
Miguel, J. [et al.] (2015) A data visualization approach for trustworthiness in social networks for on-line learning. *IEEE 29th International Conference on Advanced Information Networking and Applications, Gwangju, South Korea, March 25-27, 2015: proceedings*. [S.l.]: IEEE, 2015. Pp. 490-497. Doi: http://dx.doi.org/10.1109/AINA.2015.226.

Miguel, J. [et al.] (2015) A data visualization approach for trustworthiness in social networks for on-line learning. *IEEE 29th International Conference on Advanced Information Networking and Applications, Gwangju, South Korea, March 25-27, 2015: proceedings*. [S.l.]: IEEE, 2015. Pp. 490-497. Doi: http://dx.doi.org/10.1109/AINA.2015.226.

A Data Visualization Approach for Trustworthiness in Social Networks for On-line Learning

Jorge Miguel*, Santi Caballé*, Fatos Xhafa† and Vaclav Snasel‡
* Department of Computer Science, Multimedia, and Telecommunication
Open University of Catalonia
Barcelona, Spain
Email: jmmoneo, scaballe@uoc.edu
† Department of Languages and Informatic Systems
Technical University of Catalonia
Barcelona, Spain
Email: fatos@lsi.upc.edu
‡ Faculty of Electrical Engineering and Computer Science
VSB-Technical University of Ostrava
Czech Republic
Email: vaclav.snasel@vsb.cz

***Abstract*—Up to now, the problem of ensuring collaborative activities in e-Learning against dishonest students' behaviour has been mainly tackled with technological security solutions. Over the last years, technological security solutions have evolved from isolated security approaches based on specific properties, such as privacy, to holistic models based on technological security comprehensive solutions, such as public key infrastructures, biometric models and multidisciplinary approaches from different research areas. Current technological security solutions are feasible in many e-Learning scenarios but on-line assessment involves certain requirements that usually bear specific security challenges related to e-Learning design. In this context, even the most advanced and comprehensive technological security solutions cannot cope with the whole scope of e-Learning vulnerabilities. To overcome these deficiencies, our previous research aimed at incorporating information security properties and services into on-line collaborative e-Learning by a functional approach based on trustworthiness assessment and prediction. In this paper, we present a peer-to-peer on-line assessment approach carried out in a real on-line course developed in our real e-Learning context of the Open University of Catalonia. The design presented in this paper is conducted by our trustworthiness security methodology with the aim of building peer-to-peer collaborative activities, which enhances security e-Learning requirements. Eventually, peer-to-peer visualizations methods are proposed to manage security e-Learning events, as well as on-line visualization through peer-to-peer tools, intended to analyse collaborative relationship.**

Keywords*—*Information security, trustworthiness, on-line assessment, computer-supported collaborative learning, peer-to-peer analysis.

I. Introduction and Context

Over the last decade, the need to ensure e-Learning activities has been supported with Information and Communication Technologies (ICT) solutions. Although technological solutions have been widely adopted to cope with security vulnerabilities in e-Learning, absolute ICT security does not exist [1]. Moreover, the lack of security in e-Learning is also supported by the study of practical and real attacks in ICT services [2], [3], [4], [5], [6], [7]. These studies demonstrate a significant amount of real-life security attacks experimented by organizations and educational institutions. For this reason, we have proposed to tackle security breaches with trustworthiness models as a functional requirement devoted to improving information security [8].

Among the e-Learning activities developed in most of educational institutions, e-assessment assignments are usually performed as an essential component of the course. If we are developing an e-assessment in an on-line university, the results of this activity will conduct to grades. Hence, the security requirements of the e-assessment process, is an essential factor in terms of security levels that must be reached. The context of this research is the e-Learning paradigm named Computer Supported Collaborative Learning (CSCL), which has become one of the most influencing learning paradigms devoted to improving teaching and learning with the help of modern information and communication technology [9]. Therefore, in this paper, we present a peer-to-peer on-line assessment approach carried out in a real on-line course based on collaborative e-Learning models, security analysis, and trustworthiness functional approaches. When a peer-to-peer e-assessment activity is performed in a real on-line course, the security events of the trustworthiness model have to be detected and analysed by the tutors. Hence, we propose peer-to-peer visualizations methods with the aim of managing security e-Learning events in the course, as well as, on-line visualization tools intended to assess collaborative relationships.

