important factor in e-Learning design. Early research works about these topics [7] are focused on confidentiality and these privacy approaches can be found in [13]. Despite the relevance of privacy requirements in secure e-Learning, information security does not serve for privacy services only. Indeed, in many works [6,23], security in e-Learning has been treated following more complex analysis and design models.

In [23] the author argues that security is an important issue in the context of education. Security is mainly an organizational and management issue and improving security is an ongoing process in e-Learning. This proposal is the first

[1] The Open University of Catalonia is located in Barcelona, Spain. The UOC offers distance education through the Internet since 1994. Currently, about 60,000 students and 3,700 lecturers are involved in over 8,300 on-line classrooms from about 100 graduate, post-graduate and doctorate programs in a wide range of academic disciplines. The UOC is found at http://www.uoc.edu

approach in which information security is applied to LMS as a general key in e-Learning design and management. Furthermore, in [6] it is presented how security in e-Learning can be analyzed from a different point of view, that is, instead of designing security, the author investigates threats for e-Learning and then, several recommendations are introduced and discussed in order to avoid detected threats. On the other hand, more specific security issues in secure e-Learning have been investigated (e.g. virtual assignments and exams, security monitoring, authentication and authorization services). These works have been summarized in [10–13].

So far we have discussed on the security design in e-Learning from a theoretical point of view. However, some authors argue we actually need to understand attacks in order to discover those relevant security design factors and figure out how security services must be designed [5]. Researchers have already conducted many efforts proposing taxonomies of security attacks. In [24], through analyzing existing research in attack classification, a new attack taxonomy is constructed by classifying attacks into dimensions. This paper also offers a complete a complete and useful study examining existing proposals. Nevertheless, since attacks taxonomies might be applied to cover each kind of attack, which might occur in LMS, they are not closely related to security design in e-Learning. In order to fill this gap, in [13], we have proposed an alternative approach which associate attacks to security design factors.

We now extend the background about security in e-Learning by analyzing real-life security attacks and vulnerabilities, which could allow attackers to violate the security in a real context. In this sense, several reports are found, which justify the relevance of security attacks during the last two years. In particular, the study presented in [2] uncovered that security attacks are a reality for most organizations: 81% of respondents' organizations experienced a security event (i.e. an adverse event that threatens some aspect of security). Finally, we can consider specific LMS real software vulnerabilities. Moodle is an Open Source LMS which is massively deployed in many schools and universities. In Moodle Security Announcements [2], 40 serious vulnerabilities have been reported in 2013.

In previous research [10–13] we have argued that general security approaches do not provide the necessary security services to guarantee that all supported learning processes are developed in a reliable way. The rest of this section presents our work already done and our research results obtained at the time of this writing regarding analysis and security design in CSCL, trustworthiness and e-assessment and a trustworthiness methodology proposal.

We have investigated how to enhance CSCL security in terms of security analysis and design. To this end, we have analysed security properties models, how to model students' interaction and trustworthiness, and how security properties and students' interaction are involved in CSCL activities. These goals and research results are summarized in the following list:

- Security requirements in CSCL. In [11] it is argued that current e-Learning systems supporting on-line collaborative learning do not sufficiently meet essential security requirements and this limitation can have a strong influence in the collaborative learning processes.
- Design of secure CSCL systems. In [10] the problems caused in collaborative learning processes by the lack of security are discussed and the main guidelines

[2] https://moodle.org/mod/forum/view.php?f=996

for the design of secure CSCL systems are proposed to guide developers to incorporate security as an essential requirement into the collaborative learning process.
- Security requirements in mobile learning. In [12] it is presented an overview of secure LMSs, inspecting which are the most relevant factors to consider, and connecting this approach to specific aspects for mobile collaborative learning. Then, real-life experience in security attacks in mobile learning are reported showing a practical perspective of the learning management system vulnerabilities. From this experience and considerations, the main guidelines for the design of security solutions applied to improve mobile collaborative learning are proposed.
- Security requirements in MOOCs. In [13] it is investigated the lack of provision of IS to MOOC, with regards to anomalous user authentication, which cannot verify the actual students identity to meet grading requirements as well as satisfy accrediting institutions. In order to overcome this issue, it is proposed a global user authentication model called MOOC-SIA.

Once security and CSCL issues have been analysed, we have focused our research work on trustworthiness analysis and data processing based on trustworthiness modelling in order to define trustworthiness modelling concepts (i.e. techniques and measures). The aim is to build normalization methods and propose parallel processing techniques to speed and scale up the structuring and processing of basic data. These objectives are related to the design of secure learning objects, trustworthiness assessment and prediction, and the development of pilots for validation processes. This work has produced the following research results:

- Trustworthiness model. In [15] a trustworthiness model for the design of secure learning assessment in on-line collaborative learning groups is proposed. To this end, a trustworthiness model is designed in order to conduct the guidelines of a holistic security model for on-line collaborative learning through effective trustworthiness approaches.
- Parallel processing approach. In [14] it is proposed a trustworthiness-based approach for the design of secure learning activities in on-line learning groups. The guidelines of a holistic security model in on-line collaborative learning through an effective trustworthiness approach are presented. As the main contribution of this paper, a parallel processing approach, which can considerably decrease the time of data processing, is proposed thus allowing for building relevant trustworthiness models to support learning activities even in real-time.
- Trustworthiness normalization methods. In [19] an approach to enhance information security in on-line assessment based on a normalized trustworthiness model is presented. In this paper, it is justified why trustworthiness normalization is needed and a normalized trustworthiness model is proposed by reviewing existing normalization procedures for trustworthy values applied to e-assessments. Eventually, the potential of the normalized trustworthiness model is evaluated in a real CSCL course.
- Trustworthiness prediction. In [18] previous trustworthiness models are endowed with prediction features by composing trustworthiness modelling and assessment, normalization methods, history sequences, and neural network-based approaches. In order to validate our approach, a peer-to-peer e-assessment model is presented and carried out in a real on-line course.

The next phase of our research on security in e-Learning based on trustworthiness has been focused on building a trustworthiness methodology offering a guideline for the design and management of secure CSCL activities based on trustworthiness assessment and prediction to detect security events and evidences. In [17] the need of trustworthiness models as a functional requirement devoted to improve information security is justified. A methodological approach to modelling trustworthiness in on-line collaborative learning were proposed. This proposal aims at building a theoretical approach to provide e-Learning designers and managers with guidelines for incorporating security into on-line collaborative activities through trustworthiness assessment and prediction.

Finally, we have endowed our trustworthiness approaches with the concept of students' profile and collective intelligence features. In [16] we have discovered how security can be enhanced with trustworthiness in an on-line collaborative learning scenario through the study of the collective intelligence processes that occur on on-line assessment activities. To this end, a peer-to-peer public students profile model, based on trustworthiness is proposed, and the main collective intelligence processes involved in the collaborative on-line assessments activities were presented.

To sum up, the present paper contribute to existing security solutions models by providing an innovative approach for modelling trustworthiness in a real context of secure learning assessment in on-line collaborative learning groups. The study shows the need to combine technological security solutions and functional trustworthiness measures.

