Using trustworthy web services for secure e-assessment in collaborative learning grids

Santi Caballé*, Jorge Miguel and Fatos Xhafa

Faculty of Computer Science, Multimedia and Telecommunications,
Open University of Catalonia,
Rambla Poblenou, 156. 08018 Barcelona, Spain
Email: scaballe@uoc.edu
Email: jmmoneo@uoc.edu
Email: fxhafa@uoc.edu
*Corresponding author

Nicola Capuano

Dept. of Information Engineering, Electrical Engineering and Applied Mathematics,
University of Salerno,
Via Giovanni Paolo II, 132 84084 Fisciano (SA), Italy
Email: ncapuano@unisa.it

Jordi Conesa

Faculty of Computer Science, Multimedia and Telecommunications,
Open University of Catalonia,
Rambla Poblenou, 156. 08018 Barcelona, Spain
Email: jconesac@uoc.edu

Abstract: The paper presents innovative trustworthy services to support secure e-assessment in web-based collaborative learning grids. Although e-Learning has been widely adopted, there exist still drawbacks which limit their potential. Among these limitations, we investigate information security requirements in on-line assessment learning activities, (e-assessment). In previous research, we proposed a trustworthiness model to support secure e-assessment requirements for e-Learning. In this paper, we present effective applications of our approach by integrating flexible and interoperable Web based secure e-learning services based on our trustworthiness model into e-assessment activities in on-line collaborative learning courses. Moreover, we leverage Grid technology to meet further demanding requirements of collaborative learning applications in terms of computation performance and management of large data sets, in order for the trustworthy collaborative learning services to be continuously adapted, adjusted, and personalised to each specific target learning group. Evaluation in a real context is provided while implications of this study are eventually remarked and discussed.

Keywords: information security; trustworthiness; assessment; prediction; online collaborative learning; CSCL; service-oriented architecture; SOA; web services; grid technology.

Reference to this paper should be made as follows: Caballé, S., Miguel, J., Xhafa, F., Capuano, N. and Conesa, J. (2017) 'Using trustworthy web services for secure e-assessment in collaborative learning grids', *Int. J. Web and Grid Services*, Vol. 13, No. 1, pp.49–74.

Biographical notes: Santi Caballé is a Hab. Full Professor at the Open University of Catalonia (Barcelona, Spain). In 2003 he started as an assistant professor and in 2006 he became associate professor at the Open University of Catalonia in the area of software engineering. He has been involved in the organisation of several international conferences and workshops, and has published over 200 research contributions including 12 books and 50 journal papers. He has also acted as an editor for books and special issues of leading international journals. His research focuses on distributed technologies, e-learning and software engineering.

Jorge Miguel's professional background embraces 12 years leading departments of Information Technology and Information Security projects as well as an extensive experience on teaching in higher education. From 2012 his research activity has been focused on e-Learning and Information Security where he has published 20 journal and conference papers, and one book. He received the degree of Computer Science Engineering (2002) from the University of Zaragoza. He also holds a university master's degree in Education and ICT (2011) from the Open University of Catalonia (UOC) and he earned his PhD in Network and Information Technologies (2015) from UOC.

Fatos Xhafa holds a PhD in Computer Science from the Technical University of Catalonia (UPC), Barcelona, Spain. He was a visiting professor at the University of London, UK (2009/2010) and a research associate at the Drexel University, Philadelphia, USA (2004/2005). He is a habilitated full professor by the Spanish Ministry of Education and Science. He has widely published in peer reviewed international journals, conferences/workshops, edited books, and proceedings. He actively participates in the organisation of international conferences. His research interests include parallel and distributed algorithms, combinatorial optimisation, approximation and meta-heuristics, networking and distributed computing, grid and P2P computing.

Nicola Capuano is research assistant at the Department of Information Engineering, Electric Engineering and Applied Mathematics of the University of Salerno. His main research interest is artificial intelligence and, among its applications, intelligent tutoring systems, knowledge representation and educational data mining. He works as a project manager and research consultant within several research and development projects. He is author of about 100 scientific papers. He is scientific referee and member of editorial boards for international journals and conferences.

Jordi Conesa is an associate professor of information systems at the Open University of Catalonia. He received his PhD in software engineering from the Technical University of Catalonia. His research interest concerns the areas of conceptual modelling, ontologies, semantic web, knowledge-based systems and e-learning. His long-term goal is to develop methodologies and tools to use ontologies effectively in several application domains, such as conceptual modelling, software engineering and e-learning. He has authored more than 50 research papers, participated in several research projects, including EU FP7, CICYT and AVANZA funded projects, and contributed to the organisation of some international conferences.

1 Introduction

Over the last decade, Computer Supported Collaborative Learning (CSCL) has become one of the most influencing paradigms devoted to improving e-Learning (Koschmann, 1996). This well mature paradigm has been extensively applied in educational institutions and solidly integrated into their pedagogical models, such as Problem-Based Learning which is usually organised around small teams of students. There exist many benefits of using CSCL approaches to support e-learning activities, which positively impact in the learning process, in terms of learning performance and outcomes (Dillenbourg, 1999, Caballé et al., 2011).

In addition, CSCL environments must provide advanced enablement for distribution of both collaborative activities and the necessary functionalities and learning resources to all participants, regardless the location of both participants and resources. The aim is to enable the collaborative learning experience in open, dynamic, large-scale and heterogeneous environments (Caballé et al., 2010), thus facing the main challenges in the development of CSCL systems in terms of non-functional requirements arisen in distributed environments. To this end, service-oriented architectures, and in particular Web services, have come to play a major role in the context of e-Learning due to the benefits that provide in terms of interoperability among heterogeneous hardware and software platforms, integration of new and legacy systems, flexibility of updating software, and so on. Moreover, Grid technology (Xhafa et al., 2010) is increasingly used for complex areas, which are computationally intensive and manage large data sets. These features form an ideal context for supporting and meeting the described demanding requirements of collaborative learning applications and, as a result, providing them with important benefits, such as wide geographical distribution of resources, multiple administrations from different organisations, transparent access to the resources, and so on.

Among these challenging requirements, information security is a significant factor involved in CSCL processes. However, according to (Weippl, 2006; Eibl, 2010), e-Learning and in particular CSCL services are usually designed and implemented without much consideration of security aspects. For instance, those cheating members who plagiarise their contributions shared with the group as well as passive members taking advantage of active members' work to dishonestly improve their assessment results, and vice versa, very active members who their extra efforts are missed or little recognised (Miguel et al., 2015). These unethical situations have in common the lack of information on what is going on in the internals of the group, leaving unknown whether each group member can act correctly and securely. To overcome this limitation, the findings about cheating and abuse as well as lack of effort recognition and appreciation during the group work have been usually tackled with Information and Communication Technologies (ICT) security solutions. However, the problems encountered in ensuring modern computing systems cannot be solved with ICT alone (Dark, 2011). Despite current advanced ICT security solutions are feasible in many e-Learning scenarios, 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 and in particular CSCL security problems.

To conduct our research on security in CSCL, we focus on specific e-assessment processes. Apampa (2009) reported that e-assessment 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. In our real context of online higher education, we consider peer-to-peer e-assessment processes in CSCL activities and propose security technological solutions extended with trustworthiness-based models and methodologies (Miguel et al., 2016; Miguel et al., 2015). Our approach is devoted to improving security in CSCL by building a trustworthiness methodology to offer guidelines for designing as well as managing security in CSCL activities through trustworthiness assessment and prediction. As a result, e-Learning designers will be able to manage assessment processes with additional information from automatic prediction models.

In this paper, we take the above challenges and approaches one step further to provide CSCL systems and applications with security Web services to support secure e-assessment processes. To this end, we propose a hybrid approach combining technological security solutions and a trustworthiness-based methodology to yield secure e-assessment Web services for CSCL in a context of interoperability among heterogeneous hardware and software platforms, integration of new and legacy systems, and flexibility of updating software, and so on. The rest of the paper is organised as follows. Section 2 shows the background of this research by an overview of service-oriented architectures, learning management systems, security and trustworthiness approaches for e-Learning. Sections 3 present our methodology to enhance security in CSCL activity by secure e-assessment services. Section 4 evaluates our approach of trustworthiness-based secure Web services in a real context of CSCL. The paper ends in Section 5 by summarising the approach presented and drawing some conclusions.