This paper is structured as follows. In Section II we review the main works in the literature on security in e-Learning, e-assessment, peer-to-peer assessment, security based on trustworthiness, and visualization of peer-to-peer models. Section III is concerned with the building processes of a peer-to-peer e-Assessment component through the application of a trustworthiness and security methodology. Then, in Section Section IV, we present the main guidelines to tackle the analysis of peer-to-peer models with visual tools. The paper ends with the conclusions and the ongoing work planed.

II. Background

In this section, we first review works in the literature on information security with the aim to justify the relevance of security in e-Learning. Then, the most relevant studies on peer-to-peer e-assessments and security based on trustworthiness are presented. Finally, we discuss existing studies related to analysis and visualization of peer-to-peer models.

A. Information Security in e-Learning Justification

Nowadays, ICT solutions are available to offer technological implementations of services, which ensure the security requirements in Learning Management Systems (LMS). Among these solutions, Public Key Infrastructure (PKI) models offer a suitable technological approaches devoted to security management [10]. PKI, simply defined, is an infrastructure that allows for the creation of a trusted method for providing privacy, authentication, integrity, and non-repudiation. Since 1999, PKI related standards and specifications are available [11] with the aim of building standards to support a pervasive security infrastructure for ICT services. Although PKI models have been widely adopted over the last decade [10], other authors remark that absolute security does not exist [1]. In this respect and taking into account only technological factors, we can state that if all general software has bugs, security software also has bugs [1]. Hence, absolute security does not exist and security requirements cannot be completely reached. Whereas the model is not completely reliable, the security solutions have to include additional facilities such as audit service and failure control in order to reduce the effects and negative consequences of security vulnerabilities.

The lack of security in e-Learning is also supported by the study of practical and real attacks in ICT services. As a matter of fact, recent attack reports [2], [3], [4], [5], [6], [7] demonstrate a significant amount of real-life security attacks experimented by organizations and educational institutions. The Trustwave Global Security Report [2] presents the key insights and recommendations based on the analysis of 691 data breach investigations and threat intelligence, from global security operations centres, telemetry from security technologies, and research. This report revels that the 96 percent of the applications scanned have one or more serious security vulnerabilities, as well as, the 71 percent of compromise victims did not detect breaches themselves. The Cyberthreat Defense Report [3] informs the IT security community through a rigorous survey of ICT security decision makers and practitioners across North America and Europe. This report reveals that over the 80% of respondents indicated that their organization's ICT environment was compromised 5 or fewer times in 2014. Furthermore, the 7% of respondents indicated that their organization was subject to 10 or more successful attacks over the year [3]. The 2014 Data Breach Investigations Report (DBIR) [4] is a incident report conducted by a security company with contributions from 50 organizations from around the world. The main goal of the study is related to describe the analysed incidents from the last 10 years by basic security patterns. Namely, the 92% of the 100,000 incidents can be described by 9 basic patterns). The report demonstrates how the number of security incidents have increased significantly over the last decade (see Fig. 1). The summary of the report reveals, as more significant results, that there were 1,367 confirmed data breaches in 63,437 security incidents for 95 distinct countries in 50 contributing organizations.

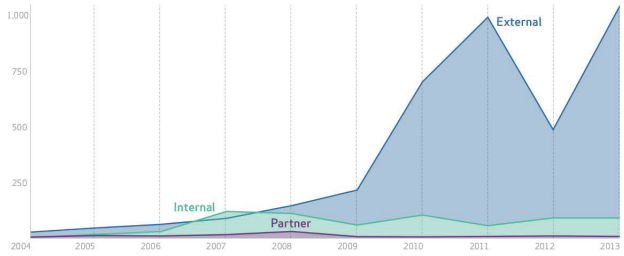

Fig. 1. Number of breaches per threat actor category over time [4]

Regarding security in universities, the scope of Spanish universities security framework can be considered in our context. The RedIRIS Computer Emergency Response Team (IRIS-CERT)[1] is aimed to the early detection of security incidents affecting centres affiliated to RedIRIS (i.e. the scientific community and Spanish universities). As stated in 2012 security report [6], 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 (i.e. Spanish universities), the report presented in [7] reveals that only 17% of the universities launched the application of the Spanish National Security Framework[2] and only 18% of the students actually use digital certificates. Although it might seem that these initiatives are related to improve security in e-Learning, they are actually focused on secure e-Administration. 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 on-line assessment activities [7].

To sum up and considering a global risk view, according to the Global Risks 2014 report [5], the escalation in large-scale cyber attacks and the breakdown of critical information infrastructure are prominent risks. For this reason, the reality of information security is a relevant global risk, which has to be considered in the e-Learning scenario.