3 Secure e-Assessment

In this section, we present a review of the main factors, classification and security issues involved in security in e-assessments. Firstly, security properties related to e-assessments are evaluated by examining and selecting most relevant ones. Then, an assessments classification is depicted in order to analyse how e-assessments types and factors are related to previously selected security properties and. Finally, we propose a security model which extends technological security techniques adding functional requirements to secure e-assessments.

3.1 Authenticity in e-Assessments

In order to determine whether or not an e-assessment is secure, both from students' as evaluators' point of view, it can be inquired if the e-assessment satisfies the following properties:

- Availability. The e-assessment is available to be performed by the student at the scheduled time and during the time period which has been established. After the assessment task, the tutor should be able to access the results to proceed to review the task.
- Integrity. The description of the e-assessment (statement of the activity, etc.) must not be changed, destroyed, or lost in an unauthorized or accidental manner. The result delivered by the student must achieve the integrity property too.

– Identification and authentication. While performing the evaluation task, the fact that students are who they claim to be must be verifiable in a reliable way. In addition, both students' outcomes and evaluation results must actually correspond to the activity that students have performed.
– Confidentiality and access control. Students will only be able to access to e-assessments that have been specifically prepared to them and tutors will access following the established evaluation process.
– Non repudiation. The LMS must provide protection against false denial of involvement in e-assessments.

Due to the difficulty of provisioning a complete secure e-assessment including all of these properties, a first approach of secure e-assessments selects a subset of properties which can be considered as critical in evaluation context. The selected properties are identification and integrity. Integrity must be considered both as authorship as well as data integrity. Therefore, we will be able to trust an e-assessment process when identification and integrity properties are accomplished. In the context of e-assessments, with regarding to identification, students are who they claim to be when they are performing the evaluation activities (e.g. access to the statement in a test, answering a question in an interview with the evaluator, etc.). In addition, dealing with integrity and authorship, we trust the outcomes of the evaluation process (i.e. a student submits evaluation results) when the stunted is actually the author and these elements have not been modified in an unauthorized way. It is important to note that e-assessments are developed in a LMS and, since the LMS is an information system, two different items are involved in this context: processes and contents which are related to integrity and identification. Therefore, services applied to e-assessment must be considered in both a static and a dynamic way.

3.2 Assessments Classification

The scope of our research, with regarding to assessment, is the evaluation model used in UOC courses. Evaluation models used in UOC may be classified in accordance with the following factors or dimensions: (i) type of subjects; (ii) specific evaluation model; (iii) evaluation application; (iv) agents involved in the evaluation processes. Fig. 1 shows factors and evaluation types.

Firstly, we have to analyse the agents who are involved in evaluations processes. The agents selected are students, tutors and the LMS, that is, students carrying out learning activities in a LMS which are assessed by tutors. In this context, we consider two types of subjects in UOC courses, a standard subject has many students in the virtual classroom and the level of collaborative learning activities is low. On the other hand, a collaborative subject is designed following a intensive collaborative learning model which is performed by few students arranged in learning groups. Regarding these evaluation models, two different models are selected, the continuous evaluation model allows the tutors to assess the students throughout the course by evaluating each activity in the subject; in contrast, a evaluation model based on final exams focuses the evaluation processes on an assessment instrument at the end of the course.

Once the subject, evaluation and agent dimension are presented, we focus the analysis on evaluation applications. In manual evaluation methods, tutors usu-

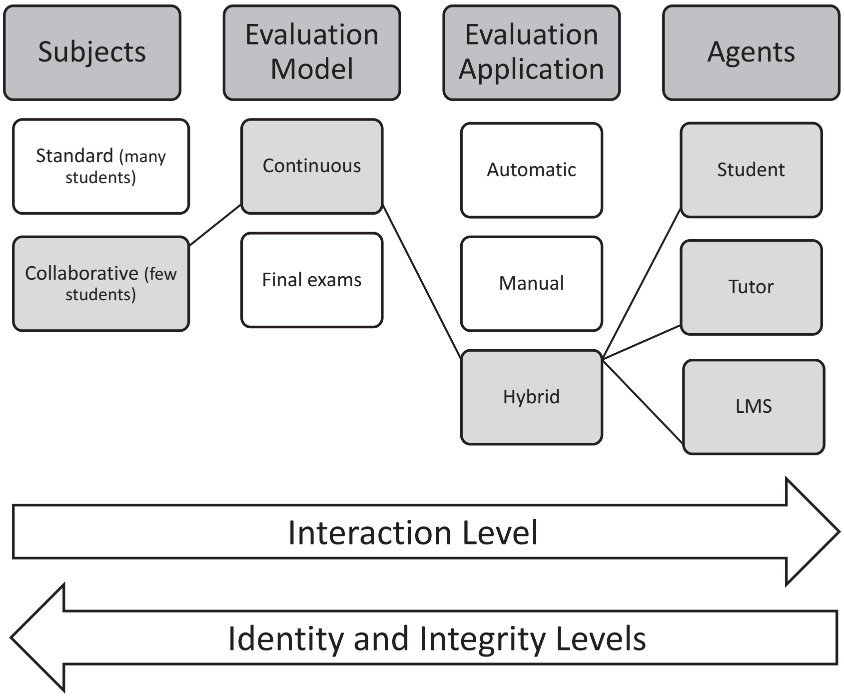

Fig. 1 Evaluation types

ally participate directly and intensely in the evaluation process. This model has scalability problems but can provide better guarantees for students' identification and authorship because the degree of interaction between tutors and students is higher than in others evaluation methods. Although this statement may be true in general cases, it may not apply to all situations, that is, the interaction level does not necessarily mean that students' identification is authentic (as defined above: data integrity and authorship). On the other hand, automatic methods do not involve tutors participation (or minimal), but this model does not carry out desirable identification and integrity levels. Finally, hybrid methods are a trade-off combination which can provide a balance between the degree of interaction and security requirements. In Fig. 1 it has been marked those elements which are involved in the model proposed. In the following sections, the secure e-assessment model is presented.

3.3 Technological Approaches

According to [4] problems encountered in ensuring modern computing systems cannot be solved with technology alone. In order to probe this statement and to justify that it is needed to extend technological models with trustworthiness functional proposals, in this section, we are going to present a use case that illustrate how Public Key Infrastructure (PKI) does not completely guarantee security requirements. The example use case is defined as follows:

The e-assessment is an e-exam with most common characteristics of virtual exams. For further information, in [8] it is discussed how unethical conduct during e-Learning exam taking may occur and it is proposed an approach that suggests practical solutions based on technological and biometrics user authentication.

The e-exam is synchronous and students have to access the LMS to take the description of the e-exam at the same time. The exam, which presents a list of tasks to be solved by the student. The statement is the same for all students who perform the e-exam and then, each student performs her work into a digital document with her own resources. When the student's work is finished, outcomes are delivered to the LMS before the deadline required.

