
Miguel, J. [et al.] (2014) A collective intelligence approach for building student's trustworthiness profile in online learning. *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2014, 8-10 November 2014, Guangzhou, Xina: proceedings*. IEEE. Pp. 46-53. Doi: http://dx.doi.org/10.1109/3PGCIC.2014.132.

Miguel, J. [et al.] (2014) A collective intelligence approach for building student's trustworthiness profile in online learning. *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2014, 8-10 November 2014, Guangzhou, Xina: proceedings*. IEEE. Pp. 46-53. Doi: http://dx.doi.org/10.1109/3PGCIC.2014.132.

A Collective Intelligence Approach for Building Student's Trustworthiness Profile in Online Learning

Jorge Miguel*, Santi Caballé*, Fatos Xhafa*, Josep Prieto* and Leonard Barolli†
* Department of Computer Science, Multimedia, and Telecommunication
Open University of Catalonia
Barcelona, Spain
Email: jmmoneo, scaballe, fxhafa, jprieto@uoc.edu
† Department of Information and Communication Engineering
Fukuoka Institute of Technology
Fukuoka, Japan
Email: barolli@fit.ac.jp

***Abstract*—Information and communication technologies have been widely adopted in most of educational institutions to support e-Learning through different learning methodologies such as computer supported collaborative learning, which has become one of the most influencing learning paradigms. In this context, e-Learning stakeholders, are increasingly demanding new requirements, among them, information security is considered as a critical factor involved in on-line collaborative processes. Information security determines the accurate development of learning activities, especially when a group of students carries out on-line assessment, which conducts to grades or certificates; in these cases, IS is an essential issue that has to be considered. To date, even most advances security technological solutions have drawbacks that impede the development of overall security e-Learning frameworks. For this reason, this paper suggests enhancing technological security models with functional approaches, namely, we propose a functional security model based on trustworthiness and collective intelligence. Both of these topics are closely related to on-line collaborative learning and on-line assessment models. Therefore, the main goal of this paper is to discover 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 student's profile model, based on trustworthiness is proposed, and the main collective intelligence processes involved in the collaborative on-line assessments activities, are presented.**

***Keywords*—Information security, user profiling, trustworthiness, on-line assessment, collective intelligence.**

I. Introduction and Context

Information and Communication Technologies (ICT) have been widely adopted in most of educational institutions in order to support e-Learning through different learning methodologies, ICT approaches and design paradigms. Over the past decade, Computer Supported Collaborative Learning (CSCL) has become one of the most influencing learning paradigms devoted to improve teaching and learning with the help of modern ICT [1]. Among these institutions, our real context of the Open University of Catalonia[1] (UOC) develops online education based on collaborative learning activities. This institution is supporting the research work presented in this paper and its results are considered and included in other UOC's research projects, with the aim of enhancing e-Learning factors, such as e-assessment cost reduction and students scalability.

The context of this paper is an e-Learning system formed by collaborative activities developed in a LMS. The system has to provide security support to carry out these activities and to collect trustworthiness data generated by learning and collaboration processes. Following this institutional framework, distance universities are developing on-line assessment processes and activities, which conduct to grades, certificates and many types of evaluation models; Information Security (IS) is an essential issue that has to be considered. This paper is focused on the target on specific on-line collaborative activities, namely, on-line assessment (e-assessment) activities, which offer enormous opportunities to enhance the student's learning experience. To overcome technological security deficiencies, we have conducted research on enhancing technological security models with trustworthiness functional approaches such as a trustworthiness-based approach for the design of secure learning activities in on-line learning groups. In this context, we propose to endow our previous trustworthiness in e-assessment research with a Student's Trustworthiness Profile (TSP) approach based on collaborative activities, e-assessment activities, and collective intelligence processes. We address the profile design for trustworthiness assessment and prediction as well as for enhance security in e-assessment.

The paper is organized as follows. Section II presents a comprehensive review of the existing works and of our previous research on security in e-Learning, as well as technological and functional security approaches devoted to enhance security in e-Learning. We also discuss on complementary solutions to secure e-assessment based on collective intelligence and trustworthiness student's profiles. In Section III, we propose our students' profile model based on e-assessment, collective intelligence, on-line collaborative learning, and trustworthiness assessment and prediction; to this end, we discuss on key factors, processes and components involved in the design of a student's trustworthiness profile as well as the implementation issues that should be taken into account. Finally, Section IV concludes the paper highlighting the main findings and outlining ongoing and future work.

[1] http://www.uoc.edu

II. Background

In this section, we first review main works in the literature on security in e-Learning and how technological and functional security approaches can be applied to e-assessment with the aim of enhancing security in e-Learning. Then, we propose complementary solutions to secure e-assessment based on collective intelligence and trustworthiness students' profiles.