2 Background and related work

In this section, an overview of existing technologies related to our research on e-Learning, secure e-assessment, and web and grid technologies is presented along with previous research on trustworthiness methodologies. This overview will serve as both related work and background for the next sections.

2.1 Service-oriented architectures

Service-Oriented Architecture (SOA) represents the next step in the software development to help organisations meet their ever more complex set of needs and challenges, especially in distributed systems (W3C, 2004). This is achieved by dynamically discovering and invoking the appropriate services to perform a request from heterogeneous environments, regardless of the details and differences of these environments. By making the service independent from the context, SOA provides software with important non-functional capabilities for distributed environments (such as scalability, heterogeneity and openness), and makes the integration processes much easier to achieve.

SOA relies on services. According to (W3C, 2004), a service is a set of actions that form a coherent whole from the point of view of service providers and service requesters. In other words, services represent the behaviour provided by a provider and used by any requesters based only on the interface contract. Within SOA, services (Caballé, 2007);

- stress location transparency by allowing services to be implemented, replicated and moved to other machines without the requester's knowledge,
- enable dynamic access as services are located, bound and invoked at runtime,
- promote interoperability making it possible for different organisations supported by heterogeneous hardware and software platforms to share and use the same services,
- facilitate integration of other existing systems and thus protect previous investments (e.g. legacy assets),
- rely on encapsulation as they are independent from other services and their context,
- enhance flexibility by allowing services to be replaced without causing repercussions on the underlying systems involved,
- foster composition from other finer-grained services.

Organisations leveraging the key properties of SOA realise many benefits (Caballé et al., 2007). By location transparency as well as dynamic discovering and invocation of a service, software mobility becomes a reality. This allows organisations to have the flexibility to move services to different machines without having repercussions on the underlying system involved. Furthermore, on the one hand, location transparency also promotes scalability and availability without the client's knowledge as it is possible both to scale the number of instances of multiple services which are running on multiple servers and to support fault tolerance by redirecting a request when a server is unavailable. In a similar way, software quality and maintenance are also benefited by allowing the service to be validated and tested independently from any application using this service. On the other hand, by making it possible for a service to be reused in different business domains, organisations have the benefit of a greater return on the investment made in the software development while substantially reducing the time and cost spent in the construction of new software.

There is a great deal of similarities between collaborative learning needs and benefits provided by SOA. As a result of this matching, SOA appears to be the best choice to support the development of the most pervasive and challenging collaborative learning environments. In the CSCL context, SOA enhances educational organisations by increasing the flexibility of their pedagogical strategies, which can be continuously adapted, adjusted, and personalised to each specific target learning group. Moreover, SOA facilitates the reutilisation of successful collaborative learning experiences and makes it possible for the collaborative learning participants to easily adapt and integrate their current best practices and existing well-known learning tools into new learning goals (Caballé et al., 2007).

2.2 Learning management systems

Learning Management Systems (LMS) are software packages to enable the management of educational content and also integrate tools that support most of groupware needs,

such as e-mail, discussion forums, chat, virtual classrooms, and so on (Baloian et al., 2004). Over the last years, a great amount of full-featured Web based LMS systems have appeared in the marketplace offering designers and instructors generic, powerful user-friendly layouts for the easy and rapid creation and organisation of courses and activities, which can then be customised to the tutor's needs, learners' profile and specific pedagogical goals. Representative LMS systems are (Moodle, 2015) and (Sakai, 2015), which are being extensively adopted by educational organisations to help both educators create effective online learning communities, and educational institutions to highly customise the system to suit their pedagogical needs, and technological requirements.

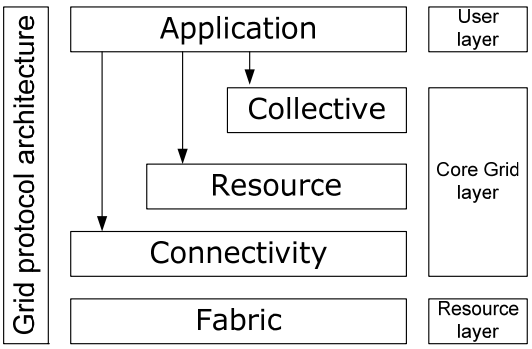
Despite the great support of LMS systems to important areas such as communication, collaboration and assessment, a very few of them are focused specifically on collaborative learning, given that they support collaboration as another learning option. Another common drawback is the lack of interoperability (e.g. Moodle is entirely written in PHP, and Sakai in Java), thus making the applications dependent from the programming language, underlying infrastructure, and so on.

2.3 Grid infrastructure

Grid computing (Foster and Kesselman, 1998) has emerged as a way of capturing the vision of a networked computing system that provides broad access not only to massive information resources, but to massive computational resources as well. The concept of computational Grid has its origins in wide-area distributed computing, and extends to a large-scale, flexible, secure, coordinated resource sharing among dynamic collections of individuals, institutions, and resources.

According to (Foster et al., 2001), Grid architecture is found in the form of five layers, which may be distributed in different levels (Figure 1): Fabric at the resource level, Connectivity, Resource, and Collective, at the core Grid level, and Application, at the user level. Detailed information of each layer can be found at (Foster et al., 2001).

Figure 1 The layered grid architecture



Many e-Learning Grids exist (Pankatrius and Vossen, 2003), such as OntoEdu (Guangzuo et al., 2004), SELF (Abbas et al., 2002), and CoAkTing (Shum et al., 2002) to overcome important non-functional requirements arisen in this context, such as scalability, availability, and distribution of computing power as well as storage capability (Foster and Kesselman, 1998; GuiLing et al., 2005). In this context, it seems clear from

the literature the key role played by SOA-based architectures, and in particular Web-service paradigm. Web-service technologies provide both interoperability to overcome the great complexity of Grid middleware and ease for the management and delivering of heterogeneous, complex learning content and courses.

From this approach, Grid provides an ideal context for supporting and producing major benefits for CSCL applications. Such important features include (: large scale of Grid infrastructures, wide geographical distribution of resources, multiple administrations from different organisations, transparent and dependable access as well as the capability of granting access to shared, heterogeneous resources in very dynamic environments.

Considering the benefits provided by Grid it is possible for educational organisations to make use of true collaborative learning environments that enable the involvement of large number of single/group participants, who can potentially belong to many different organisations, possibly situated at very different locations, and transparently share a huge variety of both software and hardware resources while enhancing human-to-human interactions (e.g. through a friendly 3D-based user interface) (Caballé, 2007).

Therefore, leveraging the inherent performance potential of Grid infrastructure for CSCL applications makes it possible to greatly enhance the collaboration experience. Moreover, the combination with SOA allows developers to cope with essential issues in CSCL, such as integration, interoperability and flexibility so as to meet the needs of different, heterogeneous and legacy environments (GuiLing et al., 2005).

2.4 Web and grid services

Although SOA can be realised with other technologies, over the last few years Web services has come to play a major role in SOA due to lower costs of integration along with flexibility and simplification of configuration.

According to W3C (2004), a Web service is a software system identified by a Uniform Resource Identifier (URI), whose public interfaces are defined and described using eXtensible Markup Language (XML). Other systems may interact with the Web service in a manner prescribed by its definition, using XML-based messages conveyed by internet protocols.

The core structure of Web services is formed by a set of widely adopted protocols and standards (W3C, 2004) such as XML, Simple Object Access Protocol (SOAP), Web Services Description Language (WSDL), and Universal Description, Discovery and Integration (UDDI), which provide a suitable technology to implement the key requirements of SOA. This is so because these protocols allow a service to be platform – and language – independent, dynamically located and invoked, interoperable over different organisation networks, and supported by large organisations (e.g. World Wide Web Consortium).

On the other hand, when servicing many requests from a highly distributed community, the problem of orchestrating and managing numerous distributed hardware and software components arises. For this reason, the term service-oriented infrastructure is introduced to denote the resource management and provisioning mechanisms used to meet quality of service goals for components and applications (Globus Toolkit 6, 2014). Grid services come to serve this purpose.

