DESIGNING A SECURE EXAM MANAGEMENT SYSTEM (SEMS) FOR M-LEARNING ENVIRONMENTS

Pravalika R, R K Pratibha, Shilpa Shree M, Sneha A P
Pursuing B.E., Computer Science and Engineering, The Oxford College of Engineering, Bengaluru, Karnataka, India
Mrs. J Jesy Janet Kumari
Assistant Professor, Dept. of CSE, The Oxford College of Engineering, Bengaluru, Karnataka, India

Abstract-M-learning has enhanced the e-learning by making the learning process learner-centered. However, enforcing exam security in open environments where each student has his/her own mobile/tablet device connected to a Wi-Fi network through which it is further connected to the Internet can be one of the most challenging tasks. It also aims to integrate the resulting secure exam system with an existing, open-source, and widely accepted Learning Management System (LMS) and its service extension to the m-learning environment. Our project aim is to provide a secured examination management system where in we have used three levels of security: Firstly, only the registered students can attend and take up the test. Secondly QR code based strategy, the exam server has to generate a QR code based exam access token for entry student. Finally, Finger print strategy is another level of security where in the exchanging of devices used by the students is prevented which has biometrics belonging to the respective, hence once the finger prints is authenticated successfully, the test starts, questions are dynamically generated by the server and the timer starts running. The test is evaluated and the results are generated instantaneously to the students and the same is sent to theserver.

Keywords-Access control, e-learning, security, randomization, biometric authentication, QR code Strategy

1 Introduction

E-LEARNING has experienced such an extraordinarygrowth over the last years that its global industry market is estimated to be worth USD 91 billion [1]. Learning Management Systems (LMSs), due to being essential tools of e-learning, have been adopted by many organizations to establish and provide access to online learning services. There have been may numerous studies to conduct exam online securelyand carry out the measurement and evaluation processes through computers since technological means such as computer and internet have been widely used in educational activities. There are numerous security threats to your computer, in particular various types of malware, which is short for malicious software

The expansion of mobile devices, meanwhile, is providingnew ways to learn (mobile learning or m-learning). The 2015 Horizon Report [7] mentions that Bring Your Own Device (BYOD) learning technology is expected to be increasingly adopted by institutions in one year's time or less to make use of mobile and online learning. Forecast of the number of smartphone users for 2019 is 5.6 billion globally which is three times that for 2013 [8].M-learning puts the control of the learning process inhands of the learner itself [10] and enhances collaborationand flexibility. It is concluded in [11] that having a mobile,accessible e-book is "perceived to benefit student learning due to the value placed on the affordance of situated study in everyday life." Some of the contributions of m-learning [14] are:

1. It is learner-centered [15].
2. It is a new alternative for information delivery and
3. It enhances collaborative learning [16].

On the other hand, m-learning faces several challenges [14] such as:
1. Lack of teacher confidence, training or technical difficulties with mobile devices [17], [18].
2. Lack of institutional support [17], [18].
3. Interoperability problems with LMSs [19].
4. Security and privacy issues [20], [21].

One possible solution to overcome these challenges is the integration of m-learning initiatives with LMSs. From students' point of view, m-learning could personalize their learning process as well as enable them to collaborate with other students or teachers.

This paper aims to design a Secure Exam ManagementSystem (SEMS) that meets the distinct security requirements of m-learning environments.This will result in a complete LMS that is both equipped with secure exam services and suitable for m-learning. However, the proposed SEMS can also work as a standalone secure exam management system for m-learning environment.

Although the proposed SEMS design is platform independent,the paper presentation adopts Android platform as a case-study for the following reasons:
1. Android devices are more affordable for students.
2. According to IDC, Android dominated the market with a 78 percent in the first quarter of 2015 [38].
3. Android is supported by many enterprises such as Google, HTC, Sony, Intel, LG, and Samsung [39].
4. For better compatibility with Fatih Project [40], the Turkish government project that seeks to integrate computer technology into Turkey's public education system. It will be fully developed on Android.

