UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

UPCommons

Portal del coneixement obert de la UPC

http://upcommons.upc.edu/e-prints

Miguel, J. [et al.] (2014) Predicting trustworthiness behavior to enhance security in on-line assessment. *2014 International Conference on Intelligent Networking and Collaborative Systems: IEEE INCoS 2014: 10–12 September 2014, University of Salerno, Salerno, Italy: proceedings.* [S.l.]: IEEE, 2014. Pp. 342-349 Doi: http://dx.doi.org/10.1109/INCoS.2014.19.

© 2014 IEEE. Es permet l'ús personal d'aquest material. S'ha de demanar permís a l'IEEE per a qualsevol altre ús, incloent la reimpressió/reedició amb fins publicitaris o promocionals, la creació de noves obres col·lectives per a la revenda o redistribució en servidors o llistes o la reutilització de parts d'aquest treball amb drets d'autor en altres treballs.

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Miguel, J. [et al.] (2014) Predicting trustworthiness behavior to enhance security in on-line assessment. *2014 International Conference on Intelligent Networking and Collaborative Systems: IEEE INCoS 2014: 10–12 September 2014, University of Salerno, Salerno, Italy: proceedings.* [S.l.]: IEEE, 2014. Pp. 342-349 Doi: http://dx.doi.org/10.1109/INCoS.2014.19.

(c) 2014 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other users, including reprinting/ republishing this material for advertising or promotional purposes, creating new collective works for resale or redistribution to servers or lists, or reuse of any copyrighted components of this work in other works.

Predicting Trustworthiness Behavior to Enhance Security in On-line Assessment

Jorge Miguel[1], Santi Caballé[1], Fatos Xhafa[1], Josep Prieto[1], Leonard Barolli[2]
Department of Computer Science, Multimedia, and Telecommunication
Open University of Catalonia
Barcelona, Spain
{jmmoneo, scaballe, fxhafa, jprieto}@uoc.edu
[2] Fukuoka Institute of Technology, Department of Information and Communication Engineering
Fukuoka, Japan
barolli@fit.ac.jp

Abstract— **Over the last decade, information security has been considered a key issue in e-Learning design. Although security requirements can be met with advanced technological approaches and these solutions offer feasible methods in many e-Learning scenarios, on-line assessment activities usually show specific issues that cannot be solved with technology alone. In addition, security vulnerabilities in on-line assessment impede the development of an overall model devoted to manage secure on-line assessment. In this paper, we propose an innovative approach to enhance technological security solutions with trustworthiness. To this end, we endow previous trustworthiness models with prediction features by composing trustworthiness modeling and assessment, normalization methods, history sequences, and neural network-based approaches. In order to validate our approach, we present a peer-to-peer on-line assessment model carried out in a real online course.**

Keywords- trustworthiness; e-assessment; security; neural network; collaborative filtering; collaborative learning.

I. INTRODUCTION

Information and Communication Technologies (ICT) have been widely adopted and exploited in most of educational institutions in order to support e-Learning through different learning methodologies, ICT solutions and design paradigms. In this context, e-Learning designers, managers, tutors, and students are increasingly demanding new requirements, among these requirements, information security is a significant factor involved in e-Learning processes. However, according to [1],[2], e-Learning services are usually designed and implemented without much consideration of security aspects. This finding and, in general the lack of security in e-Learning, has been tackled with ICT security solutions, but as stated in [3] the problems encountered in ensuring modern computing systems, cannot be solved with ICT alone. In contrast, current advanced ICT security solutions are feasible in many e-Learning scenarios though assessment processes in on-line collaborative learning involve specific components such as on-line assessment activities (e-assessment) that usually have specific issues such as student's grades or course certification that e-Learning designers have to consider when they manage security requirements. In this context, even most advanced and comprehensive technological security solutions cannot cope with the whole scope of e-Learning vulnerabilities.

An e-Learning activity is a general concept that can involve very different cases, actors, processes, requirements and learning objectives in the complex context of e-Learning. To conduct our research we focus our target on specific on-line collaborative activities, namely, on-line assessment (e-assessment). In [4] it is stated that the e-assessment process offers enormous opportunities to enhance the student's learning experience, such as delivering on-demand tests, providing electronic assessment and immediate feedback on tests. 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. For further information, in [5] it is discussed how unethical conduct during e-learning exam-taking may occur and it is proposed an approach that suggests practical solutions based on technological and biometrics user authentication.

In our context, we consider peer-to-peer assessment processes and on-line collaborative activities which will form e-assessment components. Therefore, to overcome these deficiencies, we have considered security technological solutions extended with a functional trustworthiness approach [6],[7],[8] by proposing a hybrid assessment method based on trustworthiness models. From these previous works, in this paper, we endow trustworthiness models for security in e-Learning with prediction methods, with the aim of managing reliable assessment processes in e-assessment. By predicting collaborative e-assessment results, e-Learning managers and designers will be able to manage assessment process with additional information generated by automatic prediction models.

