Baltic J. Modern Computing, Vol. 7 (2019), No. 1, pp. 86–98
https://doi.org/10.22364/bjmc.2019.7.1.07

Handling Privacy and Concurrency in an Online Educational Evaluation System*

Vasiliki LIAGKOU[1], Chrysostomos STYLIOS[1], Alexander PETUNIN[2]

[1] Computer Engineering Department, Technological Educational Institute of Epirus, Kostakioi , Arta, Greece, tel:+302681050330

[2] Institute of Mechanics and Machine-Building, Ural Federal University named after First President of Russia B. N. Yeltsin, Mira str., 19, Yekaterinburg, 620002, Russia.

liagkou@kic.teiep.gr, stylios@teiep.gr, a.a.petunin@urfu.ru

Abstract. Nowadays, all academic institutions exhibit and distribute their material over Internet. Moreover, e-learning and e-evaluation products is one of the most rapidly expanding areas of education and training, with nearly 30% of U.S. college and university students now taking at least one online course. However, Internet increases the vulnerability of digital educational content exploitation since it is a potential hostile environment for secure data management. The challenge is that providing current online educational tools that are accessible by a large number of users, these educational environments handle data of varying sensitivity thus it is increasingly important to reason about and enforce information privacy guarantees in the presence of concurrency. The present paper provides a privacy preserving approach in a concurrent online educational evaluation system. It introduces a privacy preserving approach for utilizing online concurrent evaluation of acquired student competencies that handles the increasingly complex issues of designing, developing and e-competence evaluation systems suitable for educational and e-learning environments. The proposed architecture for an online competence evaluation system offers access control and protect users' private data while, it provides concurrent procedures for evaluating competencies.

Keywords: security issues for online educational environments, cryptography, trust, educational data, personal data

1 Introduction

The huge expansion of Internet has increased the vulnerability of electronic educational environments (see Rjaibi et al. (2012), Younis et al. (2013), Chen et al. (2013), Jain

* This work has been partially supported by the "Implementation of Software Engineering Competence Remote Evaluation for Master Program Graduates (iSECRET)" project No 2015- 1-LVo1-KA203-013439 funded by ERASMUS+ of the European Commission

and Ngoh (2003),Mason and Rennie (2006) and Morrisson (2003)). E-learning portals would be characterized as hostile environments from secure data management perspective. In most cases, educational organizations have to deal with all the open security challenges that could cause huge data losses, harm their reputation and strictly affect people's trust on them. One of the main obstacles for the wide adoption of online evaluation and e-educational tools is the reluctance of users to participate. This reluctance can be, partially attributed to the relatively, low penetration of technology among citizens. However, the main reason behind this reluctance is the lack of trust towards the educational online system, which flows from the distrust of users that system, may not processing concurrent access to evaluation results and may violate users' privacy. Our point of view is that privacy and concurrency are critical requirements for ensuring that online evaluation systems produce fair results and respect users' privacy. Special care has to be taken so as the algorithms, services, applications and data uploaded to the educational portal concerning the teaching material, personal information and evaluating competencies or courses and in general the whole operation of the educational management system, provide concurrent processing and remain secure and confidential to all users.

The assessment of student learning is essential and the methodologies to implement it attracted great interest from the research community (see Jain and Ngoh (2003), Morrisson (2003), Yang and Lin (2002), Romansky et al. (2015), Huu Phuoc Dai et al. (2016), Aljbori et al. (2013) and Mason and Rennie (2006)). Thus, various methods are proposed to evaluate professional skills. LeBelau et al. introduce an Integrated Design Engineering Assessment and Learning System (LeBelau et al. (2014, 2014)). Moreover there are a lot of institutions around the world that build systems for implementing assessment on the provided knowledge and learning outcomes (see Tsinakos et al. (2012,2012), Farias et al.(2016,2016) , and Ruano et al.(2007, 2007)) . There is a vast bibliography of related research work (see Rjaibi et al. (2012), Younis et al. (2013), Chen et al. (2013), Kritzinger and Solms (2006), Mohd and Fan(2010), Saxena (2004), Yong (2007), Trek (2003), Reddy (2013), Whitson (2003) and Yand and Lin (2002)) including various suggestions regarding security tools in order to resolve certain security issues; however, it is not presented any unifying secure model focusing on a particular use case and including competence online evaluation.