B. Security in e-Assessment

In general, we can consider the e-assessment activity as an e-exam with most common characteristics of virtual exams. In [12] the authors discuss how unethical conduct during e-Learning exam taking may occur. The authors propose an approach that suggests practical solutions based on technological and biometrics user authentication.

From the general perspective of e-assessment, we concrete our research to the assessment model used in the Open University of Catalonia[3] (UOC) courses. Assessment models used in UOC may be classified in accordance with the following factors: (i) type of subjects; (ii) specific assessment model; (iii) assessment application; (iv) agents involved in the assessment processes [8]. In manual assessment methods, tutors have to

[1] http://www.rediris.es/cert/

[2] https://www.ccn-cert.cni.es/publico/seccion-ens/en/index.html

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

participate directly in the assessment process. This model has scalability problems but can provide better guarantees for students' security requirements. On the other hand, automatic methods reduce the tutors participation, but the model does not carry out desirable security levels. We focus our study on hybrid methods, which are a trade-off combination. The hybrid assessment model can provide a balance between the degree of interaction (between tutors and students) and security requirements [8], [13].

So far, we have analysed security requirements in e-assessment as a general concept, but these requirements have to be defined in terms of security services or properties. In [8], [13] we present a set of security properties whereby the secure e-assessment can be defined and managed by the e-Learning designers. These properties are summarized in the following list:

- Availability. The e-assessment is available to be performed by the student. After the assessment task, the tutor should be able to access the results.
- Integrity. The description of the e-assessment 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, the student's outcomes must correspond to the activity that the student actually 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 process.
- Non repudiation. The LMS must provide protection against false denial of involvement in e-assessments.
- Time stamping. The e-assessment components and data existed before a particular time.

In addition, we have to endow our security model with additional security properties [14]:

- Audit service. The LMS records the e-assessment process information needed to establish accountability for the activity events required by tutors.
- Failure control. The LMS must provide provide recovery of e-assessment processes and data when failures occur.

These security properties will reduce the effects and negative consequences of bugs or security vulnerabilities.

Due to the difficulty of provisioning all of these properties, our approach of secure e-assessments selects a subset of properties, which can be considered as critical requirements in evaluation context. The selected properties are identification and integrity. Integrity must be considered as authorship as well as data integrity. It is worth mentioning that integrity and identification are also selected because these properties are closely related to e-assessment specific functional features. If we are developing e-assessment in an on-line university, this activities will conduct to grades. Therefore, the integrity of the e-assessment process is a essential factor in terms of security requirements in the e-assessment process.

C. Peer-to-peer e-Assessment and Social Networks

In this section, we introduce the dimension of peer-to-peer e-assessment. Over the past decade, Computer Supported Collaborative Learning (CSCL) has become one of the most influencing learning paradigms devoted to improving teaching and learning with the help of modern information and communication technology [9]. Collaborative models are related to collective intelligence and social networks. According to [15] collective intelligence is a group or shared intelligence that emerges from the collaboration and or competition of many entities. Previous research works on collective intelligence [15], [16], [17] demonstrate how the resulting information generated by collaborative models can be seen as reflecting the collective knowledge of a community of users and can be used for different purposes.

In [16] it is presented a collaborative tagging system where users assign tags to resources and web entities. The authors use 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. In contrast to this approach of explicit collaboration, in [17] 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. From this perspective, we can discover how collective intelligence is also related to a key objective of our research, namely, peer-to-peer e-assessment following implicit and explicit models devoted to gathering collaborative data.

The authors in [16] 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 collaborative application that generates implicit rankings by considering the collective intelligence emerged from users on the web. Furthermore, regarding our application in peer-to-peer e-assessment, we assume the feasibility of a hybrid approach based on implicit and explicit collaborative data gathering.

D. Security and Trustworthiness in e-Assessment

As mentioned in Section II-A absolute technological security does not exist and security requirements cannot be completely reached. For this reason, we focus our research on functional security approaches. In [13] we justify the need of trustworthiness models as a functional requirement devoted to improving information security and a trustworthiness security methodology approach is presented. This methodology is a theoretical approach devoted to offering a guideline for designing and managing security in collaborative e-Learning

activities through trustworthiness assessment and prediction. The design of the methodology is defined in terms of cycles and phases, as well as, components, trustworthiness data and main processes involved in data management and design [13].

Most of trustworthiness models in the literature are related to business processes, network services and recommendation systems [18], [19]. Although our trustworthiness view is focused on information security, the key concept of these works is interaction between agents. The interaction processes are the same topic studied in CSCL, but in our context, we consider students' interactions and trustworthiness relationships between them.