The paper is organized as follows. Section II presents an overview of the existing works on security in e-assessment and how trustworthiness models are feasible methods to enhance e-assessment security requirements. To this end, we consider the literature on security for e-Learning, our previous research works on trustworthiness security models, and trustworthiness time factor approaches to analyze prediction techniques. In Section III, we conduct our research to peer-to-peer e-assessment, and trustworthiness sequences. Our peer-to-peer approach is carried out in a real online course in which we apply the concept of trustworthiness sequences customized for the peer-to-peer e-assessment. In Section IV, we endow our trustworthiness model with the prediction features by composing trustworthiness models, normalization methods, trustworthiness history sequences, and neural network-based approaches. Finally, Section V concludes the paper highlighting the main findings and outlining ongoing and future work.

II. BACKGROUND

In this section, we present an overview of the existing works on security in e-assessment, and how trustworthiness models are feasible methods to enhance e-assessment security requirements. We review main works in the literature on security for e-Learning and our previous research works on trustworthiness security models are summarized. Then, main works on trustworthiness time factor are presented in order to analyze prediction techniques.

A. Trustworthiness and Security for e-Assessment

Over the last decade, some authors have considered information security as a key issue in e-Learning design [2],[1]. Early research works about information security in e-Learning [9],[10] are focused on specific and isolated security properties such as privacy or identity. These security requirements are reached by designing methodological approaches and proposing technological solutions devoted to protect a subset of e-Learning vulnerabilities. Further works, have completed these approaches through more holistic models based on technological security solutions, such as Public Key Infrastructures (PKI), which is intended to cover the whole scope of e-Learning vulnerabilities [10]. Although PKI techniques and methods are feasible solutions in many e-Learning scenarios, e-assessment activities usually have specific factors that e-Learning designers have to consider when they manage security requirements. Among these factors, integrity and identity are key requirements, which, if violated by a malicious agent, the whole learning process will be compromised as well as the security e-assessment violation may cause further consequences, such as false academic certificates [6]. Some authors have argued that these security issues cannot be solved with technology solutions alone [3], and even most advanced PKI solutions have vulnerabilities that impede the development of a highly secure technological framework. The study presented in [11] also revealed that the need of trust cannot be achieved through technology alone, and a comprehensive solution would require complete knowledge about the way the e-assessment functions in a certain context.

To overcome these deficiencies, in our previous research [6],[7],[8], we have proposed a hybrid assessment method based on trustworthiness models. In [6] we proposed a trustworthiness model for the design of secure assessment in on-line collaborative learning groups by reviewing the main factors, classification and security issues involved in security in e-assessments. Furthermore, we completed this trustworthiness approach by proposing normalization enhances [8]. Furthermore, learners' trustworthiness analysis involves large amount of data generated along learning activities and processing this information is computationally costly, therefore, in [7] we proposed a parallel processing approach, which can considerably decrease the time of data processing, thus allowing for building relevant trustworthiness models to support learning activities even in real-time.

B. Trustworthiness General Models and Normalization

According to [12], there is a degree of convergence on the definition of trustworthiness. This can be summarized 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 [13], a trustworthy e-Learning system is a learning system, which contains reliable serving peers and useful learning resources.

As stated by the authors in [14], through the study of the most relevant existing trust models, trustworthiness modeling can be classified into trustworthiness assessment and prediction models (note that in the literature on trustworthiness modeling, the terms determination and estimation are also used to refer assessment and prediction respectively). To this end, we reviewed trust assessment models with the aim to build learners' trustworthiness profiles. The first formally trustworthiness model related to information technology services was proposed in [15] from three levels. This approach considers the main factors and rules dealing with trustworthiness, which can be summarized as follows: (i) Basic trust is the general trusting disposition of an agent at time; (ii) General trust represents the trust that agent has on other agent at time; (iii) Situational trust is the amount of trust taking into account a specific situation. It is worth mentioning that this early proposal takes into account the time factor as a key trustworthiness component in the model.

Although trustworthiness models can be defined and included as a service in e-assessment security frameworks, there are multiple issues related to trustworthiness, which cannot be managed without normalization [16]. Among these issues, we can highlight trustworthiness multiple sources, different data formats, measure techniques and other trustworthiness issues, such as rules, evolution, or context. Hence, in [8], we justify why trustworthiness normalization is needed and a normalized trustworthiness model is

proposed by reviewing existing normalization procedures for trustworthy values applied to e-assessments. Among these issues, time factor is considered in the next background sections from the point of view of both trustworthiness sequences and prediction.