1.1 Outline

In the present study it is examined and proposed a privacy preserving approach for utilizing concurrent online evaluations of the users' competences. The users have to prove their eligibility to participate in the evaluation process while, they are able to securely share their learning outcomes and their possessed competences. The proposed model addresses a list of fundamental operational and security requirements. It is therefore designed as a standalone solution but it can be flexibly adapted in broader educational tools and environments. This has to be the backbone of any educational organization for managing its online learning system. It is adapted in the broader competence evaluation infrastructures of educational study subjects as well as in existing management platforms of educational organizations. The proposed e-competence evaluation system includes the development of a privacy preserving approach based on the cryptographic

primitives called Attribute Based Credentials (Rannenberg et al. (2014)). The online educational system will offer to the authorized users the concurrent procedures for evaluating their competences and it will provide fair results. Moreover, the users have to prove their eligibility to participate in the evaluation while, at the same time, the evaluation process preserves their privacy and ensures that produce meaningful and consistent results. This work proposes a new architectural model with the following benefits:

1. It provides a productive environment suitable for various applications in many sectors and it covers a lot of possible use cases.
2. It is designed as a standalone solution, while it can be flexibly adapted in broader management infrastructures as well as in existing educational platforms.
3. It provides concurrent processing and protects users' privacy rights. Moreover, it can be the backbone of any modern Internet-based educational evaluation data management system.
4. It is based on the open source idea in order to be software/hardware platform independent, requiring low development and maintenance costs and it is easily adapted to future changes.
5. It provides an effective way to increase scalability while guaranteeing security on users and data.
6. It can be a suitable component for existing open-source or even commercial educational evaluation platforms.

2 The challenge of privacy and concurrency in online evaluation system

The challenge of Concurrency : Many different online systems have been proposed for concurrent accesses to their databases. A number of concurrency control methods are available in the literature (Tang et al.(2017), Souri et al. (2016), Abbott and Garcia-Molina(1988) and Ahn(1994))providing both parallel access to distributed systems databases and concurrent transactions to database records. Beyond that, several studies examined concurrency control methods for locking data objects and avoiding clobbered reads such as Harding and Aken (2017) and Wang and Kimura (2016). In Lindstroom (2000), Gray and Reuter (1993), various concurrency control methods are introduced for locking data files and provide multiple concurrent readings. Hence, it could be argued that there are no approaches focusing on online education systems that provide a unifying model in order to avoid/dismiss clobbered reads. Eventually, by the provision of current online educational tools accessible to a large number of users, an online competence evaluation system is able to handle data of varying sensitivity; Thus, it is increasingly important to reason about and enforce information privacy guarantees in the presence of concurrency.

– A competence evaluation system should process concurrent accesses to its database. The statements of an online evaluation system could update the same data within multiple simultaneous transactions. Transactions executing at the same time need to produce meaningful and consistent results. Therefore, control of data concurrency and data consistency is vital in a competence evaluation database.

- Educational data concurrency means that many users can access educational data (particularly the competence evaluation quizzes) at the same time. Educational data concurrency is provided by providing simultaneously and unlikable users' actions thought the use of polymorphic pheudonymization.
- Educational Data consistency means that each user sees a consistent view of the educational data, including visible changes made by the users' own transactions and transactions of other users. Educational data consistency is achieved by using timestamps. More precisely, when an annotation process finishes (i.e., educational or evaluation data), the resulted digital files are locked into a steady state by using hash function. The system stamps the state of each file so that no future modifications are possible without detection by utilizing electronic fingerprints including time.
- Educational data integrity means the educational data and structures must reflect all changes in the correct sequence. Educational data integrity is achieved through the computation message authentication code (MAC) functions on stored data.

A concurrency conflict in the proposed competence evaluation system occurs when a professor displays an entity's data in order to edit it, and then another professor updates the same entity's data before the first user's change is determined in the database. In this competence evaluation system, there is a detection of such conflicts, thus if a professor updates the educational content last overwrites the other users' changes. In the competence evaluation application, no concurrency conflict will be occurred among users since they can edit only their own competence evaluation quizzes.