Once defined this use case, we can improve security requirements using PKI based solutions, in concrete terms, digital certificates to guarantee students' identification and digital signature for outcomes integrity and authorship. Therefore, the process described above is adapted to this way:

- The student accesses the LMS identified by its digital certificate. Similarly, the LMS presents its digital certificate to the student.
- Since both LMS and student have been identified in a trust process, the student receives the description of the e-exam and begins her work.
- The student checks the built-in digital signature statement in order to validate the integrity of this element.
- When the student finishes her work in the outcomes document, the student performs the operation of digital signature (into the digital document and using her digital certificate).
- Eventually, the student's signed document will be delivered in the LMS, according to the procedure defined in the first step.

At this point we can formulate the question: can we trust this model? In other words, are those processes and elements involved in the e-exam bearing integrity and identification properties? As stated at the beginning of this section, ensuring modern computing systems cannot be solved with technology alone. Therefore, we should be able to find vulnerabilities in this technological security proposal. For instance, although the identification process based on the certificate public key (even signed and issued by a certification authority) is only able to be made by the holder of the private key (the student), we do not know if this certificate is being used by the student who we expect or if the student has sent this resource to another one. Although we can add additional technological measures such as certificate storage devices, there are ways to export these keys or have remote access to manage them. Therefore, we can conclude that the student may share their resources identification and signature.

4 Trustworthiness Approaches for Secure e-Assessment

In the previous section we discussed that security improvements in e-assessments cannot be reached with technology alone. To fill this drawback that impedes e-assessments to deploy their potential, we review in this section trustworthiness approaches to design secure e-assessment.

4.1 Trustworthiness and Security Related Work

In [22] it is discussed that security is both a feeling and a reality. The author points out that the reality of security is mathematical based on the probability of different risks and the effectiveness of different countermeasures. In addition, security is a feeling based not on probabilities and mathematical calculations, but on our psychological reactions to both risks and countermeasures. Since this model considers two dimensions in security and being aware that absolute security does not exist (see Section 3.3) any gain in security always involves a trade-off between technological and functional approaches. This approach is very relevant in the context of hybrid evaluation systems in which technological and trustworthiness solutions can be combined. This trade-off is proposed because, as it is concluded by the author, we need both to be and to feel secure.

Our approach providing security to e-assessments extends technological solutions and combines these services with trustworthiness models. In this context, it is also important to consider additional trustworthiness related work, even when the scope of trustworthiness models is not closely related to security in e-Learning. Next, we continue our related work study taking general trustworthiness references.

4.2 Trustworthiness Factors

Beyond the overview of security and trustworthiness presented, we need to review how trustworthiness can be measured and which are the factors involved in its quantitative study. In [3] a data provenance trust model is proposed, which takes into account factors that may affect the trustworthiness. Based on these factors, the model assigns trust scores to both data and data providers.

In our context, students and students' resources (e.g. a document, a post in a forum, etc.) can be modelled following this approach. Moreover, factors that may affect trustworthiness when students are developing collaborative learning activities must be discovered. To this end in [1], the author designs a survey to explore interpersonal trust in work groups identifying trust-building behaviours ranked in order of importance. We use these behaviours as trustworthiness factors which can measure trustworthiness in those activities that students develop in collaborative activities. The factors considered to model trustworthiness when students are performing collaborative activities are summarized in Table 1.

4.3 Trustworthiness Rules and Characteristics

Trustworthiness levels may be represented as a combination of trustworthiness factors. Moreover, according to [9] there are different aspects of consideration of trust and different expressions and classifications of trust characteristics. In essence, we can summarize these aspects defining the following rules: (i) Asymmetry, A trust B is not equal to B trust A; (ii) Time factor, trustworthiness is dynamic and may evolve over the time; (iii) Limited transitivity, if A trusts C who trusts B then A will also trust B, but with the transition goes on, trust will not absolutely reliable; (iv) Context sensitive, when context changes, trust relationship might change too.

Table 1 Trustworthiness Factors

N	Factors and Description
	Trustworthiness Building Factors (TBF) Student *S* working in the group of students *GS* is building trustworthiness when...
1	S communicates honestly, without distorting any information.
2	S shows confidence in GS's abilities.
3	S keeps promises and commitments.
4	S listens to and values what GS say, even though S might not agree.
5	S cooperates with GS and looks for mutual help.
	Trustworthiness Reducing Factors (TRF) Student *S* working in the group of students *GS* is reducing trustworthiness when...
1	S acts more concerned about own welfare than anything else.
2	S sends mixed messages so that GS never know where S stands.
3	S avoids taking responsibility.
4	S jumps to conclusions without checking the facts first.
5	S makes excuses or blames others when things do not work out.

The model presented in this paper is designed taking into account factors and rules which have been presented in this section. Furthermore, we define two additional concepts (trustworthiness levels and indicators) which are presented in the following sections.

4.4 Evidences and Signs

Trustworthiness factors are defined from the perspective of students' behaviours and, on the other hand, technological solutions cannot solve security requirements alone; in consequence, it is necessary to note that all methods discussed provide security improvements but do not completely ensure e-assessments requirements. Furthermore, neither trustworthiness nor PKI models define or manage the actions to take when the security service detects either anomalous situations or violation of the properties we have defined. Firstly we must consider that according to this fact we have to distinguish between evidences and signs. Evidence is defined as information generated by the security system in a reliable way and the evidence allows us to state that a certain security property has been violated. For example, if a process of electronic signature is wrong, we can state that the signed document does not meet the integrity property and this is an irrefutable fact regarding to mathematical properties of public and private keys involved in digital signature. On the other hand, signs allow us to assign a trustworthiness level to a system action or result. These levels are based on probabilities and mathematical calculations, in other words, potential anomalous situations are associated with probabilities.

For each type of anomalous situations detected (i.e. evidences and signs) it is necessary to define different measures. Measures which can be taken are presented below:

– Active. We act directly on the e-assessments processes. For instance, if a evidence is detected, the security service will deny access to the student and the student cannot continue with the next tasks.
– Passive. Analysis and audit. Focused on analysing the information provided by the security system without acting on the e-assessment. They may generate further actions, but the process continues as planned before the fault detection.

5 A Trustworthiness Model

In this section, we propose a trustworthiness model for security based on the previous elements and issues. Firstly, we identify those instruments and tools which will collect trustworthiness data. Then, a statistical analysis based on a model of trustworthiness levels is presented.

5.1 Research Instruments and Data Gathering

Four research instruments are considered to collect users' data for trustworthiness purposes and feed our model:

– Ratings. Qualifications of objects in relation to assessments, that is, objects which can be rated or qualified by students in the LMS.
– Questionnaires. Instruments which allow us to both collect trustworthiness students' information and to discover general aspects design in our model.
– Students' reports. Assessment instrument containing questions and ratings performed by the students and reviewed by the tutors.
– LMS usage indicators. To collect students' general activity in LMS (e.g. number of documents created).

All of these research instruments are quantitative and they have been designed to collect mainly trustworthiness levels and indicators as well as assessment information. In order to manage trustworthiness data, we define the concept of trustworthiness Data Source (DS) as those data generated by the research instrument that we use to define trustworthiness levels which are presented in the following section.