As the technology is growing more securely the examination can be done through online. There are many security measures built up in the app to take the exam. Here before taking up the exam the students have to register through app only the registered students can take up the exams. Once the students are registered manually QR code is generated and then another security level that is finger print technology is added. By using all these security measures the students can take up the exam easily on their mobile phones. The students can view their results soon after exam is over. Evaluation process takes place immediately after the exam is over.

M. Kaiiali, A. Ozkaya, and H. Haddad are with the Computer Engineering Department,MevlanaUniversity, Konya, Selcuklu 42003, Turkey E-mail: {mkaiiali, armaganozkaya, hhatem}@mevlana.edu.tr.
H. Altun is with the Electrical & Electronics Engineering Department KTO Karatay University, Turkey. E-mail: halis.altun@karatay.edu.tr.
M. Alier is with the Institute of Education Sciences, Polytechnic University of Catalonia, Barcelona, Spain. E-mail: ludo@essi.upc.edu.
Manuscript received 20 Feb. 2015; revised 8 Jan. 2016; accepted 26 Jan. 2016.
Date of publication 3 Feb. 2016; date of current version 14 Sept. 2016.
For information on obtaining reprints of this article, please send e-mail to:
reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TLT.2016.2524570
258 IEEE TRANSACTIONS ON LEARNING TECHNOLOGIES, VOL. 9, NO. 3, JULY-SEPTEMBER 2016

2 SEMS EXAM ENGINE CORE SERVICES AND FUNCTIONALITIES

There are numerous security threats to your computer, in particular various types of malware, which is short for malicious software. A in-built quiz engineis one of the basic features of any Learning Management System(LMS). Onemust consider the quiz development feature as an important criteria, when selecting a new LMS. Every institutemight be having unique quiz requirements, in spite of their entire objective is to assess learners. Pre-assessments can be used to check employee skillsets before the actual training, so that, based on the score, appropriate training can be assigned. Post-assessments are used to assess learners' skills and training effectiveness.

Well good and intuitive the LMS might be, if it doesn't have the ability to create quiz, one will have to utilize a third party author tool and publish to the SCORM or AICC format and then add it to the training curriculum. This will further impact your development time and effort. A drawback of using third party tools is that the LMS will not be able to maintain accuracy information such as score, completing status, pass or fail status, bookmarks, or interact information. It might not provide information in detail about quiz for

analysis in detail.One might not find informationlike tracking each and every attempt and response, question-wise score, and the re-usability and quick updates of questions through question banks.

Following is the checklist to evaluate the quiz builder features of an LMS. One can create and conduct quiz effectively if the LMS quiz engine has the following features:

2.1 Random Distribution of Exam Questions

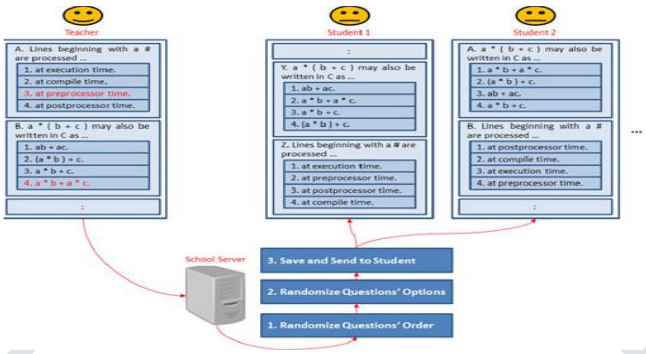

Fig 2.1 Secure distribution of exam questions

In online examination copying of the answers from one to one is common hence not giving chance for this kind of offence randomization of questions are done securely. The questions and answers options will be randomly distributed to the student so that students during the exam cannot copy from each other. Hence this approach helps to provide the secure exam management system. Moreover, the multi-choices of each question, in case of objective questions, will be flipped randomly and delivered differently to each student.