The challenge of Privacy The World Wide Web powers countless aspects of online applications that provide concurrent accesses to its databases. This is closely affiliated with social and economic benefits through the provision of more responsive services, faster/shorter interactions, remote activities, greater convenience, remote guidance support, higher availability/accessibility of electronic resources and remote control of services. However, the potential benefit will only be achieved if services and products are designed with trust and privacy so that users feel they are fair and safe to use the online system. Every online system user creates a lot of personal information. By using an online system, users leave various digital tracks that are being used for profiling and identification (Mayer and Mitchell (2012)). Furthermore, every online application user should feel confident and trust the application and its services, since it handles data that safeguard users' privacy interests. Although privacy enhancing technologies can help online users to protect their privacy, only a few privacy enhancing technologies are deployed in online applications (Spiekermann and Cranor(2009)). The online system that is introduced in this paper preserves the user's privacy and increases the trustworthiness of the system. The proposed online educational evaluation system does not use the common user authentication methods (e.g. PKI based) for controlling access to the online evaluation services. Online educational systems do not need to reveal users full identity profile in order to give access to educational services. In such types of applications there is, clearly, a need for partial and not complete, revelation of the users' identity; thus, the use of *Attribute Based Credentials* is highly recommended. *Attribute Based Credentials (ABC)* are a form of authentication mechanism that allows flexible and selective

authentication of different attributes about an entity without revealing additional information about the entity, for more details see Bichsel et al. (2009) , Camenish (2001) and Camenish et al. (2001).

Privacy Attribute-Based Credentials or *Privacy-ABCs*, is a technology that enables privacy preserving, partial authentication of users (Camenish et al. (2002) and (2004), Rannenberg et al. (2014), Zhang et al. (2016) and Liagkou et al. (2014)). Privacy-ABCs are issued just like normal electronic credentials (e.g. PKI based) using a secret signature key owned by the credential issuer. However, there is a key feature of this technology; indeed, the user is able to transform the credentials into a new form, called presentation token that reveals only the information about him/her, which is really necessary in order to access a service. This new token can be easily verified through the issuers' public key. The main ABC entities are four: the *Issuer*, the *User*, the *Verifier*, and the *Revocation Authority*. In general, the Issuer credentials contain certified user attributes attesting the validity of the attributes. The Verifier, or relying party, on the other hand, offers a service with limited access only to those users for whom it can verify the possession of certain attributes (or credentials). The Revocation Authority is responsible for revoking issued credentials, i.e. disabling the possibility of creating presentation tokens out of them.

3 Description of our architectural model

The main architecture of the competence evaluation system is shown at Figure 1. The architecture is consisted of various components that have different functionalities and roles. The main properties and interactions of the Architectural model are described as follows:

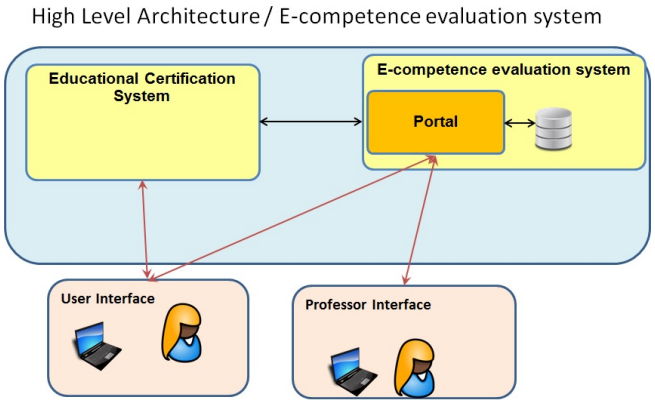

Fig. 1: Our Architectural Model

- *Portal*: his component is the web base information portal. Through this portal, the users will get information about the e-competence evaluation system and functionalities as well as about information regarding its usage. The portal includes:
  - Link to the home page
  - Information about the provided academic educational programs
  - Registration and login information
  - Help links
  - Professors' and Students' user interface
  - The Software Engineering Competence Evaluation application.
- *Educational Certification System*: This component issues credentials to the users and has the following functionalities:
  - An authorized officer inserts student information in the database of the Certification System
  - The administrator can revoke a user credential.
  - The system issues credentials to the users so that to certify their identity, eg. if they are students or professors.
  - Users are able to browse their personal data stored in the academic institution Database, through their interface.
  - Users are able to manage a limited subset of their personal information.
  - Users are issued credentials that certify that they are able to participate to the e-competence evaluation system.

