Computer Standards & Interfaces 44 (2016) 122–136

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

A methodological approach for trustworthiness assessment and prediction in mobile online collaborative learning

Jorge Miguel [a,*], Santi Caballé [a], Fatos Xhafa [a], Josep Prieto [a], Leonard Barolli [b]

[a] Department of Computer Science, Multimedia, and Telecommunication, Open University of Catalonia, Barcelona, Spain
[b] Fukuoka Institute of Technology, Department of Information and Communication Engineering, Fukuoka, Japan

ARTICLE INFO

Article history:
Received 9 February 2015
Received in revised form 8 April 2015
Accepted 27 April 2015
Available online 5 May 2015

Keywords:
Information security
Trustworthiness
e-Assessment
Online collaborative learning
Mobile learning

ABSTRACT

Trustworthiness and technological security solutions are closely related to online collaborative learning and they can be combined with the aim of reaching information security requirements for e-Learning participants and designers. Moreover, mobile collaborative learning is an emerging educational model devoted to providing the learner with the ability to assimilate learning any time and anywhere. In this paper, we justify the need of trustworthiness models as a functional requirement devoted to improving information security. To this end, we propose a methodological approach to modelling trustworthiness in online collaborative learning. Our proposal sets out to build a theoretical approach with the aim to provide e-Learning designers and managers with guidelines for incorporating security into mobile online collaborative activities through trustworthiness assessment and prediction.

1. Introduction

Over the last decade, Computer Supported Collaborative Learning (CSCL) has become one of the most influencing paradigms devoted to improving e-Learning [1]. Similarity, mobile learning is an emerging educational model devoted to providing the learner with the ability to assimilate learning any time and anywhere [2]. Mobile learning provides ubiquity and pervasiveness, which have become essential requirements to support learning and allow all learning community members from a variety of locations to cooperate with each other by means of a large variety of technological equipment [3]. While there has been an explosion of mobile devices and applications in the marketplace to gain access to e-Learning systems and collaborative learning processes, the development of mobile supported collaborative learning guided by technological security as a key and transverse factor has been, to the best of our knowledge, little investigated [4]. However, 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 [5,6], e-Learning services are usually designed and implemented without much consideration of security aspects. This finding has been usually tackled with ICT security solutions, but as stated in [7], 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 CSCL involve specific non-technological components. Indeed, online assessment activities (e-assessment) 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 domain 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 [8]. To conduct our research we focus on specific online collaborative activities, namely, online assessment (e-assessment). In [9], the authors report 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 this context, e-assessment is considered an e-exam with most common characteristics of virtual exams, and is typically employed to deliver formative tests to the students. An e-assessment activity is an e-exam with most common characteristics of virtual exams. Moreover, in [10] it is discussed how unethical conduct during e-learning exam-taking may occur and an approach that suggests practical solutions based on technological and biometrics user authentication is proposed.

[*] Corresponding author.
E-mail address: jmmoneo@uoc.edu (J. Miguel).

http://dx.doi.org/10.1016/j.csi.2015.04.008
0920-5489/© 2015 Elsevier B.V. All rights reserved.

In our real context of online higher education, we mainly consider peer-to-peer assessment processes and online collaborative activities, which will form e-assessment components. In this context, we propose security technological solutions extended with a functional trustworthiness approach [11–13] 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 a trustworthiness methodology. This approach is devoted to improving security in CSCL by building a trustworthiness methodology to offer guidelines for designing as well as managing security in online collaborative activities, through trustworthiness assessment and prediction. To this end, we propose a trustworthiness methodology with the aim of managing and predicting reliable assessment processes in e-assessment. As a result, by predicting collaborative e-assessment results, e-Learning designers will be able to manage assessment process with additional information generated by automatic prediction models.

This paper is structured as follows. In Section 2 we review the main works in the literature on mobile collaborative learning and security in CSCL, how trustworthiness assessment and prediction are related to security, and trustworthiness methodologies. In Section 3, we describe the theoretical features, phases, data, and processes of our methodological approach. In order to validate and support the application of the methodology, in Section 4 we concrete the most significant aspects in terms of specific methods through their application in real online courses. Moreover, in Section 5 we present and evaluate a neural network approach for peer-to-peer e-assessment prediction. Finally, conclusions and further work are presented in Section 6.

2. Background

In this section, we review the main works in the literature on mobile collaborative learning and security in collaborative learning, how trustworthiness assessment and prediction are related to security, and trustworthiness existing methodologies.

2.1. Security in online collaborative learning

According to [1], Computer Supported Collaborative Learning has become one of the most influencing educational paradigms devoted to improving e-Learning. Some authors argued that information security has to be considered with the aim of ensuring information managed in CSCL. In addition, several technological solutions were proposed [5,6]. These security solutions, based on technological approaches, tackle the security in e-Learning problem with specific methods and techniques that deal with particular security issues, but these models do not offer an overall security solution [4,14]. One of the key strategies in information security is that security drawbacks cannot be solved with technology solutions alone [7]. Even most advances security ICT solutions have drawbacks that impede the development of complete security frameworks.

Finally, some authors argue that we need to understand attacks in order to discover relevant security design factors [15]. Real-life security attacks and vulnerabilities are presented in many security reports, which justify the relevance of security attacks over the last years [16,17].

2.2. Mobile collaborative learning

Mobile learning has lately emerged with the increasing use of mobile technology in education. According to [2] and [3] the needs of educational organizations are increasingly related to modern online learning environments which must provide advanced capability for the distribution of learning activities and the necessary functionalities and learning resources to all participants, regardless of where these participants and resources are located, and whether this location is static or dynamic. The aim of newest learning environments is to enable the learning experience in open, dynamic, large-scale, and heterogeneous environments.

Although, from a general point of view, mobile learning can be considered as any time and anywhere learning experiences, [18] shows how we can consider multiple definitions of m-Learning. Moreover, because of the complexity and multidisciplinary factors of Mobile Computer Supported Collaborative Learning (MCSCL) paradigm, in [3] a three-dimensional approach has been provided to understand and unify the rather dispersion currently existing in advanced learning practices and pedagogical goals from the era of MCSCL. This approach considers the context of MCSCL from a multiple dimensional perspective: pedagogical, technological and evaluation.

In this paper, we will focus mobile learning specially on the use of mobile devices (i.e. tablets or smart phones) when developing CSCL activities. In this sense, mobile learning educational process can be considered as any learning and teaching activity that is possible through mobile tools or in settings where mobile equipment is available [18]. Therefore, we consider that mobile devices do not change significantly the CSCL processes and methodologies presented in the next sections. Hence, for the sake of simplicity, in the rest of the paper we will refer to online collaborative learning or CSCL only, which implicitly include MCSCL and collaborative learning supported by mobile devices.

2.3. Trustworthiness models and normalization

According to [19], 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 [20], a trustworthy e-Learning system is a learning system, which contains reliable serving peers and useful learning resources.

As stated by the authors in [21], through the study of the most relevant existing trust models, trustworthiness modelling can be classified into trustworthiness assessment and prediction models (note that in the literature on trustworthiness modelling, the terms determination and estimation are also used to refer assessment and prediction respectively). The first formally trustworthiness model related to information technology services was proposed in [22] from three levels. This approach considers the main factors and rules dealing with trustworthiness, which can be summarized as follows:

1. Basic trust is the general trusting disposition of an agent at time.
2. General trust represents the trust that agent has on other agent at time.
3. 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 (discussed in Section 2.5) 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 [23]. 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 [13], 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.