Grid services are essentially Web services with specific extensions or interfaces for use in Grids. Grid services play the central role of the Open Grid Services Infrastructure (OGSI), which intends to provide an infrastructure layer for the Open Grid Services

Architecture (OGSA, 2003). At the core of OGSI, a Grid service is a Web service that conforms to a set of conventions for such purposes as service lifetime management, inspection, and notification of service state changes. Grid services provide for the controlled management of the distributed and often long-lived state that is commonly required in distributed applications. (Czajkowski et al., 2004)

Since the replacement of OGSI in favour of the Web Service Resource Framework (WSRF) (OASIS, 2015), Grid services have been replaced by stateful Web services (among other features), and the term Grid service becomes obsolete. WSRF addresses the relationship between Web services and stateful resources through a set of conventions expressed through composable Web services specifications such as the WS-Addressing standard (Czajkowski et al., 2004). However, from the literature, the term Grid service is still on in order to distinguish between those services involved in the core grid level and stateless, typical Web-services implementing grid applications, at the user level. For the remainder of this paper, this view of Grid services will be taken.

2.5 Information security

Information Security (IS) in ICT can be defined as a combination of properties, which are provided by security services (Harris, 2002; Parker, 2002). The first security approach is the classic CIA triad that defines the three main targets of information security services: Confidentiality, Integrity and Availability (Harris, 2002). In addition, (Parker, 2002) proposed an extension to this model by including additional elements, namely, possession or access control, authenticity, and utility. However, other authors (Cheswick et al., 2003) consider technological factors and claim that as all general software has bugs, security software has also bugs. Eventually, even though security properties defined in (Parker, 2002) could be taken as a first reference, since the model proposed is not completely reliable, it is necessary to add further facilities, such as audit service and failure control in order to reduce the effects and negative consequences of security vulnerabilities. As a result, we can conclude that absolute security does not exist.

Nowadays, ICT solutions based on Public Key Infrastructure (PKI), are available to other technological implementations of services, which ensure the security issues that have been described and required in LMSs (Raina, 2003). PKI, simply defined, is an infrastructure that allows for the creation of a trusted method for providing privacy, authentication, integrity, and non-repudiation in communications between two parties. Since 1999, PKI related standards and specifications are available (Adams & Lloyd, 2003).

Finally, holistic approaches of IS are considered (Mwakalinga et al., 2009) involving different areas, such as legal aspects and privacy legislation, secure software development, networking and secure protocols, information security management systems, standards and methodologies, certification organisations, and security testing methods and tools. These approaches have introduced more complex security properties, such as authorship or non-repudiation.

2.5.1 Security dimensions

In order to address further technological security approaches, some authors (Schneier, 2003; Dark, 2011) have considered IS as a research topic beyond ICT. Schneier (2003) stated that security is both a feeling and a reality. On one hand, reality of security is

mathematical based on the probability of different risks and the effectiveness of different countermeasures. On the other hand, security is also a feeling, based on psychological reactions to both risks and countermeasures.

Moreover, absolute security does not exist and any gain in security always involves trade-offs between risk, losses, and gains (Cheswick et al., 2003). Even as it is concluded in West (2008), all security is a trade-off. This approach is very relevant in the context of this research because it is based on a hybrid security system in which technological overall solutions have to be managed beyond ICT. Moreover, Dark (2011), discussed that the issues encountered in ensuring modern computing systems cannot be solved with technology alone. Instead, IS design requires an informed, multidisciplinary approach. Therefore, the problem of IS in CSCL is tackled with a functional approach, which combines ICT security solutions with functional models, namely, trustworthiness methods and techniques in CSCL. Next, we provide an overview on security for CSCL.

2.5.2 Security in online collaborative 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 (Weippl, 2006; Eibl, 2010). 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 does not offer an overall security solution (Miguel et al., 2016; Miguel et al., 2015). One of the key strategies in information security is that security drawbacks cannot be solved with technology solutions alone (Dark, 2011). Even most advances security ICT solutions have drawbacks that impede the development of complete security frameworks.

In addition, some authors argue that attacks need to be understood in order to discover relevant security design factors (Demott, 2011). Real-life security attacks and vulnerabilities are presented in many security reports, which justify the relevance of security attacks over the last years (CSO Magazine, 2011).

To fill the previous drawbacks that impede CSCL methodologies and applications to deploy their potential, we review next trustworthiness approaches to design secure CSCL (Miguel et al., 2016).

2.6 Trustworthiness

Most of trustworthiness models in the literature are related to business processes, network services and recommendation systems (Hussain et al., 2007). However, the key concept of these works is interaction between agents, that is, the same topic studied in CSCL, where agents are students and the students' interactions and trustworthiness among them are considered.

According to Gambetta (1988) there is a degree of convergence on the definition of trustworthiness, which can be defined as follows: trustworthiness is a particular level of the subjective probability with which an agent A assesses another agent B (or group of agents). This assessment requires that the agent B will perform a particular action, before the agent A can monitor such action.

Regarding trustworthiness and e-Learning, according to Liu and Wu (2010), a trustworthy e-Learning system is a learning system, which contains reliable serving peers and useful learning resources. From these definitions, it can be claimed that trustworthiness is closely related to both students' interactions and students' actions in CSCL. Moreover, it can be considered that trustworthiness models are focused on two different dimensions, that is, trustworthiness assessment and prediction. To establish the difference between trustworthiness assessment and prediction, in Raza et al. (2012) it is stated that trust prediction, unlike trust assessment, deals with uncertainty as it aims to determine the trust value over a period in the future.

2.6.1 Trustworthiness assessment

Trustworthiness assessment is a foremost step in trustworthiness prediction. Hence, we need to review how trustworthiness can be assessed and which are the factors involved in its quantitative study. Dai et al. (2008) proposed a data provenance trustworthiness model. This model takes into account factors that may affect trustworthiness assessment.

Based on these factors, the model assigns trustworthiness scores to both data and data providers (i.e., the two agents involved in the data provenance trustworthiness assessment model). Moreover, we have to consider factors that may affect trustworthiness assessment when students are developing CSCL activities. In this sense, Bernthal (1997) designed a survey to explore interpersonal trust in work groups, identifying trust-building and trust-reducing behaviours ranked in order of importance. These behaviours can be used as trustworthiness factors, which can assess trustworthiness in CSCL activities.

Although trustworthiness levels can be represented as a combination of trustworthiness factors, in order to build these levels we also have to consider trustworthiness rules and characteristics. According to Liu and Wu (2010) there are different aspects of considering on trustworthiness, different expressions and classifications of trustworthiness characteristics. In essence, we can summarise these aspects defining the following rules: (i) Asymmetry, A trust B is not equal to B trust A; (ii) Time factor, trustworthiness is dynamic and may evolve over the time; (iii) Limited transitivity, if A trusts C who trusts B then A will also trust B, but with the transition goes on, trust will not absolutely reliable; (iv) Context sensitive, when context changes, trust relationship might change too.

2.6.2 Trustworthiness prediction

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. The existing literature suggests that the term trust prediction is used synonymously and interchangeably with the trustworthiness assessment process (Raza et al., 2012).

Several studies investigating trustworthiness prediction were carried out with neural networks (Raza et al., 2012; Zhai and Zhang, 2010; Song et al., 2004). Raza et al. (2012) proposed 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 (Raza et al., 2012).

Song et al. (2004) and Zhai and Zhang (2010) stated that trustworthiness prediction with the method of neural network is feasible. The experiments presented in this work confirm that the methods with neural networks are effective to predict trustworthiness. The work presented in Song et al. (2004) proposes a novel application of neural network in evaluating multiple recommendations of various trust standards. These cases are closely related to e-assessment regarding anomalous assessment processes as well as integrity and identity security properties.

Although we tackle the problem of predicting trustworthiness with neural network approaches, there exists other trustworthiness models without neural networks methods (Flanagin and Metzger, 2013; Liu and Datta, 2011), such as similarity approaches.