According to [18] trustworthiness can be defined as a particular level of the subjective probability with which an agent assesses that another agent 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 a trustworthy e-Learning system is a learning system, which contains reliable serving peers and useful learning resources [20]. From these definitions, we can argue that trustworthiness is closely related to students' interactions in CSCL.

Finally, it is worth mentioning that most trustworthiness proposals takes into account the time factor as a key trustworthiness component in the model [20], [21]. The authors in [20] stated that trust is dynamic and will attenuate when time goes by. For instance, A trusts B at time t_0 , but A might not trust B in a follow-up time t_1. In our previous research we also considered the time factor and in [22] we endow previous trustworthiness models with prediction features by composing trustworthiness modelling and assessment, normalization methods, history sequences, and neural network-based approaches. In order to validate our approach.

E. Analysis and Visualization of Peer-to-peer Models

The topics discussed so far are addressed to improve peer-to-peer e-assessment security with trustworthiness models. This approach allow the e-Learning tutors to manage security events such as anomalous user identification. Although the security model is built, we actually need to incorporate an analysis and visualization peer-to-peer system into the security model with the aim of presenting and informing tutors regarding the trustworthiness peer-to-peer results.

In recent years, there has been an increasing amount of literature on complex networks. In [23] the authors review the major concepts and results recently achieved in the study of the structure and dynamics of complex networks, and summarize the relevant applications of these ideas in many different disciplines. On the one hand, scientists have to cope with structural issues, revealing the principles that are at the basis of real networks. On the other hand, many relevant questions arise when studying complex networks' dynamics, such as learning how the nodes interact through a complex topology can behave collectively [23]. In our context, we generate a network structure by designing a peer-to-peer e-assessment component and the behaviour of the students is analysed in terms of trustworthiness.

Regarding social networks visualization and network graphs, there exists several software that cope with complex analysis requirements in social networks. According to [24] there exist many network analysis and visualization software tools, which are available to collect, analyse, visualize, and generate insights from the collections of connections formed from billions of messages, links, posts, edits, uploaded photos and videos, reviews, and recommendations. Among them, NodeXL[4] is an open source software tool, especially designed to facilitate learning the concepts and methods of social network analysis with visualization as a key component [25].

According to [26], the analysis of social networks is especially concentrated on uncovering hidden relations and properties of network members. This paper introduces the application of known and proven methods of learning and forgetting into the field of social networks, through a network analysis based on the forgetting curve. The forgetting curve is defined in [23] as the probability that a person can recall information at time t since previous recall.

As stated by the authors in [26], a visualization of social network is a very important part of the whole systems network architecture. The visualization tool can quickly provide relevant insight into the network structure, its vertices and their properties. In the context of e-assessment, we can apply network analysis and visualization to assessment goals, such as anomalous students behaviour.

In [26], [27], the authors propose an on-line analysis tool called Forcoa.NET, which is focused on the analysis and visualization of the co-authorship relationship based on the intensity and topic of joint publications. The visualization of co-authorship networks allows for describing the author and her current surroundings, while still incorporating historical aspect. The analysis in Forcoa.NET is based on using the aforementioned forgetting function to hold the information relevant to the selected date. After this analysis, several measures can be computed with the aim of describing different aspects of user behaviour from the point of view of scientific social network.

III. Building a Peer-to-peer e-Assessment based on Trustworthiness

In this section, we present the main guidelines of the peer-to-peer e-assessment design process in a real on-line course.

A. Real On-line Course

We have carried out several studies [8], [13], [22], [28] in our real context of e-Learning of the UOC, with the aim to experiment with specific trustworthiness and security approaches devoted to evaluating the feasibility of our trustworthiness models, tools, and methodologies. In this paper, we address the visualization and analysts to the peer-to-peer e-assessment component presented in [8], [13]. This peer-to-peer component was performed in a real on-line course during the Spring academic term of 2014. The key features of the course can be summarized as follows:

[4]http://nodexl.codeplex.com

- 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 allowed 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 course features, we have designed the peer-to-peer e-assessment component which is presented in the next section.

B. Trustworthiness and Security Methodology

The e-assessment component for the on-line course was build following the Trustworthiness and Security Methodology (TSM) presented in [13]. TSM is a theoretical approach to offer a guideline for designing and managing security in collaborative e-Learning activities through trustworthiness assessment and prediction. Moreover, TSM supports all analysis, design, and management activities in the context of trustworthiness, as well as, collaborative learning activities, reaching security levels defined as a part of the methodology. In this paper we focus our research on peer-to-peer e-assessment as a specific case of on-line collaborative learning.