  When a user requests a credential, through the e-competence evaluation portal then the e-competence evaluation system initiate the issuance protocol for the provided attribute based credentials.
- *E-competence Evaluation System:* This component implements the evaluation of the users' knowledge. The procedure is the following: a user is capable to select a study subject through the academic educational program and run the competence evaluation application. Through the Learning Outcome link, he/she will see the list of the expected learning outcomes (knowledge/skill/attitudes) for the chosen Study Subject. Whenever a user wants to evaluate a competence, he/she can access the Portal though his/her computer and complete the quizzes. After completing the evaluation, the student is informed about the evaluation result and the user's profile will be updated automatically. The competence evaluation system performs access control. Only users who own the required credentials are given access to the evaluation. More precisely:
  - The professors have credentials for satisfying the following policies:
    - Create a template to describe the set of competences for the study subject of the an academic educational program that are responsible for.
    - Rate or insert a weight factor for the competence evaluation.
    - Create tests for the competence evaluation.
  - The students have credentials that fulfill the following policies:
    - To evaluate anonymously the selected competences of a study subject to which they are registered.

  When the competence evaluation procedure is completed, professors and other subscribed members can have access to the competence evaluation results.

- *User's Interface*: In order for the internet browser to recognize anonymous credentials; the users must install in their pc a specific application which runs through user interface. The installed program helps the user to perform operation on his/her credentials and initiate credential issuance and verification protocols through the user's interface. Students are issued credentials that certify that are registered to the institution and they have enrolled to a study subject and then they can have access in the education content. They are also able to participate in the competence evaluation system. If a member of the academic educational institution such as an undergraduate or graduate student or a subscribed user, possess a valid credential attesting that the user is a registered student and is also enrolled to a study subject, then this user will be able to:
  - View a Study Subject
  - View Announcements
  - View Rubrics
  - Access the evaluation area
  - Participate in self-evaluation of a selected academic or professional competence
  - Submit evaluation
  - View evaluation results
  - View the set of professional and academic competence
- *Professor's Interface*:Professors are issued credentials that certify that are professors of the institution, they are registered to the institution and they are responsible for a study subject. If a professors possess a valid credential he will be able to log into the portal and access his interface in order to:
  - Edit/Insert data in a specific Study Subject
  - View a Study Subject
  - Add Announcements
  - Edit/View Rubrics
  - Edit the contents on the evaluation area
  - Insert/edit e-Competence
  - Insert new academic competence

4 High Level Description of the Online Educational Evaluation System

This section includes a more detailed description for the realization of the online competence evaluation. The Users interact with the Educational Certification System in order to obtain their credentials, proving their studentship or their membership and their registration to corresponding study subject. The Educational Certification System provides the students access in order to evaluate, anonymously, the competence of the subjects that they have selected. Students have to install an ABC User Client (User Service + GUI) on their computers in order to have access to User Interface and to be able to interact with components of the system.

As far as security tokens are concerned, the use of a smart card is suggested. As being a tamper proof device, it offers security and it is the ideal hardware token for

storing the Users device key. Additionally, it features a cryptographic processor, which can be utilized for performing the cryptographic operations (exponentiations etc.) that are required during issuance. Moreover, it makes a User who stores his/her personal data on it, more confident and trustful. When a user wants to be registered to the online e-competence evaluation system, he/she has to submit an application to the educational institute. The educational institute is responsible to check the submitted applications and to register the user to the e-competence evaluation system. Then the administration staff of the educational institute sends to the registered users an envelope containing a properly initialized smart card and the cards PIN and PUK values along with contact smart card reader and a slip of paper containing a one-time-password for the initial logging in the Educational Certification System. The first step for the new users is to log in the Educational Certification System using their matriculation numbers as usernames and their one-time passwords. Then, they are able to register their smart cards so that the E-competence evaluation system could link their smart cards with the user information residing in the system database. After a user has registered his smart card, he/she will be able to obtain the evaluation credentials from the E-competence evaluation system. The evaluation credential proves that the user is registered to the study subject and he/she can access E-competence evaluation system.