C. Time Factor and Trustworthiness Sequences

Several studies investigating trustworthiness have shown that time factor is strongly related to trustworthiness [13], [17], [18]. The authors in [13] 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 [17], it is presented the design and development of a trust management system. This system addresses its specifications and architecture to facilitate the system implementation through a module-oriented architecture. Among the modules of the system, the authors define a module for dynamic assessment, which includes trust levels assessment based on dynamic trust criteria; the module integrates assessment from all parts to calculate trust value by the weighted average.

As described on the previous section, we can consider both assessment and prediction trustworthiness models. So far, although the models reviewed analyzing trustworthiness include as a key component the time factor, we need further modeling techniques that allow us to conduct trustworthiness assessment towards prediction. To this end, we reviewed the concept of Trustworthiness History Sequence [18]. In the context of grid services, Trustworthy History Sequence is a history record of trustworthy of grid service that the requester has traded with. It can be denoted with an ordered tuple where each component is the trustworthy of the transaction between requester and the service.

D. Predicting Trustworthiness

Trustworthiness predictions models, to the best of our knowledge, have been little investigated in the context of e-assessment, even in a general prediction scope. It has been suggested that, in the existing literature, the term trust prediction is used synonymously and interchangeably with the trust assessment process [14] presented in the sections above. Moreover, trustworthiness does not focus on an isolated technical application, but on the social context in which it is embedded. Although trustworthiness building can be supported by institutions, there is no easy way out [11], in addition, the building of trust can be a very lengthy process, the outcome of which is very hard to predict.

To establish the difference between assessment and prediction, in [14] it is stated that trustworthiness prediction, unlike trust assessment, deals with uncertainty as it aims to predict the trust value over a period in the future. In such cases, the accuracy of the trust values at a point in time in the future is an important issue to be considered, as the future of business decisions will be based on these.

Several studies investigating trustworthiness prediction have been carried out with neural networks [14],[18], [19]. In [14], the authors propose the use of neural networks to predict the trust values for any given entities. The neural networks are considered one of the most reliable methods for predicting values [14]. A neural network can capture any type of non-linear relationship between input and output data through iterative training, which produces better prediction accuracy in any domain such as time series prediction. The key contribution of this work is focused on the dynamic nature of trust, in which the performance of this approach is tested under four different types of data sets (e.g. non-uniform stationary data, different size, etc.), and the optimal configuration of the neural network is identified.

In [18], it is stated that prediction trustworthiness with the method of neural network is feasible, and the experiments presented in this work confirm that the methods with neural network are effective to predict trustworthy. This method is based on defining neural network structure, neural network constructing, input standardization, training sample constructing, and the procedure of predicting trustworthy with trained neural network.

The work presented in [19] proposes a novel application of neural network in evaluating multiple recommendations of various trust standards. This paper presents the design of a trust model to derive recommendation trust from heterogeneous agents. In this case, the experimental results show that the model has robust performance when there is high prediction accuracy requirement or when there are deceptive recommendations.

Moreover, other trustworthiness models have been proposed without neuronal networks methods [20],[21] such as similarity approaches. In [21] it is stated that predicting trust among the agents is of great importance to various open distributed settings such as peer-to-peer systems in that dishonest agents can easily join the system and achieve their goals by circumventing agreed rules, or gaining unfair advantages. These cases are closely related to e-assessment regarding anomalous assessment processes and integrity and identity security properties. In this work [21], it is proposed a trust prediction approach to capture dynamic behavior of the target agent by identifying features, which are capable of describing context of a transaction. The measurement of similarity between context of the potential transaction and that of previous transactions can predict trustworthiness of the potential transaction based on previous similar transactions outcomes. A further work [20] on users' ratings systems presents experimental results which demonstrate that ratings volume is positively associated with trust, as well as the congruence between one's own and others' opinions. The study also demonstrates that ratings source and volume interact to impact credibility perceptions, reliance on user-generated information, and opinion congruence. These results indicate important theoretical extensions by demonstrating that social information on-line may be filtered through signals indicating its veracity, which may not apply equally to all social media users.

III. Building Trustworthiness Sequences

As discussed in the previous section, there exists considerable variation regarding goals, contexts, and scopes in trustworthiness models. In this section, we conduct our research by two key topics, namely, peer-to-peer e-assessment, and trustworthiness sequences. We first present a peer-to-peer e-assessment model carried out on a real

online course, which is analyzed through defining trustworthiness levels and data normalization. Then, we apply the concept of trustworthiness sequences customized for the peer-to-peer e-assessment.