5.2 Modelling Trustworthiness Levels, Indicators and Rules

We introduce now the concept of trustworthiness indicator tw_i (with $i \in I$, where I is the set of trustworthiness indicators) as a measure of trustworthiness factors. Trustworthiness factors have been presented (see Section 4.2) as those behaviours that reduce or build trustworthiness in a collaborative group and they have been considered in the design of questionnaires. For instance, a trustworthiness indicator measuring the number of messages in a forum is related to the TBF-5 (the student cooperates and looks for mutual help). Therefore, an indicator tw_i is associated with one of the measures defined in each e-assessment instrument (i.e. ratings, questionnaires, reports, etc.). Moreover, we introduce the concept of trustworthiness level Ltw_i as a composition of indicators over trustworthiness rules and characteristics. For instance, we can consider two trustworthiness indicators (tw_a and tw_b). These indicators are different, the first indicator could be a rating in a forum post and the second one could be a question in a questionnaire; but they measure the same trustworthiness building factor (e.g. TBF-1: communicates honestly, described in Table 1). Finally, trustworthiness rules R, may be compared to the group, over the time or considering the context. Considering all the above, trustworthiness indicators can be represented following these expressions:

$$tw_{a_{r,s}}, a \in \{Q, RP, LGI\}, r \in R, s \in S \tag{1}$$

where Q is the set of responses in Questionnaires, RP is the analogous set in Reports, LGI is the set of LMS indicators for each student (i.e. ratings and the general students' data in the LMS). S is the set of students in the group and R is the set of rules and characteristics (e.g. time factor). These indicators are described above when presenting research instruments.

Once trustworthiness indicators have been selected, trustworthiness levels can be expressed as follows:

$$Ltw_i = \sum_{i=1}^{n} \frac{tw_i}{n}, i \in I \tag{2}$$

where I is the set of trustworthiness indicators which are combined in the trustworthiness level Ltw_i.

Trustworthiness levels Ltw_i must be normalized. To this end, we have reviewed the normalization approach defined in [21] with regarding to support those cases in which particular components need to be emphasized more than the others. Following this approach, we previously need to define the weights vectors:

$$w = (w_1, \ldots, w_i, \ldots, w_n), \sum_{i}^{n} w_i = 1 \tag{3}$$

where n is the total number of trustworthiness indicators and w_i is the weight assigned to tw_i. Then, we define trustworthiness normalized levels as:

$$Ltw_i^N = \sum_{i=1}^{n} \frac{(tw_i \cdot w_i)}{n}, i \in I \tag{4}$$

To sum up, our trustworthiness approach allows us to model students' trustworthiness as a combination of normalized indicators using research and data gathering instruments. Regarding groups, this model may also be applied in cases with only one working group; in this scenario, all students would belong to the same group.

5.3 Statistical Analysis

Following the trustworthiness model presented we need to inquire whether the variables involved in the model are correlated or not. With this purpose the correlation coefficient may be useful. Some authors have proposed several methods with regarding to rates of similarity, correlation or dependence between two variables [20]. Even though the scope of [20] is focused on user-based collaborative filtering and user-to-user similarity, the models and measures of the correlations between two items applied in this context are fully applicable in our scope. More precisely, we propose Pearson correlation coefficient (represented by the letter r) as a suitable measure devoted to conduct our trustworthiness model. Pearson coefficient applied to a target trustworthiness indicator is defined bellow:

$$r_{a,b} = \frac{\sum_{i=1}^{n}\left(tw_{a,i} - \overline{tw}_a\right)\left(tw_{b,i} - \overline{tw}_b\right)}{\sqrt{\sum_{i=1}^{n}\left(tw_{a,i} - \overline{tw}_n\right)^2}.\sqrt{\sum_{i=1}^{n}\left(tw_{b,i} - \overline{tw}_b\right)^2}} \qquad (5)$$

where tw_a is the target trustworthiness indicator, tw_b is the second trustworthiness indicator in which tw_a is compared (i.e. similarity, correlation, anomalous behaviour, etc.), $\overline{tw}_a$ and $\overline{tw}_b$ are the average of the trustworthiness indicators and n is the number of student's provided data for tw_a and tw_b indicators.

It is important to note that if both a and b are trustworthiness indicators which have several values over the time (e.g. a question which appears in each questionnaire), they must be compared at the same point of time. In other words, it is implicit that $r_{a,b}$ is actually representing r_{a_t,b_t} where a_t is the trustworthiness indicator in time t.

In addition, this test may be applied to every trustworthiness indicator taking one of them as target indicator. To this end, we define the general Pearson coefficient applied to a target trustworthiness indicator over the whole set of indicators is defined as follows:

$$r_{a,t} = \left(r_{a,1}, \ldots, r_{a,i}, \ldots, r_{a,n-1}\right), i \in I, i \neq a \qquad (6)$$

where $r_{a,i}$ is the Pearson coefficient applied to a target trustworthiness indicator is defined above and I is the set of trustworthiness indicators.

Both relation and similarity are represented by $r_{a,b}$ and r_A grouping students' responses and taking the variables at the same time. We are also interested in time factor and it may be relevant the evolution of trustworthiness indicators throughout the course. To this end, we extend previous measures, adding time factor variable:

$$r_{a,t,tt} = \frac{\sum_{i=1}^{n}\left(tw_{a_{t,i}} - \overline{tw}_{a_t}\right)\left(tw_{a_{tt,i}} - \overline{tw}_{a_{tt}}\right)}{\sqrt{\sum_{i=1}^{n}\left(tw_{a_{t,i}} - \overline{tw}_{a_t}\right)^2}.\sqrt{\sum_{i=1}^{n}\left(tw_{a_{tt,i}} - \overline{tw}_{a_{tt}}\right)^2}} \qquad (7)$$

where t is the target point in time and tt is the reference point in time (i.e. t is compared against tt), all other variables have already been defined with this case they are instanced in two moments in the course.

Similarly, we can calculate $r_{a,t,tt}$ for each tt, and then the following indicator may be used:

$$r_{a,t} = \left(r_{a,1}, \ldots, r_{a,i}, \ldots, r_{a,n-1}\right), i \in I, i \neq a \qquad (8)$$

Trustworthiness indicators which have already been presented in this section are summarized in Table 2.

Since hybrid methods are considered as a suitable trade-off approach for the model, we can combine these indicators with results of manual continuous evaluation results made by the tutor. For instance, a coefficient applied to target trustworthiness indicator a is compared to a manual continuous evaluation, that is:

$$r_{a,b} = cv_t \qquad (9)$$

Table 2 Trustworthiness Basic Indicators

Indicators	Description	Group by	Target/Reference
$r_{(a,b)}$	Pearson coefficient applied to a target trustworthiness indicator.	Students	tw_a and tw_b
r_a	$r_{(a,b)}$ over the set of indicators	Indicators	tw_a
$r_{(a,t,tt)}$	Pearson coefficient applied to a tw indicator throughout the course from t to tt	Time	tw_a and t
$r_{(a,t)}$	$r_{(a,t,tt)}$ over the throughout the course.	Course	tw_a

where the second indicator b is exchanged by the value in continuous evaluation. According to this indicator, we can analyse the similarity between manuals and automatics results. Furthermore, each Pearson interpretation which has been presented until now, may be applied to continuous evaluations parameters, for instance: $r_(a, t, tt)$ where $a = cv_t$.