It should be stressed here that each user is allowed to access the CE-competence evaluation system and provide his/her evaluation several times. However, only the users' last evaluation is taken into account due to the use of scope-exclusive pseudonyms. The E-competence evaluation system contains a database for storing eligibility policies and competence evaluation data for subsequent analysis.

4.1 Archiving Concurrency and Privacy

The Figure 2 depicts the application layer and core components of the proposed architecture that are required to preserve privacy and provide concurrent operations. The application layer contains the following components for issuing and verifying attribute based credential:

- *Access Control* s achieved by presenting the required terms to the users stating what credentials they have to possess in order to proceed.
- *Key element* manages the keys of all parties and keeps them up to date (key life cycle management). On input for a request for a key, it returns a (list of) cryptographic key(s) that are currently valid.
- *Cryptographic Evidence* generates the cryptographic information required e.g., to create, present, verify or inspect a presentation issuance token. It internally orchestrates and performs the mechanism of specific cryptographic methods, such as the computation of signatures commitments, zero-knowledge proofs, etc.
- *Presentation Policy* supports a User in choosing a preferred combination of credential and/or pseudonyms, if there are different possibilities to satisfy a given presentation policy.
- *Presentation Token Generator* which generates a list of possible credentials and/or established pseudonyms when it receives the presentation policies as an input.
- Claim Selection helps user to choose a presentation token description and subset of the credentials that shall be used to generate the presentation token.

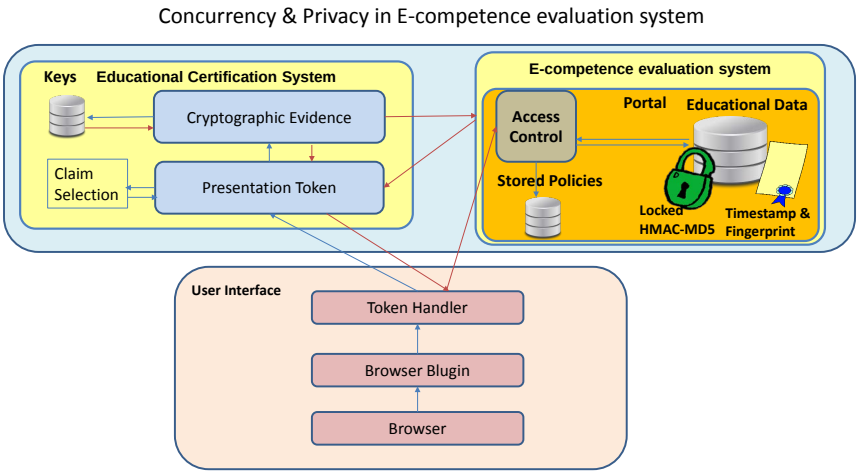

Fig. 2: Application Layer

Typically, a User requests access to educational and evaluation data from Competence Evaluation System which in turn requests a SAML assertion from an Educational Certification System. The User is redirected to the Educational Certification System to retrieve the SAML assertion before passing it back to the Competence Evaluation System. Figure 3 illustrates the protocol flow. When the competence evaluation system receives the users request to access competence evaluation procedure it interacts with Education Certification System that acts as a Verifier. The Education Certification System will then send one or more Presentation Policies. A Presentation Policy defines the set of data a user has to reveal to the Verifier in order to gain access to the requested educational data of Competence Evaluation System. The available set of credentials are the following:

- Students are issued credentials that certify that they have already been registered members of the university
- Students are issued credentials that certify that are enrolled to a study subject and they can participate to the competence evaluation system
- Professors are issued credentials that certify that they are professors of the university
- Professors are issued credentials that certify that they are responsible for a study subject

The *Education Certification System* will define the credentials that are required along with the corresponding attributes for those credentials that have to be revealed, or the conditions that the attributes have to fulfil. When *Presentation Token Generator* will define the credentials that are required along with the corresponding attributes for those credentials that have to be revealed, or for the conditions that the attributes have to fulfil. When *Presentation Token Generator* receives the presentation policies as an input, then