A. Information Security in e-Learning Justification

In order to support CSCL, e-Learning stakeholders (i.e. designers and managers, tutors and students) are increasingly demanding new requirements. Among these requirements, IS is a significant aspect involved in CSCL processes deployed in LMSs, which determines the accurate development of CSCL activities. However, according to [2], [3] CSCL services are usually designed and implemented without much consideration regarding security.

The lack of security in e-Learning is also supported by practical and real attacks in ICT. As a matter of fact, recent attack reports [4], [5] have demonstrated a significant amount of real-life security attacks experimented by organizations and educational institutions. The Cybersecurity Watch Survey [4] is a survey conducted by reputed companies and educational institutions. This report reveals 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). Since LMS are software packages, which integrate tools that support CSCL activities, technological vulnerabilities have to be considered. Moreover, other security reports [4], [5] have shown how web application servers and database management systems, which usually support LMS infrastructure, are deployed with security flaws. Dealing with more technological details related to LMSs, the Trustwave Global Security Report [5] is an informative and educational annual report on the latest security issues and trends. Finally, potential LMS attacks can be studied by analysing their specific security vulnerabilities, for instance, in Moodle Security Announcements [6], 49 serious vulnerabilities have been reported in 2013.

Regarding security in universities, the scope of Spanish universities security framework can be considered; the RedIRIS Computer Emergency Response Team is aimed to the early detection of security incidents affecting centers affiliated to RedIRIS. As stated in its 2012 security report [7], the total amount of incidents received was 10.028, and this value represents an increase of 74.15% compared to the previous year. In the same context, in [8], it is stated that only 17% of the Spanish universities have launched the application of the Spanish National Security Framework and only 18% of students use digital certificates. Although it might seem that these plans and initiatives are related to security in e-Learning, they are actually focused on secure e-Administration and management. In contrast, e-Learning security, which can determine these management processes, is not considered; for instance, a student is able to obtain a course certificate following advanced security techniques such as digital signature, but this security technique is not required when the student is performing e-assessment.

B. Technological and Functional Security Approaches

Nowadays, ICT solutions based on Public Key Infrastructure (PKI) models [9], are available to offer technological implementations of services which ensure the security issues that have been described and required in LMSs. PKI, simply defined, is an infrastructure that allows the creation of a trusted method for providing privacy, authentication, integrity, and non-repudiation in communications between two parties. Otherwise, one of the key strategies in IS is that security drawbacks cannot be solved with technology solutions alone [10]. To date, even most advances security technological solutions, such as Public Key Infrastructures (PKI), have drawbacks that impede the development of complete and overall technological security frameworks, even most advanced PKI solutions have vulnerabilities that impede the development of a highly secure framework.

Further technological security approaches, some authors [10], [11] have considered IS as a research topic beyond ICT. In [11] 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. On the other hand, security is also a feeling, based on psychological reactions to both risks and countermeasures. Since this model considers two dimensions in security and being aware that absolute security does not exist [10], it can be stated that any gain in security always involves a trade-off, for instance, a trade-off between the additional security and the cost of the guards; even as it is concluded in [11], all security is a trade-off. This approach is very relevant in the context of this research because it is based on a hybrid security system in which technological overall solutions have to be managed beyond ICT.

For these reasons, our proposal suggests to conduct research into enhancing technological security models by functional approaches. Among functional approaches, trustworthiness analysis, modelling, assessment and prediction methods are suitable in the context of CSCL. Trustworthiness can be considered as a suitable functional factor in CSCL because most of trustworthiness models are based on peer-to-peer interactions [12] and CSCL is closely related to students' interactions. Although, some trustworthiness methods have been proposed and investigated; these approaches have been little investigated in CSCL with the aim to enhance security properties. Therefore, we have investigated on security in CSCL by enhancing technological security solutions with trustworthiness, through experimenting methods, techniques and trustworthiness models, eventually arranged, in a trustworthiness methodology approach for collaborative e-Learning [13], [14], [15].

Further security applications based on trustworthiness, additional CSCL enhancements related to pedagogical factors can be considered. According to [16] the existence of trust reduces the perception of risk which in turn improves the behaviour in the interaction and willingness to engage in the interaction. In the context of CSCL, interactions between students are one of the most relevant factors in learning performance. Therefore, trustworthiness is directly related to CSCL and trustworthiness can enhance the performance of collaborative learning activities. In contrast, IS can encourage and endorse

trustworthiness, but IS does not directly enhance learning. Another significant difference between IS and trustworthiness, with respect to CSCL, is the dynamic nature of trustworthiness [17]. Students' behavior is dynamic and it evolves during the learning process. Whilst IS is static, regarding students behavior, trustworthiness also evolves and its assessment can be adapted along students' behavior changes.