On the other hand, as aforementioned in the case of questionnaires, some questions, which evaluate the same trustworthiness factor, are proposed in two different ways: individual and group evaluation. Hence, students are asked about some factors related to every member in her work group and then about the group in general. In this case, we can also compare these values using Pearson correlation. Finally, trustworthiness indicators may be gathered in a trustworthiness matrix with the aim of representing the whole relationship table for each indicator:

$$R_{tw} = \begin{pmatrix} 0 & r_{tw_1,tw_2} & \cdots & \cdots & r_{tw_1,tw_n} \\ 0 & 0 & r_{tw_2,tw_3} & \cdots & r_{tw_2,tw_n} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & r_{tw_{n-1},tw_n} \\ 0 & 0 & \cdots & \cdots & 0 \end{pmatrix} \quad (10)$$

Indicators which have been presented in this section are studied in the analysis stage of the model. Although they are proposed as suitable options, the model is refined to select those indicators oriented to perform the best similarity and correlation evaluation model. In addition, this approach is also intended to be a prediction tool, that is, similarity facts may conduct to carry out predictions about the evaluation system and its evolution.

6 Analysis of Results and Evaluation

As discussed in the section 2 with respect to trustworthiness models and bearing in mind the abstract model presented in the section 5, there exist considerable variation regarding goals, contexts, and scopes in trustworthiness approaches. In this section, we conduct our evaluation method on peer-to-peer e-assessment developed in a real on-line course. Our peer-to-peer e-assessment model is based on a collaborative assessment component and, in this section, we also present the design and implementation of the component including research instruments and technological tools. Finally, we conclude the section with important issues concerning processing trustworthiness levels and indicators as well as statistical analysis and interpretation.

6.1 Real On-line Course Features

We have carried out several studies [15, 17, 18] in our real context of e-Learning of the UOC during the Spring academic term of 2014, with the aim to experiment with specific trustworthiness and security approaches devoted to evaluate the feasibility of our trustworthiness models, tools, and methodologies. In this paper, we build and deploy our comprehensive e-assessment methodology in the real on-line course presented in [15, 17, 18], whose key features can be summarized as follows:

- Students' e-assessment was based on a manual continuous e-assessment model by using several manual e-assessment instruments.
- Manual e-assessment was complemented with automatic methods, which represented up to 20 percent of the total students overall grade.
- Taking into account below features, we implemented a hybrid e-assessment method by combining manual and automatic e-assessment methods, and the model allows us to compare results in both cases.
- 59 students performed a subjective peer-to-peer e-assessment, that is, each student was able to assess the rest of class peers in terms of knowledge acquired and participation in the class assignments.
- The course followed seven stages which were taken as time references in trustworthiness analysis. These time references allow us to compare trustworthiness evolution as well as to carry out e-assessment methods.
- Each stage corresponded to a module of the course, which had a learning component (i.e. book) that the student should have studied before developing the assessment activities of the course.

From the above methodology, we have designed the peer-to-peer e-assessment component which is presented in the next section.

6.2 Continuous Assessment Component

As aforementioned in Section 3.1, we used a subset of security properties for e-assessment security modelling, hence integrity and identification were selected as target security properties for the continuous assessment component. Following these security properties and after the analysis of potential students' interactions in peer-to-peer assessment activities as well as the peer-to-peer assessment possibilities, the first version of the continuous assessment component was proposed in [18, 17].

The Continuous Assessment (CA) component is formed by the following three assessment activities and procedures [18]:

1. Once the student has studied a module (M), she receives an invitation to answer a set of three questions about the current module; this is the first activity of the CA named the Module Questionnaire and denoted by Q.
2. The student does not have to answer as soon as Q is sent, because the second activity of the CA is a students' forum (F) intended to create a collaborative framework devoted to enhance responses in activity Q, in other words, Q and F activities are concurrent tasks.
3. The final activity is the core of the peer-to-peer assessment and the student has to complete a survey (P) which contains the set of responses from Q. The

student has to assess each classmates' responses in Q and, furthermore, the activity of each student in the forum F is assessed. The scale used to assess both forum participation and students' responses is (A, B, C+, C-, D, and N for no answer).

The formulation of the algorithm corresponding to the e-assessment process of the CA was presented in [18] (see Alg. 1 and also [17]).

Algorithm 1 Algorithm for the e-assessment process [18]

```
Require: M {the list of modules} and S {the set of students in the course}
for m: M do
    Q_m ← create_questionnaire(m)
    send(Q_m, S)
    F_m ← create_forum(m)
    F(m) ← class_discussion(F_m, S)
    Q(m) ← getResponses(Q_m, S)
    P_m ← create_p2p_eval(Q(m), S)
    send(P_m)
    P(m) ← getResponses(P_m, S)
    e_assessment(m)[] ← results(Q, F, P, S)
end for
return e_assessment(m)[]
```

6.3 Research Instruments and Technological Tools

For the purpose of the CA implementation and deployment, a questionnaire creation function has been developed (i.e. create_questionnaire). Due to the output of the first questionnaire (see variable Q(m) in the algorithm) is the input to the peer-to-peer assessment activity (i.e. variable P_m), we can automate the assessment process for each CA. These function has been implemented as a Java class named *CreateP2P*, which includes the set of attributes and methods required to automatically generate the assessment activity P_m. The automation capabilities of the process are actually focused on the set of responses and the survey P_m manual customizations such as the text or the invitation messages.

The CA uses two survey web applications. The module questionnaire (Q) is implemented in Google Forms[3] and the peer-to-peer questionnaire (P) with LimeSurvey[4]. Due to the data exchange requirements between the two survey tools, we have selected the Coma Separate Values (CSV) format as the data exchange model. For this reason and with the aim of simplifying the implementation process we have integrated in our Java components the package Super CSV[5] which offers advanced CVS features dealing with reading and writing advanced operations on lists of strings.

We have selected LimeSurvey because a high configurable export and import survey functions based on standard formats are needed. After the evaluation of several survey formats, we have selected the CSV option. The function *create_p2p_eval*

[3] http://www.google.com/drive/apps.html
[4] http://www.limesurvey.org
[5] http://supercsv.sourceforge.net/index.html

has been implemented by the Java class *create_p2p_csv*, which receives a CSV responses file containing the set of responses collected by Google Forms and creates a LimeSurvey CVS survey format by converting the responses in questions for the new peer-to-peer questionnaire. The hosting support for LimeSurvey framework has been provided by the RDlab[6].

Moreover, because of the peer-to-peer and dynamic features of the questionnaire P, we need to extract assessment results in primitive and normalized e-assessment data format as presented in the following section. To this end, we have developed the Java class *Results*.