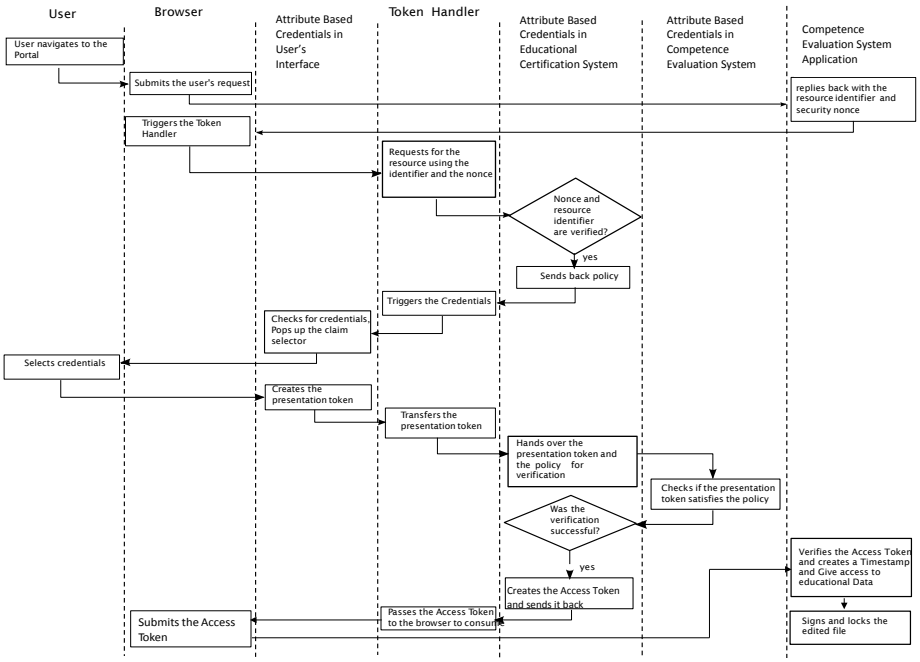

Fig. 3: Flow Diagram

it generates a list of possible credentials and/or established pseudonyms, along with the corresponding presentation token descriptions that satisfy the presentation policies. The user can choose a presentation token description and subset of the credentials that shall be used to generate his/her required presentation token. When students or professors credentials are updated, the Presentation Token Generator will generate the presentation token for the chosen presentation token description (e.g. the student is enrolled to a specific study subject or the professor who is responsible for the specific study subject).

A *cryptographic evidence* is generated that supports the token description. The cryptographic evidence uses the required credentials, or pseudonym data from the stored credentials and the required public keys in order to return the full presentation token to the user interface.

Then, the user sends the presentation token to the Competence Evaluation System. The Competence Evaluation System passes the received presentation token and the previously sent presentation policy to Educational Certification System. Educational Certification System verifies in two steps whether the presentation token satisfies the presentation policy or not. First, it checks whether the statements made in the presentation token description satisfy the required statements in the presentation policy. When the first check succeeds, i.e., the presentation token description matches the presentation policy then, it verifies the validity of the cryptographic evidence. To this point the system stores the token and returns a description of the token to the Competence Eval-

uation System. For supporting data con- currency tokens description includes unique identifier, which allows the Educational Certification System to retrieve the token later. If one of the checks fails, a list of error messages will be returned to the application. Once the Competence Evaluation System receives the verification the user can access the requested educational data. If the user has the policy to modify the educational data, in that case the Competence Evaluation System signs the edited data by using a timestamp and locks the file into the repository. Competence Evaluation System locks the edited educational data by using fingerprints (hash values); Moreover, in order to verify that this educational data has not been edited by anyone else before storing procedure begins then the system notifies the user that there has been a simultaneous modification. Otherwise, an error condition notices the professor who has created the corresponding educational data. After this, the system does not allow any access to the specific data.

5 Conclusions

This work proposed a privacy preserving approach for processing concurrent online competence evaluations. The proposed model is designed as a standalone solution but it can be flexibly adapted in broader educational tools and environments. The proposed method could be the backbone of any educational organization for managing its educational content. It is also described the architecture and main scenarios of an e-competence evaluation system. Future investigation could serve as an indicator on how to use the e- competence evaluation systems as a case study of privacy enhancement technologies in concurrent e-learning activities and in order to introduce the proposed method for the educational units of all levels within the European Union. These technologies would also support privacy preserving e-education activities in discussion groups where participants would provide their concurrent opinion anonymously but after proving that they are eligible to participate in the group discussions.

References

Abbott, R. ,Garcia-Molina, H. (1988).Scheduling real-time transactions. *ACM SIGMOD Record.*17(1),7181.