A. Peer-to-Peer E-Assessment Approach

The peer-to-peer e-assessment proposed is carried out on a real online course at the Open University of Catalonia[1]. This course has the following main features:

- Students' assessment is based on a continuous assessment model by using several manual assessment instruments. Manual assessment is completed with automatic methods, which can represent up to 20 percent of the total student's grade. Therefore, we are implementing a hybrid assessment method, which combines manual and automatics assessment methods, and the model allows us to compare results in both models.
- Number of students participating: 59 students performing a subjective peer-to-peer assessment, that is, each student can assess any student in the classroom following the assessment design.
- The course follows seven stages that can be taken as time references in order to validate and to analyze results. Each stage corresponds to a module of the course, which has a learning module (i.e. book) that the student must study before developing the assessment activities of the course.

From the above base course features, we have built the peer-to-peer e-assessment activity encapsulated as a Continuous Assessment (CA) which is formed by three assessment activities; the rest of this section describes the key design components of these activities.

Once the student has studied a module, he or she receives an invitation to answer (i.e. a short text response) a set of three questions about the current module; this is the first activity of the CA named the Module Questionnaire and denoted by Q. The student does not have to answer as soon as Q is sent, because the second activity of the CA is a students' forum (F) intended to create a collaborative framework devoted to enhance responses in activity Q, in other words, Q and F activities are concurrent tasks. The final activity is the core of the peer-to-peer assessment and the student has to complete a survey (P) which contains the set of responses from Q. The student has to assess each classmate's responses in Q and, furthermore, the activity of each student in the forum F is assessed. The scale used to assess both forum participation and students' responses is (A, B, C+, C-, D, and N for no answer). The formulation of the algorithm corresponding to the e-assessment process of the CA is shown in Fig. 1.

For the purpose of the CA implementation and deployment, a questionnaire creation function has been developed (i.e. *create_questionnaire*). Due to the output of the first questionnaire (see variable *Q(m)* in the algorithm) is the input to the peer-to-peer assessment activity (i.e. variable p_m), we can automate the assessment process for each CA. In the same way, to process the forum activity we have developed auxiliary tools (i.e. *questionnaire_count* and *forum_count*) intended to measure students' participation.

```
Input:
M: the list of modules
S: the set of students in the course
Begin e-assessment
  For (m: M) do
    Qm=create_questionnaire (m);
    send(Qm, S);
    Fm=create_forum(m);
    F(m)=class_discussion(Fm, S);
    Q(m)=getResponses(Qm, S);
    Pm=create_p2p_eval(Q(m), S);
    send(Pm);
    P(m)=getResponses(Pm, S);
    e-assessment(m)[]=results(Q,F,P,S);
  End for
End e-assessment
```

Figure 1. Algorithm for the e-assessment process.

The CA uses two survey web applications. The module questionnaire (Q) is implemented in Google Forms[2] and the peer-to-peer questionnaire (P) with LimeSurvey[3]. We have selected LimeSurvey because a high configurable export and import survey functions are needed based on standard formats. After the evaluation of several survey formats, we have selected the Coma Separate Values (CSV) option. The function *create_p2p_eval* has been implemented by the Java class *create_p2p_csv*, which receives a CSV responses file containing the set of responses collected by Google Forms and creates a LimeSurvey CVS survey format by converting the responses in questions for the new peer-to-peer questionnaire. The hosting support for LimeSurvey framework has been provided by the RDlab[4].

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*.

B. Normalizing Trustworthiness Data Sources

Once the peer-to-peer e-assessment has been designed, we analyze and define trustworthiness data sources and levels. In the context of CA, we define a trustworthiness data source as those data generated by the CA that we use to define trustworthiness levels as presented in [6],[7],[8]. Each CA (i.e. one CA per module) will manage two data sources, the first is related to the students' responses, and the second

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

[2] http://www.google.com/drive/apps.html

[3] http://www.limesurvey.org

[4] http://rdlab.lsi.upc.edu

refers to the participation degree in the forum. These data sources can be denoted with the following ordered tuples:

$$DS_{Qc} = (M, S, count)$$

where the questionnaire data source DS_{Qc} is defined as the total number of posts *count* that each student in *S* has sent to the forum regarding a specific question in *Q* in the module *M*.

$$DS_{Qr} = (M, S, Q, res)$$

where the questionnaire data source DS_{Qr} is defined as the response *res* that each student in *S* has responded regarding a specific question in *Q* in the module *M*.

$$DS_F = (M, Q, S, count)$$

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

$$DS_R = (M, Q, S, SS, score)$$

where the responses data source DS_R denotes the *score* that a student (in *S*) has assessed a student's (in *SS*) response of a question in *Q*, using the scale defined. Hence, *S* is the set of students who assess and *SS* is the set of students who are assessed by students in *S*. Although *S* and *SS* may be considered as the same set of students in certain applications, they are actually considered as different sets because we permit participation in the second stage of the activity even when the student has not carried out the first one. In other words, a student who has not participated in *Q* can assess his or her peers in *P*.