TSM is defined in terms of TSM cycles and phases, as well as, components, trustworthiness data and main processes involved in data management and design. We define a TSM phase as a set of processes, components, and data. TSM phases are sequentially arranged and the three main phases in TSM form a TSM design and deploy cycle. Each cycle corresponds to an interaction over the design process. Firstly, these concepts are presented as a methodological approach and then we complete the theoretical analysis with those methods and evaluation processes.

As presented in [13] TSM tackles the problem of security in CSCL through the following guidelines and main goals:

1) Define security properties and services required by e-Learning designers.
2) Build secure on-line collaborative activities and to design them in terms of trustworthiness.
3) Manage trustworthiness in learning systems with the aim of modelling, predicting and processing trustworthiness levels.
4) Detect security events, which can be defined as a condition that can violate a security property.

C. Building Peer-to-peer e-Assessment with TSM

The e-assessment component is formed by the following three assessment activities and procedures [22]:

1) Once the student has studied a module (M), the student receives an invitation to answer a set of three questions about the current module; this is the first activity of the e-assessment component 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 e-assessment is a students' forum F intended to create a collaborative framework devoted to enhancing responses in activity Q, in other words, Q and F activities are concurrent tasks. The forum activity is performed in LMS of the UOC named Virtual Campus.
3) The final activity is the core of the peer-to-peer assessment and the student has to complete a peer-to-peer assessment 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.

For the purpose of the e-assessment component implementation and deployment, we have used web survey services, export and import tools, parse applications, and data conversion developments. The e-assessment component is summarized in the rest of this section.

The module questionnaire Q is implemented in Google Forms[5]. Once the questionnaire Q has collected the students responses the output data are stored in Coma Separate Values (CSV) format. We selected this format because the two surveys applications involved in the e-assessment are compatible with this format. Due to the output of the first questionnaire Q is the input to the peer-to-peer assessment activity P a questionnaire creation function has been developed whereby we can automate the assessment process for each e-assessment component. When the questionnaire P is created in a text file, the questionnaire specification is loaded in the LimeSurvey[6] survey tool. After the evaluation of several survey tools, we have selected LimeSurvey because a high configurable export and import survey functions based on standard formats are needed. 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* which stores the results in a MySQL[7] relational database.

The overall process of building the assessment component is depicted in Fig. 2.

[5]http://www.google.com/drive/apps.html
[6]http://www.limesurvey.org
[7]http://mysql.org

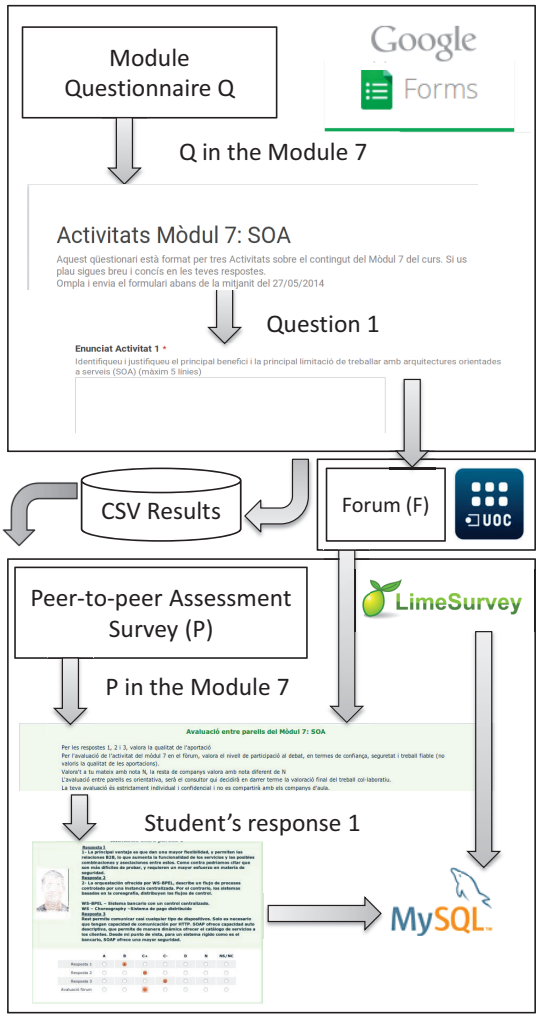

Fig. 2. The Process of Building the Peer-to-peer e-Assessment Component

D. Trustworthiness Data Processing

The peer-to-peer e-assessment in the questionnaire P produced a great amount of results. These data are stored in a relational MySQL data base as follows:

$$p2p = (M, Q, S, SS, score) \tag{1}$$

where $p2p$ denotes the score that a student has assessed a student's 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.