Ahn, I.(1994) Database issues in telecommunications network management. *ACM SIGMOD Record*. 23(2),37–43.

Aljbori, M. A., Guirguis, S. K., Madbouly, M. M. (2013). Adaptable mobile user interface for securing e-learning environment. *Transactions on Networks and Communications* 2(4), 64–83.

Bichsel, P., Camenisch, J., Gro, T. , Shoup, V. (2009). Anonymous credentials on a standard java card. *Proceedings of 16th ACM Conference on Computer and Communications Security,CCS*, 600-610. 2009

Bender, W., Gruhl, D., Morimoto, N., Lu, A. (1996).Techniques for data hiding. *IBM Systems Journal* 35,313-316.

Camenisch, J.(2001).Protecting (anonymous) credentials with the trusted computing group's TPM v1,135–147.2006

Camenisch, J., Lysyanskaya, A. (2001).An efficient system for non-transferable anonymous credentials with optional anonymity revocation.*Proceedings of EUROCRYPT*,93–118.2001.

Camenisch, J., Lysyanskaya, A.(2002). Dynamic accumulators and application to efficient revocation of anonymous credentials.*Proceedings of EUROCRYPT*,61–76.2002.

Camenisch, J., Lysyanskaya, A.(2004). Signature schemes and anonymous credentials from bilinear maps.*Proceedings of EUROCRYPT*,56–72.2004.

Chen, Y., He, W. (2013). Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learnin 14(5), 109–127

Dobbertin,H., Bosselaers,A.,Preneel, B. (1996). RIPEMD-160: A Strengthened Version of RIPEMD. *Proceedings of Fast Software Encryption 1996*, LNCS 1039, 71–82, Springer Verlag.

Farias, G., Muñoz de la Peña, D., Gómez-Estern, F., De la Torre, L., Sánchez, C., Dormido, S. (2016). Adding automatic evaluation to interactive virtual labs. *Interactive Learning Environments*. 24(7), 1456-1476.

Gray, J., Reuter, A.(1993). Transaction Processing: Concepts and Techniques. Morgan Kaufmann, 1993.

Harding, R, Aken, D.V., pavlo,A. ,Stonebraker, M. (2017). An evaluation of distributed concurrency control. *Proceedings of the VLDB Endowment* .10(5), 553–564.

Huu Phuoc Dai, N., Kerti, A., Rajnai, Z. (2016). E-Learning Security Risks and its Countermeasures. *Journal of Emerging research and solutions in ICT* 1(1), 17–25.

Jain, K., Ngoh, L. B. (2003). Motivating Factors in e-learning -a Case study of UNITAR.Jain. Student AffairsOnline, 4(1)`http://www.studentaffairs.com/ejournal/eLearning.html`.

Kritzinger, E. , von Solms, S. H. (2006). Elearning:Incorporating Information Security Governance. *Issues in Informing Science and Information Technology* 3,319–325.

LeBeau, J.E., McCormack, J., Beyerlein, S., Davis, D., Trevisan, M., Leiffer, P., Thompson, P., Davis, H., Howe, S., Brackin, P., Gerlick, R., Khan, M.J. (2014). Alumni perspective on professional skills gained through integrated assessment and learning. *International Journal of Engineering Education*. 30(1), 48–59.

Liagkou, V., Metakides, G., Pyrgelis, A., Raptopoulos, C., Spirakis, P., and Stamatiou, Y. (2014). Privacy preserving course evaluations in greek higher education institutes: An e-participation case study with the empowerment of attribute based credentials. *Proceedings of Privacy Technologies and Policy, volume 8319 of Lecture Notes in Computer Science*, 140–156. Springer Berlin Heidelberg.

Liagkou, V., Stylios,C. (2017). THE CASE STUDY OF A SOFTWARE ENGINEERING E-COMPETENCE EVALUATION PORTAL". *Proceedings of Actual Problem of Education (MIP-2017)*,21–23.

Lindstroom, J. (2000) Extensions to optimistic concurrency control with time intervals. *Proceedings of 7th International Conference on Real-Time Computing Systems and Applications*.IEEE Computer Society Press, 108–115.