C. Security in e-Assessment based on Trustworthiness

Most of trustworthiness models in the literature are related to business processes, network services and recommendation systems [18], [19], but the key concept of these works is interaction between agents, that is, the same target studied in CSCL; but in our context, considering students' interactions and trustworthiness between them.

According to [18] there is a degree of convergence on the definition of trustworthiness, which can be defined as follows: trustworthiness is a particular level of the subjective probability with which an agent assesses that another agent (or group of agents) will perform a particular action, before the agent can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects its own action.

Regarding trustworthiness and e-Learning, according to [19], a trustworthy e-Learning system is a learning system, which contains reliable serving peers and useful learning resources. From these definitions, it can be claimed that trustworthiness is closely related to both students' interactions and students' actions in CSCL. Moreover, it can be considered that trustworthiness models are focused on two different dimensions, that is, trustworthiness assessment and prediction. To establish the difference between trustworthiness assessment and prediction, in [20] it is stated that trust prediction, unlike trust assessment, deals with uncertainty as it aims to determine the trust value over a period in the future. A CSCL activity is a general concept that can involve very different cases, actors, processes, requirements and learning objectives in the complex context of e-Learning.

The context of the paper is specific CSCL activities, namely, on-line assessment (e-assessment). E-assessment processes offer enormous opportunities to enhance the student's learning experience, such as delivering on-demand tests, providing electronic marking and immediate feedback on tests [21]. In higher education, e-assessment is typically employed to deliver formative and summative tests to the students. An e-assessment is an e-exam with most common characteristics of virtual exams, which are reported on unethical conduct occurring during e-learning exam taking [22]. In our CSCL context, we have endowed e-assessment activities with trustworthiness assessment and prediction to enhance users' security requirements [23], [24].

To overcome security deficiencies discussed in this section, we have researched into enhancing technological security models with trustworthiness functional approaches [13], [14], [15]. In [13] a trustworthiness-based approach is proposed 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 [13], 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. In [14] 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. Finally, in [15] an approach to enhance IS 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.

D. Collective Intelligence

According to [25] although several definitions of collective intelligence have been proposed, a shared agreement suggests that collective intelligence is a group or shared intelligence that emerges from the collaboration and or competition of many entities, either human or digital. Previous research works [25], [26], [27] have demonstrated how the resulting information generated by models based on collective intelligence can be seen as reflecting the collective knowledge of a community of users and can be used for different purposes. In [26] it is presented a collaborative tagging system where users assign tags to resources and web entities. This article uses data from a social bookmarking site intended to examine the dynamics of collaborative tagging systems and to study how coherent categorization schemes emerge from unsupervised tagging; this information is shared with other users and the emerged community's knowledge, due to users' interaction. This example is a form of explicit collaboration, in contrast to this approach, in [27] the opposite model is presented and users' behaviour is implicitly gathered in order to form a base of knowledge useful for studying tendencies, trends and therefore to predict the most useful web resources. In this work, we can discover how collective intelligence is also related to a key objective of our research, namely, trustworthiness assessment and prediction in students' on-line collaborative learning following implicit and explicit models devoted to gather trustworthiness data.

The authors in [26] presented how university students explicitly evaluated the usefulness of several web sites, and their browsing activity were gathered. In this comprehensive analysis of collective intelligence, the authors concluded that the correlation indexes suggest the existence of a considerable relationship between explicit feedbacks and implicit computed judgements. This evidence supports the presentation of a schema for a collective intelligence application that generates implicit rankings by considering the collective intelligence emerged from users on the web. Furthermore, regarding our application in trustworthiness students' profile, we assume the feasibility of a hybrid approach based on implicit and explicit trustworthiness data gathering.

Collective intelligence, via information sharing among trusted agents, can be analysed from two different perspectives. On the one hand, social networking is globally expanding and

they lack of specifying and implementing appropriate security and privacy procedures to protect users' data [25]; therefore, technological IS solutions are needed in order to reach social networking privacy and security requirements. On the other hand, collective intelligence and social networking involves trustworthiness relationships between the agents in the system; hence, trustworthiness assessment and prediction can enhance security in collaborative frameworks.

E. Trustworthiness Student's Profiles

In an e-Learning system and following an approach based on collaborative intelligence, trustworthiness propagation is needed in order to support both e-assessment and collaborative learning activities, such as creating students' groups. As stated by the authors in [28], trust is considered as the crucial factor for agents in decision making to select the partners during their interaction in open distributed systems; in this paper a computational model which enables agents to calculate partners' trustworthiness degree is presented, as well as to support agents to judge the trustworthiness of the referee when it refers the trust of a partner from its referees, preventing agents from referring the reputation from liar agents. In our context, on-line collaborative learning requires, as a relevant activity, the creation of learning groups, and trustworthiness can support this process. Most of current trust models are the combination of experience trust and reference trust and make use of some propagation mechanism to enable agents to share his or her final trust with partners. These models are based on the assumption that all agents are reliable when they share their trust with others [28]. Therefore, among these mechanisms, students' profiles can be a suitable approach with the aim of supporting trustworthiness propagation in the e-Learning system.