2.7 Trustworthiness approaches for secure CSCL

To date, little research has been carried out to build trustworthiness methodological approaches. However, in the context of business processes, Hussain et al. (2007) propose a generic methodology, called Trustworthiness Measurement Methodology (TMM), which can be used to determine both the quality of service of a given provider and the quality of product. The scope of this study is business processes, but the key concept of this methodology is interaction between agents, that is, the same topic that we study in collaborative learning, but in our context, considering students' interactions and trustworthiness between them. This methodology is based on the following phases: (i) Determine the context of interaction between the trusting agent and the trusted entity; (ii) Determine the criteria involved in the interaction; (iii) Develop a criterion assessment policy for each criterion involved in the interaction; and (iv) Determine the trustworthiness value of the trusted entity in the given context and time slot corresponding to the time spot of interaction by making use of specific metrics.

Carbone et al. (2003) presented the foundations of formal models for trust in global information security environments, with the aim of underpinning the use of trust-based security mechanisms as an alternative to the traditional ones. As stated by the authors, this formal model is based on a novel notion of trust structures which, building on concepts from trust management and domain theory, feature at the same time a trust and an information partial order. The formal model is focused on three target aspects, namely, trust involves entities, has a degree, is based on observations and determines the interaction among entities. In addition to methodology and formal model approaches, in another work (Wojcik et al., 2006), it is presented a trust architecture by introducing a basic trust management model based on trustworthiness previous modelling work.

3 Research methodology

In this section, the merge of CSCL, trustworthiness-based security and the use of service-oriented architectures as implementing technologies, lead our research methodology to provide an innovative approach of Web-service Collaborative Learning Management Systems (CLMS) supported by Grid technologies for enhancing functional security in CSCL.

3.1 Trustworthiness for secure CSCL

In this section, we first describe the main theoretical features and services in order to model trustworthiness as described in the next three sub-sections, and finally, the key phases of our trustworthiness and security methodology are presented.

3.1.1 Trustworthiness main concepts and analysis

In these sections, we present our methodological approach called Trustworthiness and Security Methodology in CSCL (TSM-CSCL). For the sake of simplicity, the acronym TSM is used. TSM is a theoretical approach devoted to offer a guideline for designing and managing security in collaborative e-Learning activities through trustworthiness assessment and prediction. 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 that we have discussed in our previous research (Miguel et al., 2016; Miguel et al., 2015; Miguel et al., 2015). TSM aims to deliver solutions for e-Learning designers and supports all analysis, design, and management activities in the context of trustworthiness collaborative learning activities, reaching security levels defined as a part of the methodology. Therefore, TSM tackles the problem of security in CSCL through the following guidelines and main goals: (i) define security properties and services required by e-Learning designers; (ii) build secure CSCL activities and to design them in terms of trustworthiness; (iii) manage trustworthiness in learning systems with the aim of modelling, predicting and processing trustworthiness levels; and (iv) detect security events which can be defined as a condition that can violate a security property, thus introducing a security breach in the learning system. The scope of our methodological approach is an e-Learning system formed by collaborative activities developed in a Learning Management System (LMS). The LMS has to provide support to carry out these activities and to collect trustworthiness data generated by learning and collaboration processes. Although in the context of collaborative e-Learning we can consider several actors with different roles in the overall process, for the sake of simplicity we only consider the most significant actors and roles related to this research, as follows: (i) Students, as the main actors in the collaborative learning process and as targets of the trustworthiness analysis; (ii) Designers, that represent the role in charge of all e-Learning analysis and design tasks; and (iii) Managers, that develop management processes, such as deployment, monitoring or control tasks.

3.1.2 Trustworthiness services and data gathering

In this section, we propose a trustworthiness model for security based on the previous elements and issues. Four elements in terms of trustworthiness services are considered to collect users' data for trustworthiness purposes and feed our model:

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

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

3.1.3 Modelling trustworthiness

We introduce now the concept of trustworthiness indicator t_i (with $i \in I$, where I is the set of trustworthiness indicators) as a measure of trustworthiness factors, which represent those behaviours that reduce or build trustworthiness in a collaborative group and they are considered in the design of questionnaires. An indicator t_i is associated with one of the measures defined in each e-assessment instrument (i.e. ratings, questionnaires, reports, etc.). Moreover, we introduce the concept of trustworthiness level Ltw_i is a composition of indicators over trustworthiness rules and characteristics.

For instance, we can consider two trustworthiness indicators (t_a and t_b). These indicators are different, the first indicator could be a rating in a forum post and the second one could be a question in a questionnaire; but they measure the same trustworthiness building factor (e.g. communicates honestly, find all building factors in (Miguel et al., 2015)). Finally, trustworthiness rules R, may be compared to the group, over the time or considering the context. Considering all the above, trustworthiness indicators can be represented following expression (1).

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

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

Once trustworthiness indicators have been selected, trustworthiness levels can be expressed as follows (2).

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

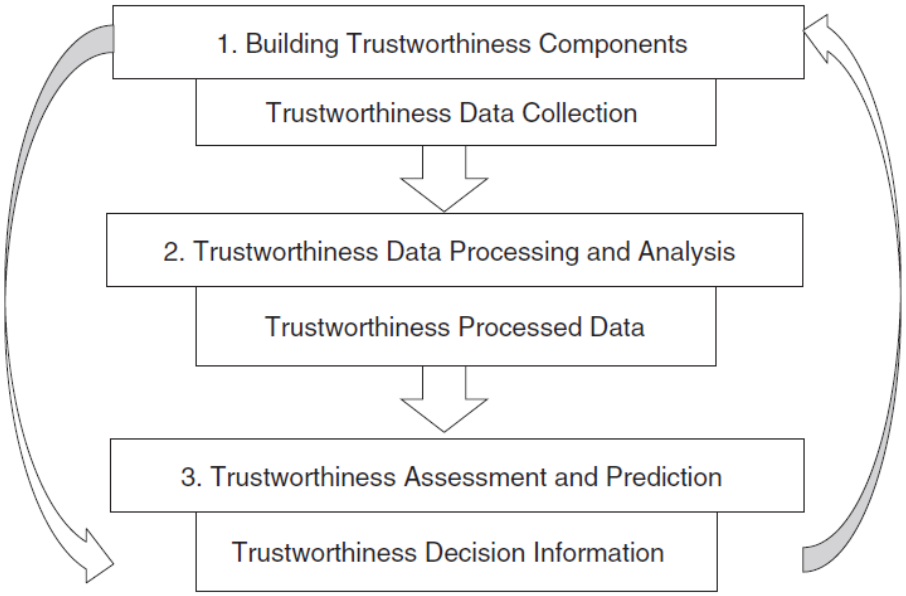
where I is the set of trustworthiness indicators which are combined in the trustworthiness level Ltw_i. Finally, trustworthiness levels Ltw_i must be normalised (see the normalisation procedure in (Miguel et al., 2016).

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

3.1.4 Trustworthiness security methodology

As shown in Figure 2, the TSM methodology is divided into three sequential phases: (i) Building Trustworthiness Components integrated into the design of secure collaborative learning activities; (ii) Trustworthiness Analysis and Data Processing based on trustworthiness modelling; and (iii) Trustworthiness Assessment and Prediction to detect security events and refine the design process. Although we have assessed each phase of the methodology as potential sets of concurrent processes (see Miguel et al., 2016), these core phases have to be developed following the sequential phases presented. The main reason for defining this sequential model is the input and output flow. In other words, the output of one phase is the input of the next one. For instance, we can only start the data collection phase when trustworthiness components are deployed. Likewise, we cannot start trustworthiness prediction or assessment until data processing has been completed.

Figure 2 Trustworthiness security methodology



Although we have defined a sequential model between each phase, we can consider the overall process, formed by these three phase, as a TSM-cycle. Each TSM-cycle allows e-Learning designers to improve the collaborative learning activities from the results, and trustworthiness decision information retrieved from the previous cycle. This information can introduce design enhances which will be deployed in the next deployment (i.e. the

next time that the students carry out the activity supported by the learning component). In terms of the data flow between TSM-cycles, the input for the new design iteration is the trustworthiness decision information. For instance, if decision information shows that there exists a deficiency in a component, this impediment can be overcome through design changes that are deployed in the next execution cycle.