When one creates a quiz with usingquestionnaire banks as reference or by direct adding of questions to the quizzes,one can randomise the questions order and also the options. Everystudent will be receiving the questions and options in the random order. Seldomlyone needs to randomise the questions order in a block. With RandomizationQuestion, one can do just that—and so much more. Some common options include:

- Displaying all the questions in a random order.
- Displaying a set number of questions from a large group.
- Locking certain questions in a specific position.
- Hiding specific questions.

Randomization Options

There are four main randomization options:

- No Randomization: display your questions in the order they appear in your survey editor.
- Randomize the order of all questions: present all of the block in random order.
- Present only of total questions: specify the number of choices (out of the total) to have randomly displayed in the survey (2 of 4,3 of 7,etc)
- Advanced Randomization: access even more Randomization options.

2.3 Preventing the "Unattended Exam" Issue

This strategy is applied to provide a token to student which is verified by proctor. After physical authentication of student, proctor verify the student and send token to verified student then only student can start the exam on appropriate subject.He/she can subsequently open his/her course notes and use it to answer the questions illegally. To encounter this issue, we propose the following strategies.

2.3.1 Proctor Approval Based Strategy

This strategy best suits the case in which we have a small number of students and the proctor is familiar with them. Once the student logs in to the exam system, before he/she gets enrolled into the exam, his/her name will be populated in a list shown in the proctor's mobile device through the Exam Enrollment Confirmation Interface. The proctor has to physically check that all students whose names are listed are present in the dedicated class room to approve their enrollment request accordingly.In case a student is found to beabsent, his/her enrollment request will be disapproved by the proctor and an alert will be auto-generated to be sent to the appropriate person such as an Exam Security Officer.

2.3.2 Registration Based Strategy

In this online examination system the students has to register with their basic details. One should make sure the details given will not be changed because the name and the mail id given for registration should be the same when the students need to scan the QR code. Hence name and mail id are kind of authentication or security level given for the examination system.

2.3.3 QR-Code Based Strategy

The QR code is applied quickly and widely in education. We are usingreferences to find solutions to the issues of QR-codesscanning in adaptive exam method. Most of the scholars declared that QR code has many potential advantages for learning approach. There are two main processes encoding and decoding. The data entered by user is encoded into the QR code image,later the same QR code image is recorded through the Java enabled smart phone camera object and laterthe data is retrieved through the decoding process.

- MOBILE CLIENT(module1)

- This is designed for the purpose of QR code scanning which is generated by the server.
- In the side of student consist of android phone contain QR Code Reader
- They will be enabled with objective exam.

- EXAM SERVER(module2)

- These are especially for the use of the generating QR code.
- The teacher should be able to control the function of whole QR code generation from a single centralized server.
- He can access any information related with previous work and should be able to take decision on that.

- SUB MOUDLES

1. Student Registration

The students should register to the particular website to take up the exam.

2. QR code generator

As soon as the student gets registered QR code is generated manually and this code will be stored in admin info and this code will be given to the student in the time of examination.

Generated Code	Student Name	Qualification	Country	Address	State	Phone	Email
	Lakshya kumawat	MCA	India	BTM 2nd Stage	Karnataka	9292992929	lak@gmail.co
	Pravalika	BE	India	btm 2nd stage	karnataka	9999999999	praval@gmail.c
	sneha	BE	India	bangalore	karnataka	3845412	sneha@gmail.c
	sehyy	BE	India	bangalore	karnataka	3845412	shil@gmail.co

Fig 2.3.3 QR code Generated Screenshot

2.3.4 Fingerprint Based Strategy

Here we propose a fingerprint based examination hall authentication system. The system is designed to pass only users verified by their fingerprint scan and block non verified users. Once the students access the QR code and move forward for the next process fingerprint based technology is added. Finger print technology is one the security technology used. As students have android mobile finger print lock will be there. So there won't be chance of exchange of process of mobiles here. The below is the screenshot (fig 2.3) from student mobile. After the QR code authentication is succeeded the fingerprint authentication has to be. Once the students give their fingerprint the below dialogue box will open saying that the fingerprint authentication is succeeded and can access the app.