Since we propose the design of a collective intelligence application (i.e. students' profile application), we have to review the main principles designing collective intelligence applications. In [29] the seven principles presented by O'Reilly [30] are adapted focusing the principles on the Collective Intelligence Application (CIA) requirements. This approach can be summarized as follows:

- Task specific representations. The CIA should support views of the task. Data is the key, that is, the CIA is data centric and should be designed to collect and share data among users.
- Users add value. The CIA should provide mechanisms for them to add, to modify, etc. with the aim of improving its usefulness.
- Facilitate data aggregation. The CIA should be designed such that data aggregation occurs naturally through regular use.
- Facilitate data access. The data in CIAs can be used beyond the boundaries of the application. The CIA should offer web services interfaces and other mechanisms to facilitate the re-use of data.
- Facilitate access for all devices. The CIA needs to be designed to integrate services across handheld devices and internet servers.
- The perpetual beta. The CIA is an ongoing service provided to its users, thus new features should be added on a regular basis based on the changing needs of the user community.

Regarding LMSs and students' profiles, although some LMSs include a service intended to support the management students' profiles, these services are not designed with the aim of managing either trustworthiness or collective intelligence data gathering. Without seeking to carry out an exhaustive LMSs analysis, we can select Moodle[2] as representative LMS system, which are being extensively adopted by educational organizations to help educators create effective online learning communities. The Moodle student's profile, as presented in the Moodle documentation Moodle Docs[3], allows a user to manage his or her own profile as follows:

- A student can see the course profiles of users.
- Course managers and administrators can access the full students' profile.
- Additional functions allow a manager to edit another user's profile details.
- A user views and manages his or her full profile.

Although Moodle users' profiles offer a basic set of operations, this functionality does not reach CIA requirements presented in this section. Even those related to collaborative learning activities cannot be developed using Moodle students' profiles. Despite this, Moodle offers additional modules devoted to enhance collaborative activities, for instance, Moodle badges are a suitable way of showing achievement and progress. As stated in Moodle Docs, badges are based on a variety of chosen criteria; they are fully compatible with other systems and can be displayed on a user's profile.

To sum up, LMSs such as Moodle offers collective intelligence tools and services related to students' profile, which can be taken as starting point, but they do not reach CIA requirements and cannot offer an overall technological solution to support a student's security profile model for on-line assessment based on trustworthiness and collective intelligence.

Finally, we have reviewed specific literature on students' profiles. In [31] it is presented an adaptive computer assisted assessment system that automatically scores the students and gives feedback to them according to their responses, that is, the questions are chosen according to the students' profile based on previous answers. Another interesting students' profile approach is presented in [32] by determining students' academic failure through building students' profiles founded on data mining methods. This profile approach is based on information extracted from on-line surveys filled out by the students and the data analysis is conducted by classification methods. Although both studies solve a specific goal related to on-line assessment applications (i.e. students' responses in surveys and previous answers in e-assessments) and the proposal is based on students' profiles, they are conducted by assessment components, which do not support collaboration and collective intelligence. To the best of our knowledge,

[2]https://moodle.org
[3]http://docs.moodle.org

these students' profiles approaches are specifically focused on concrete objectives, which cannot be extended to the scope of collective intelligence, trustworthiness and security in on-line assessment. Therefore, in the rest of the paper, we propose how to apply previous research presented in this section to student's profile with the aim of enhancing security in on-line assessment through trustworthiness and collective intelligence.

III. Building Students' Profiles in e-Assessment

In this section, we propose our students' profile model based on e-assessment, collective intelligence, on-line collaborative learning, and trustworthiness assessment and prediction.

A. Collective Intelligence in e-Assessment and CSCL

Collective intelligence principles have been presented in the background section as those requirements for designing collective intelligence applications; in this section, we adapt these principles to e-assessment in CSCL. To this end, we consider the peer-to-peer e-assessment component described in [23] as a Continuous Assessment (CA).

The CA is formed by three assessment activities: (i) The Questionnaire (Q). The student receives an invitation to answer a set of questions; (ii) The Forum (F). The student does not have to answer as soon as Q is sent, as the second activity is a students' forum (F) intended to create a collaborative framework devoted to enhance responses in Q; and (iii) The Peer-to-peer Survey (P), where the student has to complete a survey (P) which contains the set of responses from Q. The student has to assess each classmate's responses in Q and, furthermore, the activity of each student in the forum F is assessed by the students.