Miguel et al. (2016) described the processes of each phase of this methodology in detail.

3.2 Web and grid services

This section explores the most common existing CSCL needs identified in educational organisations. To this end, an overview is provided with the core services required to support collaborative learning applications. The services presented have been chosen by, first, intersecting the most successful e-Learning frameworks and systems such as (ELF, 2012; IAF, 2015; OSID, 2014). Then, services no specific for security in CSCL have been omitted. Finally, CSCL-specific secure services of each framework have been added even though they keep outside the intersection. Note that security may be explicitly (e.g., authentication and authorisation) and implicitly (e.g., messaging, content, assessment, etc) involved in any of the services described as non-functional requirement in any e-Learning service.

In order to provide a readable, useful set of secure services, they are grouped together following similar criteria as the frameworks themselves do. Therefore, in this section, we focus on the two main service layers, namely common and application services.

3.2.1 Common services

The services in this sub-section are general purpose so that they may form the basis to any e-Learning environment and may be common across multiple application domains. Common services provide lower-level functionality which is not education-specific, but upon which educational-domain services and users depend:

- Authentication. Gather required credentials from an agent, vouches for their authenticity and introduce the agent to the system.
- Authorisation. Allow an application to establish and query a user's privileges to view, create, or modify application data, or use application functionality.
- Messaging. Allow broadcast of messages to users and groups using appropriate communication technology, without being required to understand in advance the specific delivery mechanism that the service implementation will use.
- Logging. Enable any other service to be tracked and the corresponding information and events throughout the system are logged for diagnostic, performance, user and, group awareness, feedback, and so on.
- Metadata Schema Registry. Enable access to, and the manipulation of, a registry that apart from meta-data schema typically holds configuration data, application profiles, identifiers or other lookup data.

- Identifier. They are responsible for producing and making available learning objects identifiers.
- Archiving. Support access to remote storage facilities for storage and retrieval of arbitrary static content.
- Workflow. Provide a way to manage an interdependent succession of activities each of which has completion constraints.
- Search. Enable the discovery of learning materials and other related information delivered from a system.
- Service directory. Hold information about entities such as services, other repositories, people and organisations, and provides support to the finding of available services.
- Agent. These are an abstraction of an agent, device, etc. that may include basic information such as id, name, type, role, properties and contact information.
- User Preferences. Provide machine-readable information about users' personal preferences, and allows user agents, such as portals, to automatically configure themselves for particular end-users and to prevent end-users from having to enter their preferences into multiple user agents.

3.2.2 Application services

The services in this category are educational domain dependent and provide the functionality required by agents. Application services may be implemented so that they have some sort of user interface. Their key requirement is to expose their functionality for reuse by any number of agents or other application services, while implementing a standard interface to support this reuse.

- Sequencing. Define the data structures and interfaces responsible for describing the set of possible presentation sequences for the collection of content resources.
- Content Management. Provide mechanisms for the creation, flexible management and publishing of content.
- Assessment. Support the use of automated assessments. The assessment presentation and reporting is managed at the group and individual level.
- Grading. Record the grades, comments, attendance, and scores for a student or group.
- Group. Handle the creation, deletion, updating and reading of groups.
- Member. Handle the creation, deletion, updating and reading of group members.
- Course Management. Handle the creation, reading, updating and deleting of units of learning, courses, modules as well as people information, membership of units of learning, etc.
- Collaboration. Abstract service supporting specific synchronous and asynchronous collaboration, such as forum, chat, and whiteboard services.

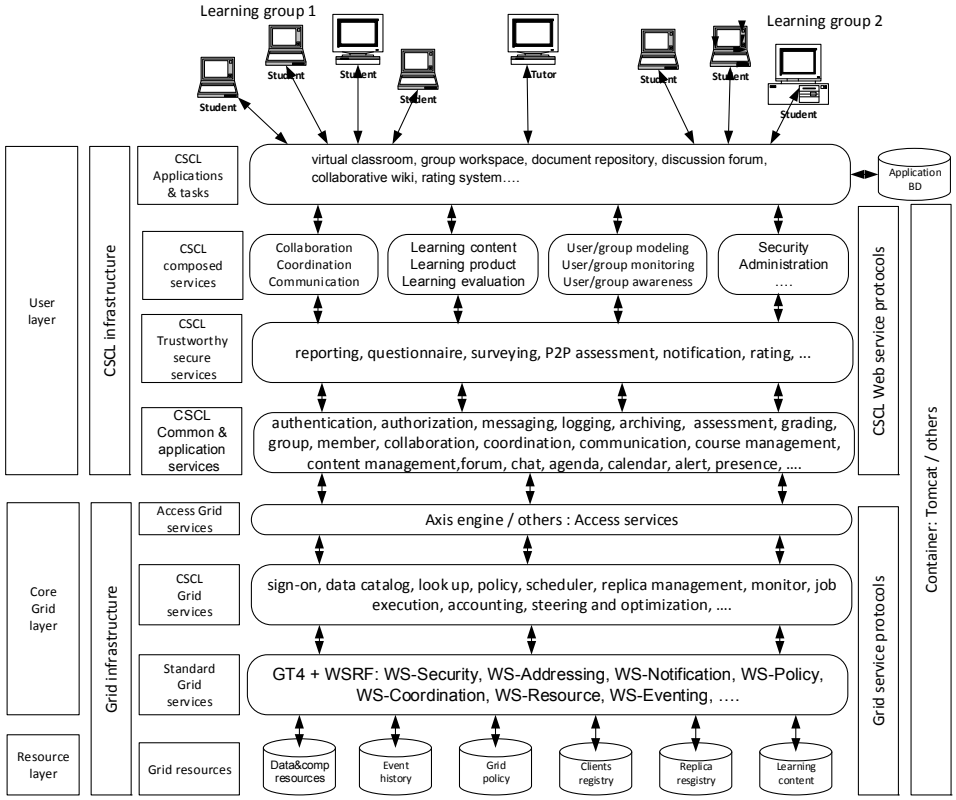
- Coordination. Abstract service supporting specific learning group formation and the definition and planning of the group objectives, such as calendaring and scheduling services.
- Communication. Abstract service supporting specific interaction between users, such as e-mail.
- Awareness. Abstract service reporting users/groups of what is happening in the learning activity, such as alert, and presence services.

3.2.3 Core grid infrastructure services

From current Grid technologies and standards (Globut Toolkit, 2014; OSID, 2014) there exist many service-oriented infrastructures for use in grids. They provide a cross-domain set of Grid services. By intersecting them with the CSCL and e-Learning domains (Pankatrius et al., 2003; Abbas et al., 2005), core Grid services for collaborative learning can be drawn:

- Sign-on. Provide authentication, authorisation, and access control for data and computing resources.
- Data Catalogue. Allow datasets to be looked up based on meta-data.
- Lookup. Represent the main entry point to access the Grid. They allow dynamic lookup of the Grid services, eliminating the need to know the service locations in advance.
- Policy. Set the access rights, rules, and permissions to allow users, agents, and applications to use Grid services.
- Scheduler: Resolve a job execution plan for Grid applications. They also submit the plan to the grid for execution.
- Replica Management. Add to Grid robustness and scalability by providing the capability to copy and move data around the Grid.
- Replica Selection: Locate the optimum replica to use for processing.
- Steering and optimisation. Allow job requests to adapt to the dynamic environment of the Grid.
- Monitor. Provide information on the current state of the job plan. They keep track of the current state of the job and the resources on which jobs are submitted.
- Accounting. Enable a fair access to resources as specified by policies.
- Estimators. Provide feedback to users, agents, and applications about how much resource a particular action might take.
- Job Execution. Execute a set of jobs as part of a job plan.
- Data Collection. Provide a way for the application to obtain the final result from the execution of the job execution.

Figure 3 Architecture of a secure web service CLMS grid



3.2.4 Architecture of a trustworthy service-oriented CLMS grid

Despite the many e-Learning Grids appeared over the last years, a very few (Abbas et al., 2005) are entirely focused on collaborative learning in a service-oriented fashion. In this section, the merge of CSCL, trustworthiness, service-oriented e-Learning Grids, and the use of Web and Grid services as implementing technologies, lead to an innovative approach of secure Collaborative Learning Management Systems (CLMS) for use in grids.