Note that all the tuples include the module in *M*, which will be used as a point in time references.

In this case, modeling trustworthiness involves multiple complex and heterogeneous data sources with different formatting, which cannot be managed without normalization.

According to the model presented in [8], we define a normalized trustworthiness indicator for the case of an CA as follow:

$$tw^N_{a_{q,m,s}} = N\left(tw_{a_{q,m,s}}\right)$$

$$a \in DS_{R,F,Qr,Qc}, q \in \mathrm{Q}, m \in M, s \in S$$

where $DS_{R,F,Qr,Qc}$ are the CA data sources, *S* is the set of students, *M* is the set of modules, and *Q* is the set of questions in each module.

Note that although in [8] we included four normalization functions, in this case, a subset is selected: N_2 and N_4.

Regarding the responses data source *R*, a student can assess every classmate's responses. To this end, we use the normalization function N_2:

$$N_2\left(tw_{R_{q,m,s}}\right) = \sum_{i=1}^{n} \frac{tw_{R_{q,m,i}}}{n-1}, \qquad \mathrm{i} \neq \mathrm{s}$$

where $tw_{a_{q,m,s}}$ is the responses indicator, *s* is the target student (i.e. the student who is assessed); *n* is the number of students in the course, and *q* is the one of the questions assessed in the module *m*.

It is worth mentioning that the scale for $tw_{R_{q,m,s}}$must be converted to integer values before normalizing with function N_2.

Similarity, forum participation also needs normalization. In this case, we apply the normalization function N_4:

$$N_4(tw_F) = \frac{tw_F}{T_F}$$

where T_F is the maximum number of post by an student in the forum.

C. Trustworthiness Levels and Sequences in e-Assessment

We have normalized forum and responses trustworthiness indicators. Then, trustworthiness levels [6] are defined in order to measure students' overall trustworthiness. To this end, we define the following trustworthiness levels:

$$L^N_I = \sum_{i=1}^{n} \frac{\left(tw^N_i * w_i\right)}{n}, i \in I, w = (w_1, \dots, w_i, \dots w_n), \sum_{i}^{n} w_i = 1$$

where n is the total number of trustworthiness indicators and w_i is the weight assigned to tw_i.

Following this model, we first combine the trustworthiness indicators of each question in the module, and then the overall trustworthiness level for the student in a specific module is defined:

$$L^N_{R,m,s} = \sum_{i=1}^{n} \frac{(tw^N_i * w_i)}{n}, i \in \mathrm{Q}, w = \left(w_i = w_j\right), m \in M$$

$$L^N_{F,m,s} = N_4(tw_F), m \in M$$

$$L^N_{m,s} = \sum_{i1}^{n} \frac{(Ltw^N_i * w_i)}{n}, i \in \{L^N_{F,m}, L^N_{R,m}\}, w = \left(w_i = w_j\right), m \in M$$

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

Once trustworthiness levels have been defined, we endow our model with time factor. Although this approach is based on the concept of Trustworthiness History Sequence presented in background section, we have to customize the model in order to manage trustworthiness levels in the context of e-assessment. Although the concept of

trustworthiness sequence has been defined in the context of grid services and requesters [18], it is feasible to apply this approach to another modeling scenario such as peer-to-peer e-assessment. The only requirement is time factor, in other words, the model should allow us to compute an overall trustworthiness level referred to multiple points of time. Therefore, we define CA trustworthiness history sequence CATS as the ordered list of a student's trustworthiness levels over several points in time:

$$CATS_s = (L^N_{m_1,s}, \dots, L^N_{m_i,s}, \dots, L^N_{m_q,s})\ i \in M, s \in S$$

where M is the set of modules, each module m_i refers to a point in time and $L^N_{m_i,s}$ is the overall trustworthiness level for the student s in the module m_i.

Likewise, we can define the overall students' CA trustworthiness history sequence as the matrix:

$$CATS = \begin{pmatrix} L^N_{m_1,s_1} & \cdots & L^N_{m_1,s_r} \\ \vdots & \ddots & \vdots \\ L^N_{m_q,s_1} & \cdots & L^N_{m_q,s_r} \end{pmatrix}$$

where q is the number of modules and points in time analyzed, and r is the number of students in the course.

D. Trustworthiness Sequences Results

Processing trustworthiness sequences results involves large amount of data generated by the peer-to-peer activity of the CA. To this end, we compute the following elements:

- The trustworthiness history sequence matrix has $r * q, r = |S|, q = |M|$ elements.
- For each element in $CATS$, $L^N_{m_i,s_j}$, we compute both forum and responses trustworthiness levels.
- Although forum participation is a single indicator, with respect to responses, there are three different questions.
- Moreover, for each trustworthiness levels we compute each student's score for the indicator.