As can be seen from the CA description above, the assessment result emerges from the collaboration of many students who carry out collaborative learning activities and e-assessment processes. Collective intelligence principles are considered in CA design as follows:

- Task specific representations. The e-assessment activity supports multiple views of the task. The responses of the questions proposed are involved in each activity of the e-assessment. In the first activity, the question is the students' challenge; in the second one, a collaborative target; and finally every response is presented as result, which has to be assessed.
- Data is the key. We can consider that the students' responses are the collected and shared data among students. Moreover, since students assess the responses in Q, we can state that the students add value to both the system and the original data.
- Facilitate data aggregation. The activities Q and P are quite static, whereas the forum activity F is completely dynamic and open. Therefore, the forum activity allows students to carry out data aggregation.
- Facilitate data access. Mechanisms to facilitate the reuse of data are implemented in our CA model by developing an interface that automatically generates the activity P from data collected in activity Q (i.e. responses in Q, are the assessment target).
- Facilitate access for all devices. The CA does not require advanced technological systems or devices. The only requirement is a web browser and an internet connected device.
- The perpetual beta. The CA component is designed with the aim of being repeated several times in the course. For each iteration, the CA can be enhanced following decision information generated by the e-assessment processes (i.e. design cycles).

The CA activity offers e-assessment processes based on collective intelligence and on-line collaborative learning, but this model is an isolated e-Learning component due to each iteration does not remember or refer to previous history. In other words, when a student performs a certain peer-to-peer survey (P), he or she does not consider previous activity or past results of the student who is currently assessing. This drawback impedes the overall trustworthiness analysis in our model, therefore we propose a profile based approach. Moreover, the students assess individual and basic values (i.e. other students' responses) and they cannot assess overall students' trustworthiness information about their classmates.

B. Profiles based on Collective Intelligence

We address our profile-based approach to collaborative e-Learning knowledge and e-assessment analysis purposes; considering the collective intelligence emerged from the group of students is the students' profile. The student's profile collects, stores, and publishes trustworthiness student's information, such as the CA collaborative e-assessment results presented. Along these sections the main design decisions, rules, and features of the trustworthiness student's profile are presented and these issues are depicted in Fig. 1.

Following the process defined to the development of a CA activity, in order to incorporate students' profiles to the model, the CA activity design has to be modified in order to add such components and processes required to reach the following profile goals: (i) Collect trustworthiness students' information; (ii) Trustworthiness modeling and assessment; (iii) Store students' information in their persistent profiles; and (iv) Publish computed trustworthiness values. In the rest of this section, we detail these processes.

In our previous work [24], we have research on how trustworthiness data can be collected and modeled and we have proposed a methodological approach called trustworthiness and security methodology in CSCL (TSM-CSCL). The main concepts related to trustworthiness data collection are research instruments and data sources. Following the example of CA, we can considerer that the peer-to-peer survey is a research instrument which collects responses in Q and generates the scores for each students. Data sources allow us to define the format, source and input processes for each search instrument.

Once basic trustworthiness data have been collected, this source has to be processed in order to generate more complex and useful trustworthiness values. To this end, we define trustworthiness indicators and levels. The concept of trustworthiness level is a composition of indicators over trustworthiness rules and characteristics and a trustworthiness indicator is a measure of trustworthiness factors. Trustworthiness factors

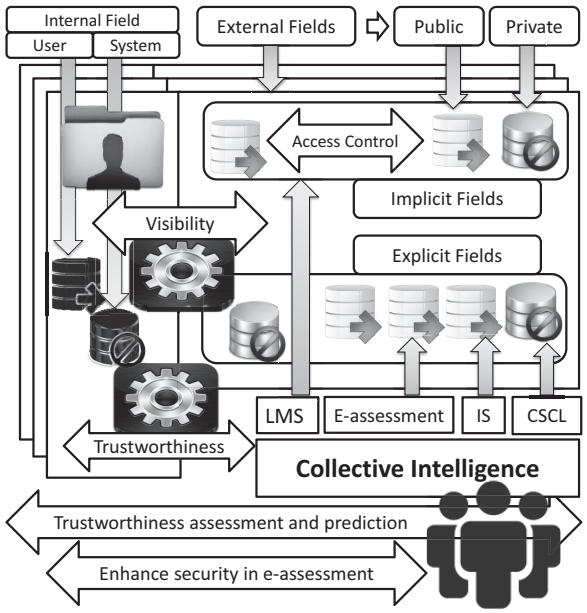

Fig. 1. Collective Intelligence for Trustworthiness Student's Profile

have been presented as those behaviours that reduce or build trustworthiness in a collaborative activity and they have been integrated in the design of research instruments [24].