The main reason of creating service-oriented CLMS grids is to produce and consume secure, flexible, interoperable, available, reduced-cost services so as to realise the different pedagogical models designed to fulfil the collaborative learning goals. In addition, these services, and in particular the trustworthy secure services, can be shared and reused by the rest of the organisation and cross over different CLMS in the educational sector.

In Figure 3 (see Caballé, 2007) for the base CLMS Grid architecture where the secure services layer is here added), a fully service-oriented layered architecture for CLMS grids is provided to demonstrate the feasibility of the approach. This architecture is kept as simple as possible so that technical complexity are hidden (e.g. specific protocols and

connectivity issues) and the key aspects can show up. It is made up of two parts: the CLMS and Grid infrastructure. The former is based on the common and application services for secure CSCL needs described in the last section, which are realised as Web services. The latter consists of both CSCL-specific and standard grid infrastructure services, which are realised as Grid services (i.e. stateful Web-services). Next, the architecture is described in a top-bottom way, using simple terms.

At the upper level, all collaboration actors, equipped with just a Java-enabled browser, see a set of secure CSCL applications, which they interact with according specific pedagogical goals. Before the collaboration starts, the tutor is in charge of planning and designing appropriate collaborative tasks assisted by specific collaborative learning application s/he will reach by the browser.

All collaborative learning applications and tasks are packaged in high level components or abstract services to support the collaborative learning process. This will serve to group and organise the whole behaviour available as course-grained content-related packages of services so that they can be individually reused and located nearby each other. These abstract services are then backed up by secure Web services featuring a trustworthiness approach (see next subsection for our trustworthiness methodology). Group members and tutors use these trustworthiness services explicitly (e.g., report group members knowledge and attitudes) or implicitly (e.g., receive group members' rating).

At the next level, these packaged secure services are used in the concrete form they were created or with certain degree of composition. In this point, orchestration and choreography standards, such as BPEL and WS-CDL (W3C, 2004), may enter to play an important role by dynamically form the most suitable grain of Web service to be used. In any case, an independent Web service or group of Web services is to solve a specific users' and system's need, such as authentication, check the agenda, and log the last event.

From this point down, the architecture is about entering the Grid infrastructure. When accessing a grid, some services come to play in the form of external libraries. They are transparent from the application and prepare the current transaction for entering the grid. These services are dependent from the specific environment used to deploy and run the Web services, and are used for administrative, general security, and configuration purposes.

In the grid, the appropriate computational and data resources to serve the current CSCL transaction are discovered, replicated, monitored and executed according to a job schedule. All these agents and operations are seen as Grid services (e.g., look up, replica management, monitor, job execution, scheduler, etc.), and thus they are used as services performing a specific CSCL function.

Finally, each CSCL Grid service invokes the suitable service o services provided by the underlying standard framework (i.e. WSRF), which is implemented by the chosen grid middleware platform, such as GT4. WSRF provides composable Web services specifications such as the WS-Addressing standard, which provides capability for transport- neutral mechanisms for locating stateful Web services. WSRF is on top of the Resource layer (i.e. Fabric layer in the Grid architecture), and it is responsible for conveniently accessing the resource requested.

From the architectural view, all CSCL support is modelled as services. This provides collaborative learning with high degree of flexibility. No longer have group participants, learning resources, and infrastructure to be tied up in a physical location, but mobility and update are greatly achieved instead.

Standard protocols used by Web and Grid services guarantee maximum interoperability and so legacy and external CSCL applications can easily join the CLMS and also foster reuse. This allows educational organisations to share their distinct pedagogical models and experiences in the CSCL domain.

On the other hand, the fine-grained service-oriented approach and the use of Web protocols may cause repercussions on the global efficiency of the CLMS. However, the speed-up provided by using grid technology is expected to reduce it and make the system run smoothly.

4 Evaluation

In order to evaluate the potential of the deployment of our service-oriented TSM approach in a CLMS, in this section, we apply several significant aspects of TSM provided by secure services. These services are considered in terms of specific methods and techniques through their application in real online courses.

4.1 Real online courses

We have carried out three studies, based on real online courses, on the CLMS of the Open University of Catalonia (www.uoc.edu), with the aim of experimenting the specific trustworthiness methods and techniques involved in TSM, to evaluate its feasibility and to illustrate its applications.

In the first study, the collaborative activities represented a relevant component of the e-assessment phase of the course. Students' evaluation was based on a hybrid continuous model by using several manual and automatic evaluation tools. There were 12 students distributed in three groups and the course was arranged in four stages that were taken as time references in order to implement trustworthiness sequences. At the end of each collaborative stage, each student had to complete a survey. The coordinator of the group had to complete two reports, public and private and, at the end of each stage, the group members were evaluated by the coordinator. General e-Learning and CSCL activities were supported by a standard CLMS, which offered both rating systems and general learning management indicators. The low number of students involved, allowed us to study the data in detail and gave us enough flexibility to manually experiment several design alternatives, adapting the model to the design cycles proposed in TSM (see Section 3.1).

The second study extended the scope of the first one to a more standard scenario in which we could not manage so much flexibility and manual processes. Students' evaluation was based on a manual continuous evaluation model relying on several evaluation tools. Manual evaluation was complemented with automatic methods, which represented up to 20 percent of the total student's grade. Therefore, we implemented a hybrid evaluation method by combining manual and automatic approaches, and the

model allowed us to compare results in both cases. 59 students performed a subjective peer-to-peer evaluation (Richardson, 2007), that is, each student was able to evaluate the rest of class peers in terms of knowledge acquired and participation in the class assignments. The evaluation was performed for all course stages, which were taken as time references in trustworthiness history sequences.

The third study was an improvement of the first one, made within an on-line course on software development. Here 41 students were divided in 9 groups made of 4 or 5 peers and the course was divided in 6 subsequent modules. The trustworthiness indicators were calculated on data coming from three different data sources: student questionnaires, reports coming from group coordinators and forum participation data. Also in this case, the course modules were taken as references for trustworthiness sequences. The increased number of participants with respect to the first study allowed us to gather additional hints from the application of the TSM model as detailed in the next sub-sections.

4.2 Building collaborative components with TSM

After the experience designing components in the first study; in the second and third ones, we built a comprehensive peer-to-peer assessment component. We selected integrity and identity as target security properties for the component and, after the analysis of potential students' interactions in basic activities, the first version of the peer-to-peer assessment component was proposed. The final version of the component had three stages: Once the student had studied a module, the student received an invitation to a survey (S1) with questions about the current module. Students did not have to answer S1 as soon as the invitation is received. The second activity of the component was a students' forum (F), which created a collaborative framework devoted to enhance responses' quality in S1. Eventually, the student had to complete another survey (S2), which contained the set of responses over the first one (S1). By using S2, the student had to evaluate each classmate's responses as well as the participation of each student in the forum F. The design of this activity endorsed our proposal regarding the analysis of security properties, students' interactions, and factors.

Regarding trustworthy services for data collection, we included the following services: (i) Surveys; (ii) Ratings; (iii) Students reports; and (iv) CLMS indicators. To sum up, each service was integrated into the collaborative activity and it manages its own data formats.

4.3 Analysis and data processing with TSM

We analysed research instruments data formats in terms of data sources in TSM and, for each case; we selected a set of normalisation functions intended to convert basic trustworthiness data in normalised trustworthiness values. Normalisation functions were combined with trustworthiness levels and indicators. Examples of normalisation can be found in (Miguel et al., 2016).

Regarding data processing, we experimented with sequential and parallel implementations (Miguel et al., 2014). Sequential approaches were feasible to manage data sources from several activities, such as responses in a survey or number of posts in a forum. However, due to performance issues, we were not able to process log data from

our LMS with a sequential approach. For this reason, we endowed our trustworthiness framework with parallel processing facilities. To this end, we designed a MapReduce algorithm implemented in an Apache Hadoop (hadoop.apache.org) and deployed in the RDlab computing cluster of the Technical University of Catalonia (rdlab.lsi.upc.edu). Using this model, a considerable speed up was achieved in processing large log file, namely, more than 75% for 10 nodes (see (Miguel et al., 2014) for an overview of these distributed technologies and for the whole results).