Finally, dealing with processing the Pearson correlation coefficient, we have used the statistical analysis program GNU PSPP[7].

6.4 Trustworthiness Data Sources, Levels and Indicators

Before the statistical analysis phase, we define trustworthiness data sources, indicators and levels in the context of our CA. We have defined a trustworthiness data source as those data generated by the CA that we use to define trustworthiness features presented in Section 4. Each CA (i.e. one CA per module) will manage four data sources. The first is related to the students' responses count and can be denoted with the following ordered tuple:

$$DS_{Q_C} = (M, Q, S, count) \tag{11}$$

where the questionnaire data source is defined as the total number of responses (*count*) that each student in S has answered in the questionnaire Q for the module M.

The second data source also refers to the students' responses and the DS offers each specific response:

$$DS_{Q_R} = (M, Q, S, res) \tag{12}$$

where the questionnaire data source DS_{Q_R} is defined as the response res (i.e. a student answers res to a question) that each student in S has responded regarding a specific question in Q in the module M.

The third data source refers to the participation degree in a forum. These data sources can be denoted with the following ordered tuple:

$$DS_F = (M, F, S, count) \tag{13}$$

where the forum data source DS_F is defined as the total number of posts (*count*) that each student in S has sent to a forum F regarding a specific question in Q in the module M.

Finally, we introduce a score data source as follows:

$$DS_R = (M, Q, S, SS, score) \tag{14}$$

where the responses data source denotes the score that a student (in S) has assessed a student's (in SS) response of a question in Q. Hence, S is the set of students who assess and SS is the set of students who are assessed by students in S. Although

[6] http://rdlab.lsi.upc.edu
[7] http://www.gnu.org/software/pspp/

S and SS may be considered as the same set of students in certain applications, they are actually considered as different sets because we permit participation in the second stage of the activity even when the student has not carried out the first one.

Tuples in DS_R are stored in a relational database table, namely MySQL[8].

Once trustworthiness data sources have been defined we define three trustworthiness levels. Following the model defined in Section 5.3, we first combine the trustworthiness indicators of each question in the module, and then the overall trustworthiness level for the student in a specific module is defined:

$$L_{R,m,s} = \sum_{i=1}^{n} \frac{(tw_i \cdot w_i)}{n}, i \in Q, w = (w_i = w_j), m \in M \tag{15}$$

where $L_{R,m,s}$ is the trustworthiness level for the student s in the module m measured by the trustworthiness indicator tw_i which considers the responses for each question in Q.

$$L_{F,m,s} = tw_{F,m}, m \in M \tag{16}$$

where $tw_{F,m}$ is the trustworthiness indicator for the responses in the collaborative forum F for the module m.

$$L_{m_i s} = \sum_{i=1}^{n} \frac{Ltw_i \cdot w_i}{n}, i \in \{L_{R,m}, L_{F,m}\}, w = (w_i = w_j), m \in M \tag{17}$$

where $L_{m_i s}$ is the overall trustworthiness level for the student s in the module m, calculated by combining the trustworthiness level for responses $L_{R,m,s}$ and the trustworthiness level for forum participation $L_{F,m,s}$.

6.5 Statistical Analysis and Interpretation

Here we analyse the trustworthiness levels and indicators presented in the previous section. The graph presented in Fig. 2 shows the overall $L_{R,m,s}$ for each student and for each module. It is worth mentioning that students who had not participated in any CA activity have been omitted. In this graph the $L_{R,m,s}$ level for each student has been accumulated by module, hence as shown in Fig. 2 those students who did not participate in all the activities proposed, they were considered in the study.

Regarding students' participation, we have monitored participation values (see Fig. 3) revealing a decrease of participation level after considering the following information:

- Q: Questionnaire participation.
- F: Total number of post in the forum.
- FP: Participation in the forum.
- P: Peer-to-peer survey participation.

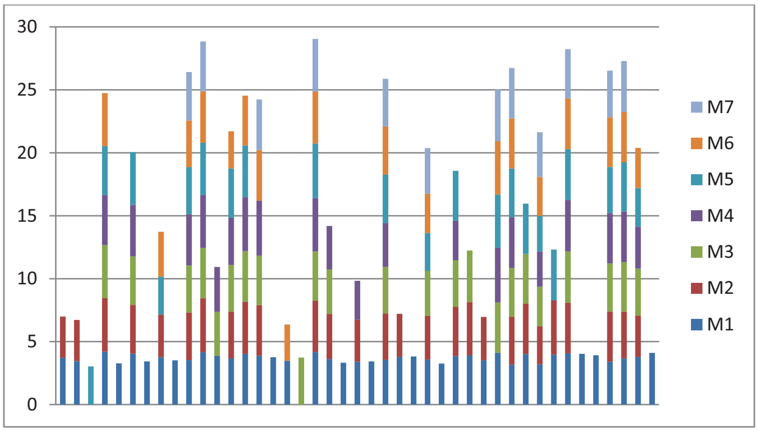

Fig. 2 $L_{R,m,s}$ level for each student and module

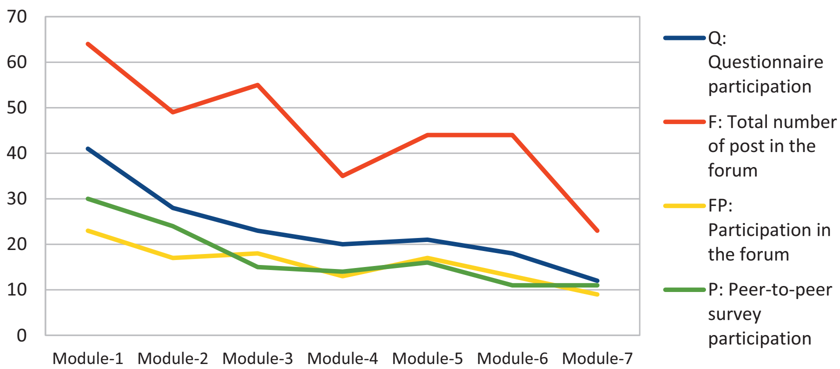

Fig. 3 Students' participation evolution

In contrast to the decrease in the participation level, with respect to the evolution of the overall scores in the course, these values are steady along all the modules in the course. The overall scores evolution are shown in Fig. 4, which presents the overall score result for each module activity, that is, $L_{R,m,s}$ and $L_{F,m,s}$ without considering each specific student's values and detailing each questions for $L_{R,m,s}$ (i.e. $Q1$, $Q2$ and $Q3$).