A foremost step is needed before adding these data into the student's profile: the normalization process. This process consists in determining, selecting and applying those normalization functions that convert different formats and data sources into a unified measurement system. Then, the process of trustworthiness modelling and assessment is completed. The process of storing students' information in their persistent profiles may seem a simple task based on a classic file system or relational data base implementation, but the dynamic nature of trustworthiness converts this requirement in a challenge. If only trustworthiness levels are stored and basic data are removed, we lose basic data that could be needed in later trustworthiness assessment. Moreover, if we implement trustworthiness prediction processes, the previous basic and detailed data should be stored in order to compare and verify trustworthiness predictions. We propose a trade-off solution to tackle with the storage problem based on two layers (i.e. user layer and system layer) for trustworthiness data persistence.

The student's profile is formed by a set of trustworthiness levels and/or indicators, which can be directly assessed by a student. In addition, the internal layer contains internal system fields that the system requires to develop internal process such as control, validation, and further trustworthiness assessment. The set of trustworthiness indicators and levels must be carefully defined due to the potential limits in storage size and computational cost. In addition to control, processing and internal design requirements, the design based on two layers of trustworthiness levels has two major purposes related to students and tutors functional aspects. The first layer involves user fields and it is based on collective intelligence and on-line collaborative learning. The user layer provides a presentation layer devoted to publishing students' trustworthiness levels which are significant source information when the students are developing collaborative activities (e.g. the process of a learning group creation) and e-assessment processes (e.g. assessing the quality of a classmate's response in a questionnaire). The internal user layer covers fields for hybrid evaluation methods. We have proposed hybrid methods as a trade-off combination, which can provide a balance between the degree of interaction and security requirements regarding manual and automatic evaluation methods. This model requires additional information that cannot be published in the external student layer. For instance, whereas the trustworthiness history levels may be a private value in the students' context, tutors need to know and assess these values with the aim of comparing manual and automatic results.

Finally, the trustworthiness levels and indicators are published in the students' profiles. In this case, we have to consider two publication rules that we present in the next sections; namely, privacy and security rules related to the design of the profile and the LMS integration issues.

C. Technological Security Measures Fields

As was mentioned in the background section, technological and functional security approaches are closely related. With respect to the specific trustworthiness profile applications, these relations can involve particularly important issues due to the nature of students' assessment information. A foremost step is to define the visibility and access rules for students profile fields, mandatory data, optional data and private data that can only be accessible by special LMS users such as tutors. Due to the nature of e-assessment and trustworthiness data, information managed has to be published according to the laws, responsiveness, and the protection of privacy principles established for each educational institution. Moreover, students should decide if they prefer not to publish certain information. To this end, we propose a customizable control access module intended to offer a visibility students' profile configuration tool. This tool should be developed as an integrated module in the LMS.

We have also introduced that technological and functional solutions are complementary approaches and mutually dependent. Moreover, ICT security solutions are needed in order to reach social networking privacy and security requirements. For this reason, we propose including ICT security fields into the students' profiles. An ICT security field can be defined as the information, which represents the ICT security level that the student usually uses in the LMS. For instance, a low ICT security level could be a identification process based on classical login and password procedure, and a high ICT security level might be a student signing a message with a digital certificate (i.e. an advanced PKI solution).

D. Explicit and Implicit Trustworthiness Information

The development of the learning activity involves behavioural aspects that can be analysed in terms of explicit trustworthiness. For instance, when a student assesses a classmate's response or when a group of students are discussing a topic a forum, they are generating explicit trustworthiness information, that is, the development of the activity involves behavioural aspects that can be analysed in terms of trustworthiness. In addition to collaborative and e-assessment activities which

generate trustworthiness and collective intelligence information, there exists another sources that can be taken into account with the aim of defining profile fields. For instance, if a student spends much time reading discussions in collaborative documents, the LMS can monitor this action and this fact can be interpreted as trustworthiness building factor. We define these indicators as implicit trustworthiness fields in the profile as far as they are not directly related to trustworthiness factors and behaviours. Although implicit trustworthiness information could be processed automatically and presented in real time, it is important to note that we have to solve the processing limitations that can be derived from automatic and real time approaches. Firstly, the computational cost has to be considered and reduced in order to provide effective and just-in-time trustworthiness information from the LMS. It is required a continuous processing and analysis of students' activity during his or her learning processing, which produces huge amounts of valuable data stored typically in server log files. In previous research [13] we have studied the computational cost limitation with a parallel processing proposal, which can considerably decrease the time of data processing, thus allowing for building relevant trustworthiness models to support learning activities even in real-time.