In order to respect the students' privacy and protect the e-assessment results, we created an additional table, which store a random integer value for each student. This random value is assigned to every student, hence the data stored for each $p2p$ tuple is not linked to the identity of the student. In other words, the students' assessment information remains anonymous when we export the students' results to external systems.

The peer-to-peer e-assessment responses maximum size is:

$$max\{p2p\} = |M| \times (|Q| + 1) \times |S| \times |S| \tag{2}$$

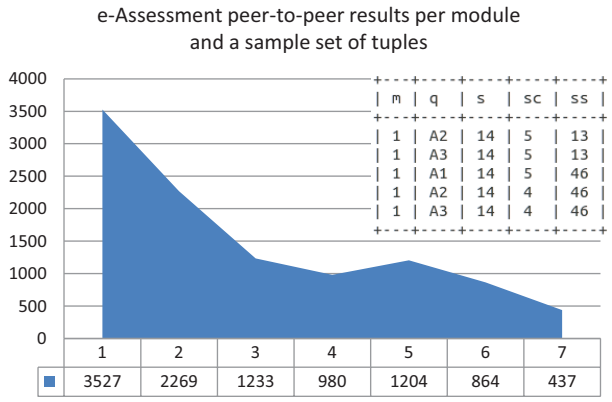

Fig. 3. Trustworthiness Data Processing Overall Results

where $|M|$ is the number of modules, $|Q|$ is the number of questions (+1 is added because the student assesses the forum activity and the questions in the questionnaire Q), and $|S|$ is the number of students who could participate in both questionnaires (i.e. Q and P).

The total number of computed tuples produced was:

$$|p2p| = 10.522 \tag{3}$$

Finally, Fig. 3 shows a sample set of data extracted from the $p2p$ e-assessment results and the number of results per module.

IV. Visualization and Analysis Tools of Peer-to-peer Models

In this section we present two suitable visualization and analysis tools for the case of peer-to-peer e-assessment based on trustworthiness.

A. e-Assessment Results Analysis with NodeXL

As presented in Section II-E, NodeXL is an open source software tool, especially designed to facilitate learning the concepts and methods of social network analysis with visualization as a key component [25]. NodeXL works with Microsoft Excel and it is managed as a blank NodeXL template which shows the usual Microsoft Excel appearance and functionalities.

The way we select to begin using NodeXL is to use the import command to load relationship data from an existing file or data source. Our data source is the CSV file containing all the data set of MySQL. Once data have been loaded into the template file, NodeXL offers several automatic layouts that can be selected from the control in the graph. The selected value used for our peer-to-peer e-assessment model in the layout type for NodeXL is called Fruchterman-Reingold [29]. The Fruchterman-Reingold layout is a force-directed layout algorithm, which treats edges like springs that move vertices closer or further from each other in an attempt to find an equilibrium that minimizes the *energy* of the system.

Although, in NodeXL the default graph type is undirected (i.e.the relationship between $student1$ and $student2$ is symmetric), we are considering a directed relation, which