4.4 Assessment, prediction and evaluation with TSM

Peer-to-peer components were designed considering the time factor. Activities were arranged in stages that conducted the definition of trustworthiness sequences. In both studies, trustworthiness indicators and levels were instanced in points of time (e.g. the same indicator measured for each module) and arranged in trustworthiness sequences. The concept of trustworthiness sequence in an evaluation component allowed us to support assessment and prediction. Actually, it could be directly incorporated, in some cases, as input for assessment and prediction methods. Regarding validation, we experimented with a hybrid validation approach by combining manual, automatic, external, and internal validation methods. As an example of this model, we analysed similarity between manual evaluation results and automatic trustworthiness levels. The method to tackle similarity proposed is based on Pearson correlation (Mobasher et al., 2007).

Finally, we considered two different methods to deal with prediction. The first approach was based on neural networks (Raza et al., 2011) and the second one on collaborative filtering. A neural network captured any type of non-linear relationship between input and output. In our case, the input was the trustworthiness history sequence and the output was the prediction calculated by the neural network (i.e., trustworthiness predicted value). On the other hand, filtering recommendation algorithms concerned the prediction of the target user's assessment, for the target item that the user was not given the rating, based on the users' ratings on observed items. In our context, items involved in the recommendation system were the students themselves.

5 Conclusions and future work

In this paper we have presented an innovative approach of service-oriented trustworthiness in the context of secure learning assessment in on-line collaborative learning grids. This approach is based first on trustworthiness factors, indicators and levels which allow for discovering how trustworthiness evolves into the learning system. Then the study shows the need to propose a service-oriented secure assessment model which combines both technological security solutions and functional trustworthiness services in order to meet challenging requirements in CSCL systems, such as security, interoperability, flexibility and so on. To this end, a holistic security model is designed, implemented and evaluated in a real context of e-Learning. The service-oriented approach realised with trustworthy Web and Grid services is designed in the paper and its potential is evaluated. It is planned to achieve a first implementation of the architecture proposed and test it using real Grid infrastructure.

Moreover, we plan to continue the methodology testing and evaluation processing by deploying e-assessment learning components in additional real on-line courses. The proposed trustworthy services will be implemented with Web services and validated in next iterations of this work, and eventually used by learning designers and developers to create real secure CSCL activities following our trustworthiness and service-oriented methodology.

Ongoing work is to incorporate a data layer in our secure Web service CLMS Grid architecture (see Figure 3) based on the Data as a Service (DaaS) of Cloud technology as the appropriate service for effective large data storage and data provision on demand to the user regardless of geographic or organisational separation of both provider and consumer (Terzo et al., 2013). In this context, SOA has also rendered the actual platform on which the location where the data resides is irrelevant. However, new issues have raised that need to be addressed, such as lack of an integrated data view and data interoperability concerns (Aflab et al., 2015). We plan to address these issues by using semantic web technologies in the context of collaborative learning from previous research (Conesa et al., 2012) by enforcing a framework for modelling, representing populating and enriching data from online collaborative sessions from Web forums. To this end, an ontology called Collaborative Session Conceptual Schema (CS^2) (Conesa et al., 2012) will be extended to define the terms and semantics of the different elements that may appear during learning in a LMS. This way, providing a particular meaning (and a given way to describe) for each element would enhance interoperability and facilitate the implementation of the presented trustworthiness indicators and levels, since the way to describe (and therefore to access the characteristics of) the different elements would be the same regardless of the LMS or technology used.

Finally, we plan to evaluate and test trustworthiness predictions methods in order to predict both trustworthiness students' behaviour and evaluation alerts, such as anomalous results. To this end, we plan to evaluate neural networks and data mining models by designing a methodological approach to construct a trustworthiness normalised model. In addition, in our future work, we would like to improve our students' public profile model in real on-line courses.

Acknowledgements

This research was partly funded by the Spanish Government through the project TIN2013-45303-P 'ICT-FLAG' (Enhancing ICT education through Formative assessment, Learning Analytics and Gamification).

References

Abbas, Z., Umer, M., Odeh, M., McClatchey, R., Ali A. and Ahmad, F. (2005) 'A semantic grid-based e-learning framework (SELF)', *Proceedings of CLAG + Grid.edu 2005*.

Adams, C. and Lloyd, S. (2003) *Understanding PKI Concepts, Standards, and Deployment Considerations*, 2nd ed., Addison Wesley.

Aftab, S., Afzal, H. and Khalid, A. (2015) 'An approach for secure semantic data integration at data as a service (DaaS) layer', *International Journal of Information and Education Technology*, Vol. 5, No. 2, pp.124–130.

Apampa, K.M. (2010) *Presence Verification for Summative E-assessments*, PhD Thesis, University of Southampton, Southampton, England.

Baloian, N., Galdames, P., Collazos, C. and Guerrero, L. (2004) 'A model for a collaborative recommender system for multimedia learning material', *Proceedings of the 10th International Workshop on Groupware*, Springer, Berlin.

Bernthal, P. (1997) 'A survey of trust in the workplace', *Executive Summary*, HR Benchmark Group, Pittsburgh, PA.

Caballé, S. (2007) 'On the advantages of using web & grid services for the development of collaborative learning management systems', *Proceedings of the 1st International Workshop on P2P, Parallel, Grid and Internet Computing* (3PGIC-2007), pp.263–270.

Caballé, S. and Xhafa, F. (2010) 'CLPL: providing software infrastructure for the systematic and effective construction of complex collaborative learning systems', *Journal of Systems and Software*, Vol. 83, No. 11, pp.2083–2097.

Caballé, S., Daradoumis, T., Xhafa F. and Juan, A. (2011) 'Providing effective feedback, monitoring and evaluation to on-line collaborative learning discussions', *Computers in Human Behavior*, Vol. 27, No. 4, pp.1372–1381.

Caballé, S., Xhafa, F. and Daradoumis, Th. (2007) 'A service-oriented platform for the enhancement and effectiveness of the collaborative learning process in distributed environments', *Proceedings of the International Conference on Grid Computing, High-Performance and Distributed Applications* (*GADA 2007*), Vilamoura, Algarve, Portugal, 29–30 November, *Lecture Notes in Computer Science*, Vol. 4804, pp.1280–1287.

Carbone, M., Nielsen, M. and Sassone, V. (2003) 'A formal model for trust in dynamic networks', *Proceedings of the International Conference on Software Engineering and Formal Methods* (*SEFM'03*), pp.54–63.

Cheswick, W.R., Bellovin, S.M. and Rubin, A.D. (2003) *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, Boston.

Conesa, J., Caballé, S., Gañán, D. and Prieto, J. (2012) 'Exploiting the semantic web to represent information from on-line collaborative learning', *International Journal of Computational Intelligence Systems*, Vol. 5, No. 4, pp.653–667.

CSO Magazine, US Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University, and Deloitte (2011) *2011 Cybersecurity Watch Survey*, Technical report, CSO Magazine.

Czajkowski, K., Ferguson, D., Foster, I., Frey, J., Graham, S., Maguire, T., Snelling, D. and Tuecke, S. (2004) *From Open Grid Services Infra-structure to WS-Resource Framework: Refactoring and Evolution*. Available online at: http://www.globus.org/wsrf/specs/ogsi_to_wsrf_1.0.pdf (accessed in June 2016).

Dai, C., Lin, D., Bertino, E., and Kantarcioglu, M. (2008) 'An approach to evaluate data trustworthiness based on data provenance', in Jonker, W. and Petkovic, M. (Eds): *Secure Data Management*, Vol. 5159, Springer, pp.82–98.

Dark, M.J. (2011) *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives, Information Science Reference*, Hershey, PA.

Demott, J.D., Sotirov, A. and Long, J. (2011) *Gray Hat Hacking*, 3rd ed., McGraw-Hill Companies, New York.