Moreover, even if we endow or model with parallel processing, we have to overcome another type of limitations. We can assume that the model is suitable, the parallel processing reduce the computational cost and implicit trustworthiness information is automatically included and published in the student's profile, but this process does not ensure that implicit information is reliable. For instance, a student, who knows that the system is monitoring certain LMS use parameters, may fake the system with the help of a web injection software application. These applications applications allows a web administrator to automate the testing process of web applications and web services, in the same way, a student can simulate a real learning activity in the LMS. Since this vulnerability has to be solved, we propose to compare data from multiple sources. In [14] we have presented validation data based on Pearson correlation coefficient as a suitable measure devoted to conduct our trustworthiness model by comparing implicit and explicit trustworthiness fields. If validation tests do not meet the established thresholds, the implicit trustworthiness information will not be published in the student's profile.

E. Trustworthiness Student's Profile and Overall Services

So far, our student's trustworthiness profile can be summarized as TSP services, fields, and goals. Regarding TSP fields, the TSP is formed by a set of quantitative fields with the following features:

- The TSP fields design is based on two layers
- The TSP field can be implicit or an explicit field
- They are based on trustworthiness, e-assessment and collective intelligence
- A TSP may contain ICT security information.

With respect to TSP services, we have included three services intended to manage, maintain and monitor the TSP: data validation processes, access control and visibility students' tools. Dealing with data sources and those e-Learning activities devoted to collect students' information, we focus on collaborative activities, e-assessment activities, and collective intelligence processes. Finally, regarding the main goals of the TSP application we address the profile design to trustworthiness assessment and prediction and to enhance security in e-assessment.

At this point, TSP guidelines have been proposed, but we can endow our model with an overall further view. In particular, we can consider overall trustworthiness levels related to the group and the course. This approach may allow the course managers and tutors to assess and predict results regarding the overall learning process and with respect to the groups' activity.

IV. Conclusions and Further Work

In this paper, we first motivated the need to improve security in e-assessment based on security in e-Learning, technological and functional security approaches devoted to enhance security in e-Learning with the aim to discover complementary solutions to secure e-assessment based on collective intelligence and trustworthiness student's profiles. Then, a students' profile based on e-assessment, collective intelligence, CSCL, and trustworthiness assessment and prediction has been proposed.

As ongoing work, we plan to evaluate and test our students' profile model in real online courses. Due to these deployments will require large amount of data analysis, we will continue investigating parallel processing methods to manage trustworthiness factors and indicators.

Acknowledgment

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] T. Koschmann, "Paradigm Shifts and Instructional Technology," in *CSCL: Theory and Practice of an Emerging Paradigm*, T. Koschmann, Ed. Mahwah, New Jersey: Lawrence Erlbaum Associates, 1996, pp. 1–23. [Online]. Available: http://opensiuc.lib.siu.edu/meded_books/4

[2] E. R. Weippl, "Security in E-Learning," in *Handbook of information security Vol. 1, Key concepts, infrastructure, standards and protocols.*, H. Bidgoli, Ed. Hoboken, NJ: Wiley, 2006, vol. 1.

[3] C. J. Eibl, "Discussion of Information Security in E-Learning," Ph.D. dissertation, Universität Siegen, Siegen, Germany, 2010. [Online]. Available: http://dokumentix.ub.uni-siegen.de/opus/volltexte/2010/444/pdf/eibl.pdf

[4] CSO Magazine, US Secret Service, Software Engineering Insistute CERT Program at Carnegie Mellon University, and Deloitte, "2011 Cybersecurity Watch Survey," CSO Magazine, Tech. Rep., 2011.

[5] Trustwave, "Trustwave 2012 Global Security Report," Trustwave, Tech. Rep., 2012.

[6] Moodle, "Moodle Security Announcements," 2012. [Online]. Available: https://moodle.org/mod/forum/view.php?id=7128

[7] Equipo de Serguridad de RedIRIS, "Informe de incidentes de seguridad año 2012," Tech. Rep., 2013.

[8] S. Píriz, J. P. Gumbau, and T. Jiménez, "Universitic 2013: situación actual de las TIC en el sistema universitario español," in *Conferencia de Rectores de las Universidades Españolas (CRUE)*, 2013.

[9] K. Raina, *PKI security solutions for the Enterprise : solving HIPAA, E-Paper Act, and other compliance issues*. Indianapolis, Ind: Wiley Pub., 2003.

[10] M. J. Dark, *Information assurance and security ethics in complex systems: interdisciplinary perspectives*. Hershey, PA: Information Science Reference, 2011.

[11] B. Schneier, "The psychology of security," in *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology*, ser. AFRICACRYPT'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 50–79.

[12] S. P. Marsh, "Formalising Trust as a Computational Concept," Ph.D. dissertation, University of Stirling, 1994.

[13] J. Miguel, S. Caballé, F. Xhafa, and J. Prieto, "A Massive Data Processing Approach for Effective Trustworthiness in Online Learning Groups," *Concurrency and Computation: Practice and Experience*, 2014.