With the aim of managing this trustworthiness sequences results, we have developed a parse java tool called *parse_tw_tuples* that converts peer-to-peer values into basic tuples presented above. This tool generates basic tuples from the web applications and these primitive records can be imported in a relational database for further processing. In order to deal with results we have to consider the size of the result set of records generated by each data source, at the end of the process the responses data source maximum size is:

$$|DS_R| = |M| \times (|Q| + 1) \times |S| \times |S|$$

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

The diagram depicted in Fig. 2 shows the overall process including how we have to normalize data sources, then, creating trustworthiness indicators and levels, and finally, the procedure presented to compose trustworthiness sequences.

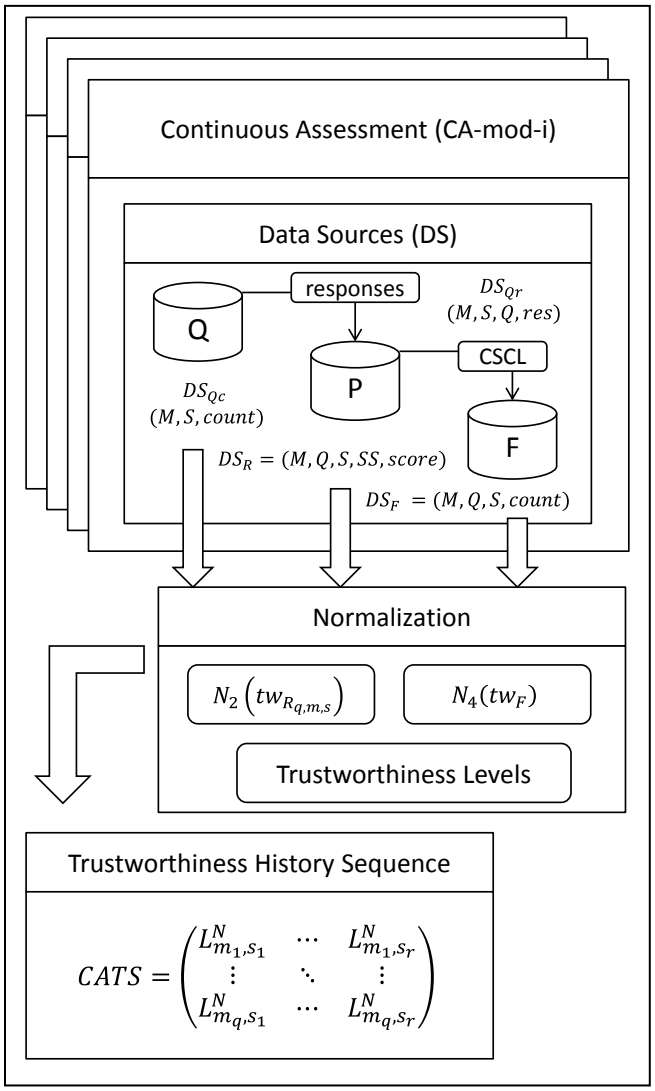

Figure 2. CA datasources, normalization and trustworthiness sequences.

IV. Predicting Trustworthy Behavior

In this section, we endow our trustworthiness model with the prediction features by composing: (i) trustworthiness models presented, (ii) normalization methods, (iii) trustworthiness history sequences, and (iv) several neural network-based approaches.

A. Predicting with Trustworthiness Sequences

So far, we have presented the design of trustworthiness history sequences in the peer-to-peer assessment components of the target online course. To this aim, we have to consider the main concepts presented in [18] related to trustworthiness history sequence as a foremost step in trustworthiness prediction and neural network design.

Active trustworthiness history sequence is the recent trustworthy history sequence. Then, we define active CA

trustworthiness history sequence $CATS_s^a$ as the ordered list of students' trustworthiness levels over the points in time:

$$CATS_s = \left(L^N_{m_1,s}, \dots, L^N_{m_i,s}, \dots, L^N_{m_q,s}\right) i \in \mathrm{M}, s \in S$$

$$CATS_s^a = \left(L^N_{m_{q-a+1},s}, L^N_{m_{q-a+2},s}, \dots, L^N_{m_q,s}\right), s \in S$$

where M is the set of modules; each module m_i refers to a point in time and $L^N_{m_i,s}$ is the overall trustworthiness level for the student *s* in each module.

Constrictive trustworthy history is the subsection average of active trustworthy history sequence.

$$CATS_s^c = \left(L^N_{m_{1..r},s}, L^N_{m_{r+1\dots q},s}, \dots\right) s \in S$$

where each element in the tuple is the average of a subset of elements in $CATS_s^a$ and k is the number of inputs of NN.