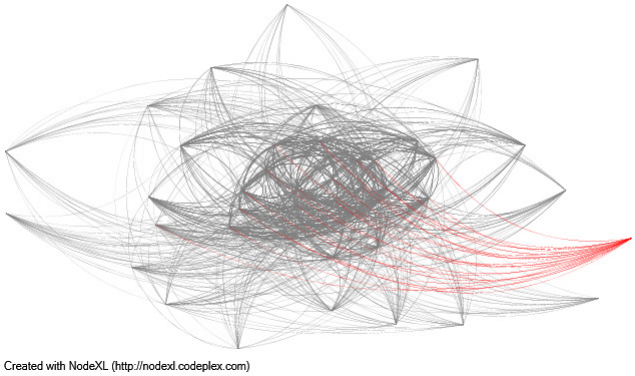

Fig. 4. The students' e-assessment relationships

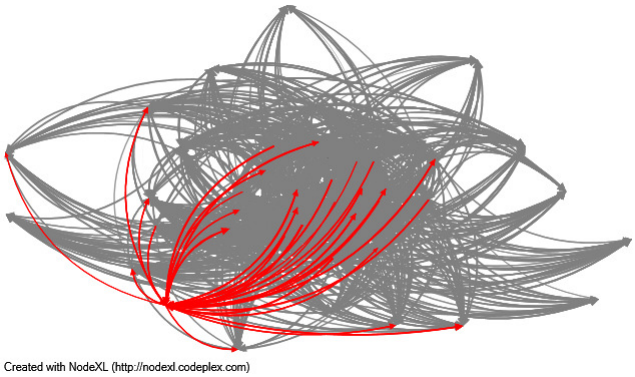

Fig. 5. Weighted students' e-assessment relationships

represent that $student1$ assess $student2$. As shown in Fig. 4, the tutor can select a student and the vertex for the students' e-assessment relationships are remarked. The remarked edges correspond to the assessment relation between a student in the peer-to-peer process, that is, those students who assessed the selected student and the students who were assessed by the selected student. We also have introduced the score value assessed by each student by using an edge weight column. For this reason, the score value is also represented as a edge weight in the graph (see Fig. 5). This type of column can be used to set visual properties of the edges and NodeXL uses automatic fill functions to set the edge width (see Fig. 5).

B. Forcoa.NET Overview

The Forcoa.NET system is built over the DBLP (Digital Bibliography & Library Project) dataset[8] from the field of computer science [27]. The design and development of the system was driven by the requirement for the visualization of co-authorship data. A key requirement was the need for the visualization of an author and the author's surroundings in the context of their publication activities, including a simple animation for the visualization of historical data [27].

In the context of the peer-to-peer e-assessment presented in Section III we can apply the Forcoa.NET system with the aim of visualize peer-to-peer assessment interactions between the students. The visualization capabilities with respect to historical data are also related to e-assessment processes, because trustworthiness (see Section II-D is closely related to time factor.

Moreover, time factor was included in the e-assessment component implementation when students assessed their classmates throughout the sequence of seven modules in the course. Therefore, Forcoa.net is a feasible visualization system for the peer-to-peer e-assessment component described in this paper.

C. e-Assessment Results as Forcoa.NET Input

Since the source format of Forcoa.NET was DBLP, we decided to adapt the e-assessment results to an compatible DBLP format. Whereas e-assessment students' results are stored in a relational database, we can export these data to a XML template following the model of DBLP dataset. The following schema allows us to extract the students' assessment information and to insert each value as a DBLP field:

```
<article key="p2p-assessment-q1_s1_s2_m3"
         mdate="2015-01-01">
 <author>student 1</author>
 <author>student 2</author>
 <title>p2p assessment question 1</title>
 <pages>null</pages>
 <year>3</year>
 <volume>null</volume>
 <journal>null</journal>
 <number>4</number>
 <ee>null</ee>
 <url>null</url>
</article>
```

Where the element *p2p-assessment-q1_s1_s2_m3* represents that *student 1* assessed *student 2* in *module 3*. The field title *p2p assessment question 1* is the assessed item (i.e. the question in the questionnaire Q) and the field number 4 is the score (i.e. scale of ratings) assigned by the *student 1*.

We evaluated several tools intended to convert a relational database tuples to a XML specific model. For the sake of simplicity, we directly export e-assessments results from MySQL.

```
SELECT
 CONCAT(
  '\n<article key="p2p-assessment-question-', q,
                  '_student-', s,
                  '_student-', ss,
                  '_mod-', m, '">\n',
      '<author>student ', s,  '</author>\n',
      '<author>student ', ss, '</author>\n',
      '<title>p2p assessment question ', q, '</title>\n',
      '<pages>null</pages>\n'
      '<year>', m,  '</year>\n',
      '<volume>null</volume>\n',
      '<journal>null</journal>\n',
      '<number>', sc, '</number>\n',
      '<ee>null</ee>\n',
      '<url>null</url>\n',
     '</article>\n'
 ) AS xmldoc
FROM scores_a;
```

Finally, those data generated by above SQL statement, are prepared and organized to import to Forcoa.NET on-line service.

[8] http://dblp.uni-trier.de/xml/

V. Conclusions and Further Work

In this paper, we first motivated the need to improve information security in peer-to-peer e-assessment. To this end, we justified the feasibility of an approach focused on trustworthiness. Since the peer-to-peer e-assessment has to be analysed and managed by tutors, we have proposed a trustworthiness data processing and visualization model based on two software visualization solutions.

As ongoing work, we plan to continue the testing and evaluation of these visualization tools and to enhance the visualizations capabilities for the tutors with additional facilities.