Madhavi Latha, M., Kesavan Pillai, G., Anitha Sheela, K. (2007). Watermarking based Content Security and Multimedia Indexing in Digital Libraries. *Proceedings of International Conference on Semantic Web and Digital Libraries (ICSD-2007)*.

Mason, R. ,Rennie, F. (2006). *E-learning: the key concepts*. Oxon, England: Routledge Press, New York.

Mohd Alwi, N., Fan, I. (2010). E-Learning and Information Security Management. *International Journal of Digital Society* 1, 148–156.

Mayer, J. ,Mitchell, J.(2012). Third-party web tracking: Policy and technology.). *Security and Privacy (SP IEEE Symposium)*

Morrison, D. (2003). *E-learning strategies*, Wiley Chichester.

Rannenberg,K.,Camenisch,J., Sabouri,A. (2014).Attribute-Based Credentials for Trust: Identity in the Information Society. Springer Publishing Company, Incorporated.

Rjaibi, N., Rabai, L. B. A., Aissa, A. B., Louadi, M. (2012). Cyber Security Measurement in Depth forE-learning Systems. *International Journal of Advanced Research in Computer Science and Software Engineering* 2(11), 1–15.

Romansky, R., Noninska, I. (2015). Implementation of Security and Privacy Principles in e-Learning Architecture. *Proceedings of the 29th International Conference on Information Technologies (InfoTech-2015)*, St. St. Constantine and Elena, Bulgaria, 66–77.

Ruano , M., Colomo , P. R., Gómez, J., García Crespo, Á. (2007). A Mobile Framework for Competence Evaluation: Innovation Assessment Using Mobile Information Systems. *Journal of Technology Management & Innovation*. 2(3), 49–57.

Saxena, R. (2004). Security and online content management: balancing access and security, Breaking boundaries: integration and interoperability. *Proceedings of the 12th Biennial VALA Conference and Exhibition Victorian Association for Library Automation*. A Dynamic Data Replication with Consistency Approach in Data Grids: Modeling and Verification

Souri, A., Norouzi, M., Safarkhanlou, A., Sardroud, S.(2016). A Dynamic Data Replication with Consistency Approach in Data Grids: Modeling and Verification.*Baltic Journal of Modern Computing*. 4(3), 546–560.

Tang, D., Jiang, H., Elmore, A. (2017). Adaptive concurrency control: Despite the looking glass, one concurrency control does not fit all. *Proceeding of Biennial Conference on Innovative Data Systems Research (CIDR 2017)*.

Tsinakos, A., Kazanidis, I. (2012). Identification of Conflicting Questions in the PARES System. *International Review Of Research In Open And Distributed Learning*. 13(3),298-314.

Yong, J. (2007). Digital Identity Design and Privacy Preservation for e-Learning. *Proceeding of the 2007 11th International Conference on Computer Supported Cooperative Work in Design*,858-863.

Treek, D. (2003). An integral framework for information systems security management.*Computers and Security* 22(4), 337–360.

Abrams, M. D., Jajodia, S., Podell, H. J. (1995). Information Security: An Integrated Collection of Essays. *IEEE Computer Society Press*, Los Alamitos, CA, USA, 98–99.

Reddy, G. S. (2013). Security Issues and Threats in Educational Clouds of E-Learning: A review on Security Measures. *Computer Technology and Applications* 4,312–316.

Spiekermann, S. , Cranor,L.. Engineering privacy. *Software Engineering, IEEE Transactions*. 35(1).

Wang, T., Kimura,H.(2016).Mostly-optimistic concurrency control for highly contended dynamic workloads on a thousand cores. *Proceedings of the VLDB Endowment* .10(2), 49–60.

Whitson, G. (2003). Computer security: theory,process and management. *Journal Compututer Small Coll*18(6), 57–66.

Yang, C., Lin, F. O. ,Lin, H. (2002). Policybased Privacy and Security Management for Collaborative E-education Systems.*Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002)*, 501–505.

Younis Alsabawya, A., Cater-Steel, A., Soar,J. (2013). IT infrastructure services as a requirement for elearning system success. *Computers and Education* 69, 431–451.

Zhang ,Z., Yang ,K., Hu ,X., Wang,Y.. Practical Anonymous Password Authentication and TLS with Anonymous Client Authentication, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.*

Received July 9, 2018 , revised November 3, 2018, accepted February 15, 2019