These tuples are presented in order to prepare those input sets that are required in neural network training and validation. The concept of trustworthiness sequences in prediction with neural networks is also suggested in [14]. In this proposal, the trustworthiness sequence is split into subsequences of fixed sizes, without average transformation:

$$CATS_s^W = \left(L^N_{m_1,s}, \dots, L^N_{m_w,s}\right), \left(L^N_{m_{w+1},s}, \dots, L^N_{m_{2w},s}\right), \dots \; s \in S$$

where each component in the trustworthiness window is a subset of the $CATS_s$.

B. Designing a Neural Network e-Assessment Proposal

Although we have reviewed complementary related trustworthiness prediction work, we select the neural network-based approaches for predicting trust values presented in [14] and [18], because these approaches are feasible in the context of e-assessment. These models present several significant differences, especially with respect to how to build training sets, these differences are considered in our e-assessment proposal.

A neural network can capture any type of non-linear relationship between input and output data through iterative training. In our case, the input is the CA trustworthiness history sequence formed by trustworthiness results generated by the peer-to-peer assessment component, and the output is the prediction calculated by the neural network (i.e. trustworthiness predicted value):

$$L^N_{m_{t+1},s} = NN(CATS_s), s \in S$$

where entity *s* denotes the identity of the student whose normalized trustworthiness level value is being predicted through the $CATS_s$ representing data generated by the peer-to-peer activity of the CA, and m_{t+1} denotes the trustworthiness point in time in the future predicted by the function NN for the student *s* (i.e. the output of the NN).

As presented in [14], the main principle of neural computing is the decomposition of the input-output relationship into a series of linearly separable steps using hidden layers. The NN architecture is composed of sets of neurons that are arranged in multiple layers. The first layer, which inputs are fed to the network, is called the input layer. The last layer, which produces the NN output, is called the output layer. The layers in between these two layers (i.e. between input and output layers) are all hidden layers. The input consists of values that constitute the inputs for the hidden layers (i.e. it is not composed of full neurons).

Every node computes a weighted function of its inputs and applies an activation function to compute the next output. The output is transmitted to all the connected nodes on the next layer with associated weights. The activation of each node depends on the bias of the node, which calculates the output as follows:

$$y_j = \sum_{i=0}^{n} w_{ij} x_i$$

where *y* is the result of the summation of the product of the input *x* with its associated interconnection weight *w*. The initial weights are assigned randomly but are gradually changed to reduce the error. The difference between the desired output and the actual output constitutes the input to the back propagation algorithm for training the network based on the difference.

Through the iterative training, the NN produces better prediction accuracy in the domain of time series prediction, such as trustworthiness history sequences. In [14], the training set is formed by each the window of *w* trust values $CATS_s^W$. However, in [18], the trustworthiness training set is the constrictive trustworthy history and the actual trustworthiness value. Furthermore, the training process can be enhanced with manual assessment data from our hybrid assessment model. If a tutor performs the same assessment process than students, these results can be included as reference students' trustworthiness levels.

C. Predicting Trustworthiness with other Models

Although we have propose NN methods devoted to manage trustworthiness in e-assessment, there exists additional approaches based on others models; namely, collaborative filtering methods can be suitable in the context of peer-to-peer assessment. As stated in [22] the task of the collaborative filtering recommendation algorithm concerns the prediction of the target user's rating for the target item that the user has not given the rating, based on the users' ratings on observed items. Moreover, collaborative filtering is a three-stage process of finding similar users, computing predicted ratings, and applying the predictions as recommendations to the user [23].

We consider these approaches in order to predict students' trustworthiness. In this case, the item involved in the recommendation system are the students themselves, in other words, the collaborative filtered system is formed by students assessing other students, and, therefore, the recommendation target is the student's trustworthiness level. When a collaborative filtering system generates predictions

for a target user, the system first identifies the other users whose interests correlate highly to the target user (i.e. user's neighbors). From this perspective, we may consider that if a tutor performs manual assessment, those students, which are tutors' neighbors, would be trustworthy students.

Regarding collaborative filtering and recommendation data sources, we can define peer-to-peer scores pre-assessment processes. For instance, through computing students recommendation over the set of scores (i.e. $R = (M, Q, S, SS, score)$), the system allows us to group students in trustworthiness groups. Moreover, we can predict the target student's score when he or she has not given the score.

V. Conclusions and Further Work

In this paper, we have presented an innovative prediction approach for trustworthiness behavior to enhance security in on-line assessment and this study has shown how neural network methods may support e-assessment prediction. We first motivated the need to improve information security in on-line assessment with trustworthiness solutions based on time factor models in order to analyze prediction techniques. Then, we conducted our research to peer-to-peer e-assessment, and trustworthiness sequences with the aim to apply the concept of trustworthiness sequences customized for the peer-to-peer e-assessment. Finally, we endowed our trustworthiness model with the prediction features by composing trustworthiness models, normalization, history sequences, and neural network models.