Acknowledgment

This research was partly funded by the following projects: TIN2013-45303-P "ICT-FLAG" Enhancing ICT education through Formative assessment, Learning Analytics and Gamification; and TIN2013-46181-C2-1-R, Computational Models and Methods for Massive Structured Data (COMMAS).

References

[1] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, *Firewalls and Internet security : repelling the wily hacker*. Boston: Addison-Wesley, 2003.

[2] Trustwave, "2014 Trustwave Global Security Report," Trustwave, Tech. Rep., 2014.

[3] CyberEdge Group, "2014 CyberThreat Defense Report," CyberEdge Group, Tech. Rep., 2014.

[4] Verizon, "2014 Data Breach Investigations Report," Verizon, Tech. Rep., 2014. [Online]. Available: http://www.verizonenterprise.com/DBIR/2014/

[5] World Economic Forum, *Global Risks 2014*, 9th ed. Geneva: WEF, 2014.

[6] Equipo de Serguridad de RedIRIS, "Informe de incidentes de seguridad año 2012," Red Académica y de Investigación Española (RedIRIS), Tech. Rep., 2013.

[7] 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.

[8] J. Miguel, S. Caballé, F. Xhafa, and J. Prieto, "Security in Online Web Learning Assessment. Providing an Effective Trustworthiness Approach to Support e-Learning Teams," *World Wide Web*, 2014.

[9] 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.

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

[11] IETF, "Public-Key Infrastructure (X.509) (pkix) - Documents," 2011. [Online]. Available: http://datatracker.ietf.org/wg/pkix/

[12] 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, pp. 93–101.

[13] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, and L. Barolli, "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: IEEE Computer Society, 2014, pp. 451–456.

[14] J. Miguel, S. Caballé, and J. Prieto, "Providing Security to Computer-Supported Collaborative Learning Systems: An Overview," in *Fourth IEEE International Conference on Intelligent Networking and Collaborative Systems (INCOS 2012)*. Bucharest, Romania: IEEE Computer Society, 2012, pp. 97–104.

[15] 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.

[16] 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¿

[17] 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

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

[19] F. Hussain, O. Hussain, and E. Chang, "Trustworthiness Measurement Methodology (TMM) for Assessment Purposes," in *Computational Cybernetics, 2007. ICCC 2007. IEEE International Conference on*, 2007, pp. 107–112.

[20] 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

[21] S. Msanjila and H. Afsarmanesh, "Automating Trust Assessment for Configuration of Temporary Partnerships," in *Innovation in Manufacturing Networks*, ser. IFIP – The International Federation for Information Processing, A. Azevedo, Ed. Springer US, 2008, vol. 266, pp. 95–104.

[22] 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: IEEE Computer Society, 2014, pp. 342–349.

[23] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex networks: Structure and dynamics," *Physics Reports*, vol. 424, no. 4–5, pp. 175 – 308, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S037015730500462X

[24] R. Ackland, D. L. Hansen, B. Shneiderman, and M. A. Smith, *Analyzing social media networks with NodeXL: insights from a connected world*. Amsterdam [u.a.: Elsevier, Morgan Kaufmann, 2011. [Online]. Available: http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10408229

[25] M. A. Smith, B. Shneiderman, N. Milic-Frayling, E. Mendes Rodrigues, V. Barash, C. Dunne, T. Capone, A. Perer, and E. Gleave, "Analyzing (Social Media) Networks with NodeXL," in *Proceedings of the Fourth International Conference on Communities and Technologies*, ser. C&T '09. New York, NY, USA: ACM, 2009, pp. 255–264. [Online]. Available: http://0-doi.acm.org.cataleg.uoc.edu/10.1145/1556460.1556497

[26] M. Kudelka, Z. Horak, V. Snasel, and A. Abraham, "Social Network Reduction Based on Stability," in *Computational Aspects of Social Networks (CASoN), 2010 International Conference on*, 2010, pp. 509–514.

[27] Z. Horak, M. Kudelka, V. Snasel, A. Abraham, and H. Rezankova, "Forcoa.NET: An interactive tool for exploring the significance of authorship networks in DBLP data," in *Computational Aspects of Social Networks (CASoN), 2011 International Conference on*, 2011, pp. 261–266.

[28] J. Miguel, S. Caballé, F. Xhafa, and J. Prieto, "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.

[29] T. M. J. Fruchterman and E. M. Reingold, "Graph drawing by force-directed placement," *Software: Practice and Experience*, vol. 21, no. 11, pp. 1129–1164, 1991. [Online]. Available: http://dx.doi.org/10.1002/spe.4380211102