Dillenbourg, P. (1999) 'Introduction: What do you mean by 'Collaborative Learning"?' in Dillenbourg, P. (Ed.): *Collaborative Learning. Cognitive and Computational Approaches*, Elsevier Science, Oxford, pp.1–19.

Eibl, C.J. (2010) *Discussion of Information Security in E-Learning*, PhD Thesis, Universität Siegen, Siegen, Germany.

E-Learning Framework (ELF) www.elframework.org, 2012 (Web page as of June 2016).

Flanagin, A.J. and Metzger, M.J. (2013) '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.

Foster, I. and Kesselman, C. (1998) *The Grid: Blueprint for a Future Computing Infrastructure*, Morgan Kaufmann, San Francisco, CA, pp.15–52.

Foster, I., Kesselman, C. and Tuecke, S. (2001) 'The anatomy of the grid: enabling scalable virtual organizations', *International Journal of Supercomputer Applications and High Performance Computing*', Vol. 15, No. 3, pp.200–222.

Gambetta, D. (1988) 'Can we trust trust?' *Trust: Making and Breaking Cooperative Relations*, Blackwell, pp.213–237.

Globus Toolkit 6. www.globus.org/toolkit/, 2014 (Web page as of June 2016).

Guangzuo, C., Fei, C., Hu, C. and Shufang, L. (2004) 'OntoEdu: Ontology basedEducation Grid System for e-learning', *Proceedings of the 18th Global Chinese Conference on Computers in Education (GCCCE 2014)*, Hong Kong.

GuiLing, W., YuShun, L., ShengWen, Y., ChunYu, M., Jun, X. and Meilin, S. (2005) 'Service-oriented grid architecture and middleware technologies for collaborative e-learning', *IEEE International Conference on Services Computing (SCC'05)*, 11–15 July, pp.67–74.

Harris, S. (2002) *All-In-One CISSP Certification Exam Guide*, McGraw-Hill Osborne Media, New York.

Hussain, F.K., Hussain, O.K. and Chang, E. (2007) 'Trustworthiness measurement methodology (TMM) for assessment purposes', *IEEE International Conference on Computational Cybernetics, ICCC 2007*, pp.107–112.

Hussain, O., Chang, E., Hussain, F. and Dillon, T. (2009) 'Determining the failure level for risk analysis in an e-commerce interaction', in Dillon, T., Chang, E., Meersman, R. and Sycara, K. (Eds): *Advances in Web Semantics I*, Vol. 4891 of *Lecture Notes in Computer Science*, Springer, Berlin Heidelberg, pp.290–323.

IMS Abstract Framework (IAF) www.imsglobal.org/af, 2015 (Web page as of June 2016).

Koschmann, T. (1996) 'Paradigm shifts and instructional technology', in Koschmann, T. (Ed.): *CSCL: Theory and Practice of an Emerging Paradigm*, Lawrence Erlbaum Associates, Mahwah, New Jersey, pp.1–23.

Liu, X. and Datta, A. (2011) 'A trust prediction approach capturing agents' dynamic behaviour', *Proceedings of the 22nd International Joint Conference on Artificial Intelligence*, Barcelona, Catalonia, Spain, AAAI Press, pp.2147–2152.

Miguel, J., Caballé, S., Xhafa, F. and Prieto, J. (2014) 'Massive data processing approach for effective trustworthiness in online learning groups', *Concurrency and Computation: Practice and Experience*, Vol. 27, No. 8, pp.1988–2003.

Miguel, J., Caballé, S., Xhafa, F. and Prieto, J. (2015) 'Security in online web learning assessment. Providing an effective trustworthiness approach to support e-learning teams', *World Wide Web Journal*, Vol. 18, No. 6, pp.1655–1676.

Miguel, J., Caballé, S., Xhafa, F. and Prieto, J. (2016) 'A methodological approach for trustworthiness assessment and prediction in mobile online collaborative learning', *Computer Standards & Interfaces*, Vol. 44, pp.122–136.

Mobasher, B., Burke, R., Bhaumik, R. and Williams, C. (2007) 'Toward trustworthy recommender systems: an analysis of attack models and algorithm robustness', *ACM Transactions on Internet Technology*, Vol. 7, No. 4.

Moodle is found at http://moodle.org (Web page as of June 2016).

Mwakalinga, J., Kowalski, S. and Yngstrom, L. (2009) 'Secure e-learning using a holistic and immune security framework', *International Conference for Internet Technology and Secured Transactions, ICITST 2009*, pp.1–6.

OASIS, Web Services Resource Framework (WSRF) 2015. https://www.oasis-open.org/ committees/tc_ home. php?wg_abbrev=wsrf (Web page as of June 2016)

Open Grid Services Infrastructure, version 1.0, Proposed Recommendation, 2003 http://www.ggf. org/documents/GFD.15.pdf (Web page as of June 2016).

Open Service Interface Definitions (OSID) osid.org, 2014 (Web page as of June 2016).

Pankatrius, V. and Vossen, G. (2003) 'Towards e-learning grids: using grid computing in electronic learning', *Proceedings of IEEE Workshop on Knowledge Grid and Grid Intelligence*, Halifax, New Scotia, Canada, pp.4–15.

Parker, D. (2002) 'Toward a new framework for information security', *The Computer Security Handbook*, 4th ed., John Wiley & Sons, Inc., New York,

Raina, K. (2003) *PKI security solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues*, Wiley, Indianapolis.

Raza, M., Hussain, F.K. and Hussain, O.K. (2012) 'Neural network-based approach for predicting trust values based on non-uniform input in mobile applications', *The Computer Journal*, Vol. 55, No. 3, pp.347–378.

Richardson, J.C., Ertmer, P.A., Lehman, J.D. and Newby, T.J. (2007) 'Using peer feedback in online discussions to improve critical thinking', *Proceedings of the Annual Meeting of the Association for Educational Communications and Technology*, Anaheim, CA.

Sakai Project is found at http://www.sakaiproject.org (Web page as of June 2016).

Schneier, B. (2003) *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Copernicus Books, New York.

Shum, S.B., De Roure, D., Eisenstadt, M., Shadbolt, N. and Tate, A. (2002) 'CoAKTinG: collaborative advanced knowledge technologies in the grid', *2nd Workshop on Advanced Collaborative Environments, 11th IEEE International Symposium on High Performance Distributed Computing (HPDC 11)*, 24–26 July, Edinburgh, Scotland.

Song, W., Phoha, V. and Xu, X. (2004) 'An adaptive recommendation trust model in multiagent system', *Intelligent Agent Technology*, pp.462–465.

Terzo, O., Ruiu, P., Bucci, E. and Xhafa, F. (2013) 'Data as a service (DaaS) for sharing and processing of large data collections in the cloud', *Proceedings of CISIS-2013*, pp.475–480.

The Internet Engineering Task Force – IEFT (2011) Public-key infrastructure (x.509) (pkix).

Web Services Architecture Document. *W3C Working Group*, 2004 http://www.w3.org/TR/ws-arch/ (Web page as of June 2016).

Weippl, E.R. (2006) 'Security in e-Learning', in Bidgoli, H. (Ed.): *Handbook of Information Security: Key Concepts, Infrastructure, Standards and Protocols*, Vol. 1, Wiley, Hoboken, NJ, pp.279–293.

West, R. (2008) 'The psychology of security', *Communications of the ACM*, Vol. 51, No. 4, pp.34–40.

Wojcik, M., Eloff, J.H.P. and Venter, H.S. (2006) 'Trust model architecture: defining prejudice by learning', in Fischer-Hübner, S., Furnell, S. and Lambrinoudakis, C. (Eds): *Trust and Privacy in Digital Business*, Vol. 4083, Springer, Berlin Heidelberg, pp.182–191.

Xhafa, F., Paniagua, C., Barolli, L. and Caballé, S. (2010) 'A parallel grid-based implementation for real time processing of event log data in collaborative applications', *International Journal of Web and Grid Services*, Vol. 6, No. 2, pp.124–140.

Zhai, Z. and Zhang, W. (2010) 'The estimation of trustworthy of grid services based on neural network', *JNW*, Vol. 5, No. 10, pp.1135–1142.