In our future work, we would like to implement a neural network by combining the training methods presented in this paper, and to validate this approach through the online course data and trustworthiness levels that we have proposed. Moreover, from our previous work on specific trustworthiness models and the results presented in this paper, we plan to enhance trustworthiness in e-assessment with the design of a methodological approach towards a comprehensive trustworthiness theoretical model for predicting trustworthiness in any e-assessment scenario.

Acknowledgment

This work was partly funded by the Spanish Government through projects TIN2011-27076-C03-02 "CO-PRIVACY" and CONSOLIDER INGENIO 2010 CSD2007-0 004 "ARES"; and the project TIN2013-46181-C2-1-R Computational Models and Methods for Massive Structured Data (COMMAS).

References

[1] E. R. Weippl, *Security in e-learning*. New York, NY: Springer, 2005.

[2] C. J. Eibl, "Discussion of Information Security in E-Learning," Universität Siegen, Siegen, Germany, 2010.

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

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

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

[6] J. Miguel, S. Caballé, F. Xhafa, and J. Prieto, "Security in Online Assessments: Towards an Effective Trustworthiness Approach to Support e-Learning Teams," presented at the 28th International Conference on Advanced Information Networking and Applications (AINA 2014), Victoria, Canada, 2014, pp. 123–130.

[7] 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. *Submitted*.

[8] J. Miguel, S. Caballé, F. Xhafa, J. Prieto, and L. Barolli, "Towards a Normalized Trustworthiness Approach to Enhance Security in On-line Assessment," presented at the Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS 2014), Birmingham, UK, 2014. *Accepted. To be presented*.

[9] S. K. Ferencz and C. W. Goldsmith, "Privacy issues in a virtual learning environment," in *Cause/Effect, A practitioner's journal about managing and using information resources on college and university campuses*, vol. 21, Educause, 1998, pp. 5–11.

[10] B. Gelbord, "On the Use of PKI Technologies For Secure and Private e-learning Environments," presented at the CompSysTech 2003 Proceedings of the 4th international conference on Computer systems and technologies: e-Learning, Sofia, Bulgaria, 2003, pp. 568–572.

[11] K. Konrad, G. Fuchs, and J. Barthel, "Trust and electronic commerce-more than a technical problem," in *Reliable Distributed Systems, 1999. Proceedings of the 18th IEEE Symposium on*, 1999, pp. 360–365.

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

[13] Y. Liu and Y. Wu, "A Survey on Trust and Trustworthy E-learning System," 2010, pp. 118–122.

[14] 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, pp. 347–378, 2012.

[15] S. P. Marsh, "Formalising Trust as a Computational Concept," University of Stirling, 1994.

[16] I. Ray and S. Chakraborty, "A Vector Model of Trust for Developing Trustworthy Systems," in *Computer Security – ESORICS 2004*, vol. 3193, P. Samarati, P. Ryan, D. Gollmann, and R. Molva, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 260–275.

[17] S. Msanjila and H. Afsarmanesh, "Automating Trust Assessment for Configuration of Temporary Partnerships," in *Innovation in Manufacturing Networks*, vol. 266, A. Azevedo, Ed. Springer US, 2008, pp. 95–104.

[18] Z. Zhai and W. Zhang, "The Estimation of Trustworthy of Grid Services Based on Neural Network," *JNW*, vol. 5, no. 10, pp. 1135–1142, 2010.

[19] W. Song, V. V. Phoha, and X. Xu, "An adaptive recommendation trust model in multiagent system," in *Intelligent Agent Technology, 2004. (IAT 2004). Proceedings. IEEE/WIC/ACM International Conference on*, 2004, pp. 462–465.

[20] A. J. Flanagin and M. J. Metzger, "Trusting expert- versus user-generated ratings online: The role of information volume, valence, and consumer characteristics," *Computers in Human Behavior*, vol. 29, no. 4, pp. 1626 – 1634, 2013.

[21] X. Liu and A. Datta, "A Trust Prediction Approach Capturing Agents' Dynamic Behavior," in *Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence - Volume Volume Three*, Barcelona, Catalonia, Spain, 2011, pp. 2147–2152.

[22] S. Gong, H. Ye, and P. Su, "A Peer-to-Peer Based Distributed Collaborative Filtering Architecture," in *Artificial Intelligence, 2009. JCAI '09. International Joint Conference on*, 2009, pp. 305–307.

[23] I. Soboroff and C. Nicholas, "Collaborative Filtering and the Generalized Vector Space Model (Poster Session)," in *Proceedings of the 23rd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, New York, NY, USA, 2000, pp. 351–353.