We have calculated the correlation coefficient between the values in the point of time 1 to 7 (i.e. each module). The results of the correlation analysis are shown in Fig. 5. Pearson's correlation is close to 1 for most of the cases, hence there is a strong relationship between trustworthiness levels in modules. The observed correlation is positive; consequently, when the trustworthiness level increases in module i, trustworthiness level in module $i+x$ also increases in value. The *sig.* value

[8] http://www.mysql.com/

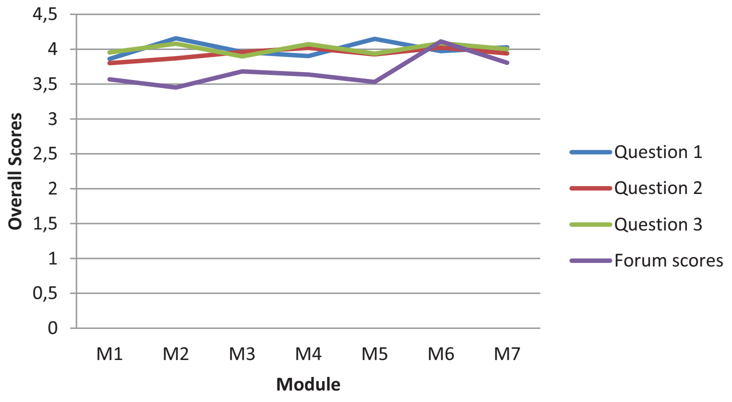

Fig. 4 Overall scores in the course

		M1	M2	M3	M4	M5	M6	M7
M1	**Pearson Correlation**	1,00	**,70**	,64	,54	,59	,54	,63
	Sig. (2-tailed)		,00	,00	,01	,01	,02	,03
	N	40	26	22	20	20	18	12
M2	**Pearson Correlation**	,70	1,00	**,89**	,81	,86	,81	,69
	Sig. (2-tailed)	,00		,00	,00	,00	,00	,02
	N	26	26	20	18	19	16	11
M3	**Pearson Correlation**	,64	,89	1,00	**,83**	,76	,80	,79
	Sig. (2-tailed)	,00	,00		,00	,00	,00	,00
	N	22	20	23	19	18	16	12
M4	**Pearson Correlation**	,54	,81	,83	1,00	**,78**	,76	,80
	Sig. (2-tailed)	,01	,00	,00		,00	,00	,00
	N	20	18	19	20	16	15	11
M5	**Pearson Correlation**	,59	,86	,76	,78	1,00	**,75**	,90
	Sig. (2-tailed)	,01	,00	,00	,00		,00	,00
	N	20	19	18	16	21	16	11
M6	**Pearson Correlation**	,54	,81	,80	,76	,75	1,00	**,86**
	Sig. (2-tailed)	,02	,00	,00	,00	,00		,00
	N	18	16	16	15	16	18	12
M7	**Pearson Correlation**	,63	,69	,79	,80	,90	,86	1,00
	Sig. (2-tailed)	,03	,02	,00	,00	,00	,00	
	N	12	11	12	11	11	12	12

Fig. 5 SPSS Pearson coefficient between trustworthiness levels in modules

is less than 0.05, because of this, hence we can conclude that there is a statistically significant correlation between trustworthiness levels. Note that in Fig. 5 we have marked those values which correspond to correlation between consecutive module (i.e. $r_{m_i,m_{i+1}}$), in these cases, the coefficient is always more than 0.7.

Finally, in order to compare manual an automatic assessment results, a foremost step is needed. We organized both manual and peer-to-peer activities in a timeline diagram with the aim to compare manual and automatic activities in suitable time references. To this end, we have designed a course plan that permits the comparison process between manual and peer-to-peer assessment. The manual assessment activities are taken as time reference.

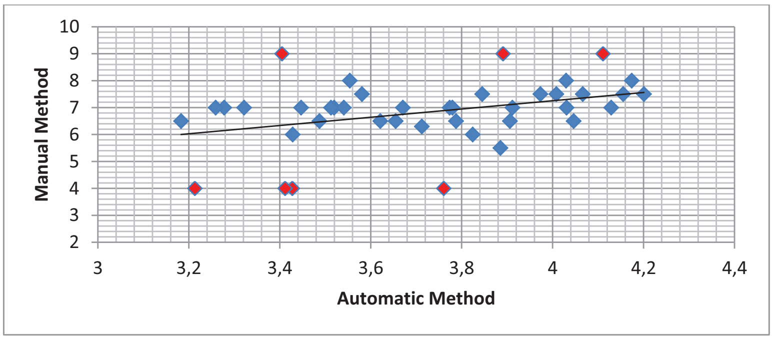

Fig. 6 Dispersion chart

Once the time references have been defined, we can compare overall values between manual and automatics method. For instance, Fig. 6 shows the dispersion chart between the automatic peer-to-peer activity for the module 1 (i.e. R_1) and the first manual assessment method. It can be seen from the function in Fig. 6 that there exist anomalous cases detected with respect to the difference between the manual and the automatic value. The rest of the values follow a significant relation between these parameters.

6.6 Findings

In this section we summarize the most relevant findings that emerge from the results and the statistical analysis.

The participation level has experimented a marked decrease along the course, especially at the end of e-assessment activities. We plan to tackle this problem with alternative course schedule with the aim to balance the students' peer-to-peer activities and other students' assignments.

Regarding overall peer-to-peer (i.e. automatic) and continuous (i.e. manual) assessment overall levels, the results reveal a notable difference between the overall range of these values. Fig. 6 shows that most of peer-to-peer assessment values are in the range from 3,5 to 4,3 (the e-assessment scale was from 1 to 5) and the continuous assessment, from 1 to 9.

Although the model has to be enhanced and we have to solve the aforementioned problems, the statistical analysis shows significant findings regarding the feasibility of the hybrid evaluation method. The results of the comparisons between manual and automatic assessment indicate (also see Fig. 6):

- The mean difference between manual and automatic method is 0,81 (the scale used from 0 to 10).
- The maximum and minimum difference: 0,03 and 2,82.
- The percentage of assessment cases in which the difference between manual and automatic assessment is less than 1 (i.e. 10% with respect the maximum score) is the 76,92%.
- If we extend the difference to more than 2 points in the scale, the percentage of assessment cases in this range is the 92,31%.

The most significant finding is related to anomalous user assessment. From these data, 3 students whose deviation is greater than 20% were found anomalous and required further investigation for potential cheating in order to validate the authenticity (i.e. identification and integrity) of her learning processes and results.

7 Conclusions and Further Work

In this paper we have presented an innovative approach for modelling trustworthiness in the context of secure learning assessment in on-line collaborative learning groups. The study shows the need to propose a hybrid assessment model which combines technological security solutions and functional trustworthiness measures. To this end, a holistic security model is designed, implemented and evaluated in a real context of e-Learning. This approach is based on trustworthiness factors, indicators and levels, which allow us to discover how trustworthiness evolves into the learning system.

As ongoing work, we plan to continue the methodology testing and evaluation by deploying e-assessment learning components in additional real on-line courses. Due to further deployments will require large amount of data analysis, we will continue investigating parallel processing methods to manage trustworthiness factors and indicators by improving the MapReduce [14] configuration strategies that would result in improvement of a parallel speed-up, such as customized size of partitions. Moreover, we plan to evaluate and test trustworthiness predictions methods. With respect to prediction, we would like to improve our approach in order to predict both trustworthiness students' behaviour and evaluation alerts such as anomalous results. To this end, we plan to evaluate neural networks and data mining models by designing a methodological approach to construct a trustworthiness normalized model. In addition, in our future work, we would like to improve our students' public profile model in real on-line courses.