[14] ——, "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)*. Victoria, Canada: IEEE Computer Society, 2014, pp. 123–130.

[15] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, and L. Barolli, "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)*. Birmingham, UK: IEEE Computer Society, 2014, pp. 147–154.

[16] O. Hussain, E. Chang, F. Hussain, and T. Dillon, "Determining the Failure Level for Risk Analysis in an e-Commerce Interaction," in *Advances in Web Semantics I*, ser. Lecture Notes in Computer Science, T. Dillon, E. Chang, R. Meersman, and K. Sycara, Eds. Springer Berlin Heidelberg, 2009, vol. 4891, pp. 290–323. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-89784-2_12

[17] G. Carullo, A. Castiglione, G. Cattaneo, A. D. Santis, U. Fiore, and F. Palmieri, "FeelTrust: Providing Trustworthy Communications in Ubiquitous Mobile Environment," *2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)*, vol. 0, pp. 1113–1120, 2013.

[18] D. Gambetta, "Can We Trust Trust?" in *Trust: Making and Breaking Cooperative Relations*. Blackwell, 1988, p. 213–237.

[19] Y. Liu and Y. Wu, "A Survey on Trust and Trustworthy E-learning System," in *2010 International Conference on Web Information Systems and Mining*. IEEE, 2010, pp. 118–122. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5662295

[20] M. Raza, F. K. Hussain, and O. K. Hussain, "Neural Network-Based Approach for Predicting Trust Values Based on Non-uniform Input in Mobile Applications," *Comput. J.*, vol. 55, no. 3, p. 347–378, 2012. [Online]. Available: http://dx.doi.org/10.1093/comjnl/bxr104

[21] K. M. Apampa, "Presence verification for summative e-assessments," Ph.D. dissertation, University of Southampton, Southampton, England, 2010.

[22] Y. Levy and M. Ramim, "A Theoretical Approach For Biometrics Authentication of E-Exams," in *Chais Conference on Instructional Technologies Research*, The Open University of Israel, Raanana, Israel, 2006.

[23] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, and L. Barolli, "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.

[24] ——, "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.

[25] M. Mazzara, L. Biselli, P. P. Greco, N. Dragoni, A. Marraffa, N. Qamar, and S. d. Nicola, "Social Networks and Collective Intelligence: A Return to the Agora," *CoRR*, vol. abs/1311.2551, 2013.

[26] L. Longo, P. Dondio, and S. Barrett, "Enhancing Social Search: A Computational Collective Intelligence Model of Behavioural Traits, Trust and Time," in *Transactions on Computational Collective Intelligence II*, ser. Lecture Notes in Computer Science, N. Nguyen and R. Kowalczyk, Eds. Springer Berlin Heidelberg, 2010, vol. 6450, pp. 46–69. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-17155-0¡sub¿3¡/sub¿

[27] V. Robu, H. Halpin, and H. Shepherd, "Emergence of Consensus and Shared Vocabularies in Collaborative Tagging Systems," *ACM Trans. Web*, vol. 3, no. 4, pp. 14:1–14:34, Sep. 2009. [Online]. Available: http://0-doi.acm.org.cataleg.uoc.edu/10.1145/1594173.1594176

[28] M. Nguyen and D. Tran, "A Computational Trust Model with Trustworthiness against Liars in Multiagent Systems," in *Computational Collective Intelligence. Technologies and Applications*, ser. Lecture Notes in Computer Science, N.-T. Nguyen, K. Hoang, and P. Jdrzejowicz, Eds. Springer Berlin Heidelberg, vol. 7653, pp. 446–455. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-34630-9¡sub¿4¡/sub¿6

[29] D. G. Gregg, "Designing for Collective Intelligence," *Commun. ACM*, vol. 53, no. 4, pp. 134–138, Apr. 2010. [Online]. Available: http://doi.acm.org/10.1145/1721654.1721691

[30] T. O'Reilly, "What is Web 2.0: Design patterns and business models for the next generation of software," 2005. [Online]. Available: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

[31] D. Pérez-Marín, E. Alfonseca, and P. Rodríguez, "On the Dynamic Adaptation of Computer Assisted Assessment of Free-Text Answers," in *Adaptive Hypermedia and Adaptive Web-Based Systems*, ser. Lecture Notes in Computer Science, V. Wade, H. Ashman, and B. Smyth, Eds. Springer Berlin Heidelberg, vol. 4018, pp. 374–377. [Online]. Available: http://dx.doi.org/10.1007/11768012¡sub¿5¡/sub¿4

[32] V. Bresfelean, M. Bresfelean, N. Ghisoiu, and C.-A. Comes, "Determining students' academic failure profile founded on data mining methods," in *Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on*, Jun. 2008, pp. 317–322.