Acknowledgements This research was partly funded by the Spanish Government through the following projects: TIN2011-27076-C03-02 "CO-PRIVACY"; CONSOLIDER INGENIO 2010 CSD2007-0 004 "ARES"; TIN2013-46181-C2-1-R "COMMAS" Computational Models and Methods for Massive Structured Data; and TIN2013-45303-P "ICT-FLAG" Enhancing ICT education through Formative assessment, Learning Analytics and Gamication.

References

1. Bernthal, P.: A survey of trust in the workplace. Executive summary, HR Benchmark Group, Pittsburg, PA (1997)
2. CSO Magazine, US Secret Service, Software Engineering Insistute CERT Program at Carnegie Mellon University, Deloitte: 2011 Cybersecurity Watch Survey. Tech. rep., CSO Magazine (2011)
3. Dai, C., Lin, D., Bertino, E., Kantarcioglu, M.: An Approach to Evaluate Data Trustworthiness Based on Data Provenance. In: W. Jonker, M. Petković (eds.) Secure Data Management, vol. 5159, pp. 82–98. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
4. Dark, M.J.: Information assurance and security ethics in complex systems: interdisciplinary perspectives. Information Science Reference, Hershey, PA (2011)
5. Demott, J.D., Sotirov, A., Long, J.: Gray Hat Hacking, Third Edition Reviews, 3 edn. McGraw-Hill Companies, New York (2011)

6. Eibl, C.J.: Discussion of Information Security in E-Learning. Ph.D. thesis, Universität Siegen, Siegen, Germany (2010). URL http://dokumentix.ub.uni-siegen.de/opus/volltexte/2010/444/pdf/eibl.pdf
7. Ferencz, S.K., Goldsmith, C.W.: Privacy issues in a virtual learning environment. In: Cause/Effect, A practitioner's journal about managing and using information resources on college and university campuses, vol. 21, pp. 5–11. Educause (1998). URL http://net.educause.edu/ir/library/html/cem/cem98/cem9812.html
8. Levy, Y., Ramim, M.: A Theoretical Approach For Biometrics Authentication of E-Exams. In: Chais Conference on Instructional Technologies Research. The Open University of Israel, Raanana, Israel (2006)
9. Liu, Y., Wu, Y.: A Survey on Trust and Trustworthy E-learning System. In: 2010 International Conference on Web Information Systems and Mining, pp. 118–122. IEEE (2010). DOI 10.1109/WISM.2010.62. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5662295
10. Miguel, J., Caballé, S., Prieto, J.: Providing Security to Computer-Supported Collaborative Learning Systems: An Overview. In: Fourth IEEE International Conference on Intelligent Networking and Collaborative Systems (INCOS 2012), pp. 97–104. IEEE Computer Society, Bucharest, Romania (2012). DOI 10.1109/iNCoS.2012.60
11. Miguel, J., Caballé, S., Prieto, J.: Security in Learning Management Systems: Designing collaborative learning activities in secure information systems. eLearning Papers. European Comission: elearningeuropa.info (2012). URL http://elearningeuropa.info/en/article/Security-in-Learning-Management-Systems%3A-Designing-Collaborative-Learning-Activities-in-Secure-Information-Systems?paper=116112
12. Miguel, J., Caballé, S., Prieto, J.: Information Security in Support for Mobile Collaborative Learning. In: The 7th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS-2013), pp. 379–384. IEEE Computer Society, Taichung, Taiwan (2013). DOI 10.1109/CISIS.2013.69
13. Miguel, J., Caballé, S., Prieto, J.: Providing Information Security to MOOC: Towards effective student authentication. In: 5-th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2013), pp. 289 – 292. IEEE Computer Society, Xian, China (2013). DOI 10.1109/INCoS.2013.52
14. Miguel, J., Caballé, S., Xhafa, F., Prieto, J.: A Massive Data Processing Approach for Effective Trustworthiness in Online Learning Groups. Concurrency and Computation: Practice and Experience (2014)
15. Miguel, J., Caballé, S., Xhafa, F., Prieto, J.: Security in Online Assessments: Towards an Effective Trustworthiness Approach to Support e-Learning Teams. In: 28th International Conference on Advanced Information Networking and Applications (AINA 2014), pp. 123–130. IEEE Computer Society, Victoria, Canada (2014). DOI 10.1109/AINA.2014.106. Best paper of AINA 2014
16. Miguel, J., Caballé, S., Xhafa, F., Prieto, J., Barolli, L.: A Collective Intelligence Approach for Building Student's Trustworthiness Profile in Online Learning. In: 2014 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2014). GUANGZHOU, P.R. China (2014)
17. Miguel, J., Caballé, S., Xhafa, F., Prieto, J., Barolli, L.: A Methodological Approach to Modelling Trustworthiness in Online Collaborative Learning. In: Fourth International Workshop on Adaptive Learning via Interactive, Collaborative and Emotional Approaches (ALICE 2014). Salerno, Italy (2014)
18. Miguel, J., Caballé, S., Xhafa, F., Prieto, J., Barolli, L.: Predicting Trustworthiness Behavior to Enhance Security in On-line Assessment. In: 2014 6th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2014). Salerno, Italy (2014)
19. Miguel, J., Caballé, S., Xhafa, F., Prieto, J., Barolli, L.: Towards a Normalized Trustworthiness Approach to Enhance Security in On-line Assessment. In: Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS 2014), pp. 147–154. IEEE Computer Society, Birmingham, UK (2014). DOI 10.1109/CISIS.2014.22
20. Mobasher, B., Burke, R., Bhaumik, R., Williams, C.: Toward Trustworthy Recommender Systems: An Analysis of Attack Models and Algorithm Robustness. ACM Trans. Internet Technol. (2007). DOI 10.1145/1278366.1278372. URL http://doi.acm.org/10.1145/1278366.1278372
21. Ray, I., Chakraborty, S.: A Vector Model of Trust for Developing Trustworthy Systems. In: D. Hutchison, T. Kanade, J. Kittler, J.M. Kleinberg, F. Mattern, J.C. Mitchell, M. Naor,

O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M.Y. Vardi, G. Weikum, P. Samarati, P. Ryan, D. Gollmann, R. Molva (eds.) Computer Security – ESORICS 2004, vol. 3193, pp. 260–275. Springer Berlin Heidelberg, Berlin, Heidelberg (2004)

22. Schneier, B.: The psychology of security. In: Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology, AFRICACRYPT'08, pp. 50–79. Springer-Verlag, Berlin, Heidelberg (2008)
23. Weippl, E.R.: Security in E-Learning. In: H. Bidgoli (ed.) Handbook of information security Vol. 1, Key concepts, infrastructure, standards and protocols., vol. 1. Wiley, Hoboken, NJ (2006)
24. Wu, Z., Ou, Y., Liu, Y.: A Taxonomy of Network and Computer Attacks Based on Responses. In: Information Technology, Computer Engineering and Management Sciences (ICM), 2011 International Conference on, vol. 1, pp. 26 –29 (2011)