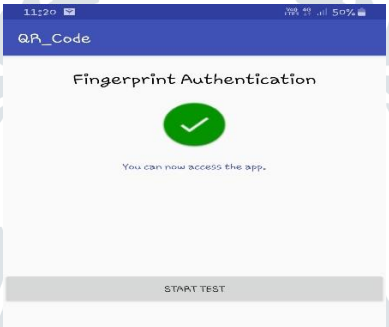

Fig 2.3.4 Fingerprint Authentication

2.4 Preventing Students from ExchangingMobile/Tablet Devices during an Exam

A student may bring mobile devices, sign into the exam system using them.Though the standard paper-based exam systems have the same issue of the possibility of students exchanging information through hidden mobile devices, with SEMS such a scenario can be prevented by the following procedure: Enforce the students to the security based strategy that are implemented in the project. Apply a security policy on the authentication server which ensures that a student can sign into the network via a single mobile device only.

2.5 Following the widely accepted Industrial Standards

SEMS Exam Engine must conform to a well-known andwidely-adopted set of standards and specifications developedby IMS Global Learning Consortium (IMS-GLC) [54].IMSGLC is a specific authorizedinstituteconsisting of distributed computer learnsystem producers,publishing agents, digital information producers, government institutes,Universities, training institutes, and other enthusiastic people. It is a global and non-profit member organizationsupported by over 190 of the world's leaders in educationaland learning technology. It has been approved and publishedfew 20 standards that are the most broadly used learningtechnologies standard in higher education around the world.These include meta-data, content packaging, enterpriseservices, question & test, competencies, tools interoperability,sharable state persistence, vocabulary definition, andlearning design. All IMS-GLC standards are available free ofcharge via the IMS GLC web site and can be used without

royalty. The IMS Question & Test Interoperability (QTI)specification enables the exchange of item, test and resultsdata between authoring tools, item banks, test constructionaltools, learning systems, and assessment delivery systems.The standard question types (e.g., multiple choice, fill inthe blank, or true/false choice) are constructed in QTIspecification using a core set of presentation and responsestructures, and results of questions are collected andscored by using a variety of methods. To represent theseoptions, the QTI specification defines the 'Item'. Items includes all the relevant data elements needed for composing,rendering, score, and providing feedback from the questions. Therefore,the key difference between a 'Question' and 'Item' isthat an 'Item' contains the 'Question', layout renderinginformation, the associated response processing information,and the corresponding hints, solutions, and feedback.Similarly, the 'test' is an instance of an Assessment. Assessmentsare assembled from Items that are contained withina 'Section' to resemble a traditional test. Additionally,assessments may be assembled from blocks of items thatare related logically. These groups are also defined as'Sections' and so Assessments are composed of one or moreSections which themselves are composed of Items, or moreSections. Collectively, these three data objects are referred toas the ASI (Assessment, Section, and Item) structures. The evaluation object could be combined together to make an objectsbank. An object bank can then be externallyreferenced andused as a single evaluation object. To avoid limitations associated
with words like user, student, or learner the IMS QTIworking group adopted the term 'participant' to refer to the
person interacting with an assessment. So, the key definitions
are:
Item - A combination of interrogatory, rendering,
and scoring information;
Section - A collection of zero or more items and/or
other Sections;
Assessment - A collection of one or more Sections;
Object Bank - A group of Items and/or Sections that
have been bundled to create an Item-bank;
Participant - The user interacting with an assessment.

3 SEMS Security Agent

It is centralized software which cannot block adhoc Bluetooth communications between students' mobile/tablet devices; neither can it block the regular cellular communications. It cannot address certain issues such as the "**unattended exam**" issue. For such special issues, we need a protocol specifically designed for m-learning environments.

3.1 Offline Exam Strategy

In this strategy, ECS itself acts as a simplified SA. It has to download the exam questions from the Exam Server through a secure channel established using predefined parameters into a temporal repository at the mobile device side. Upon completing the download, ECS, which has administrative privileges on the mobile device, blocks the Wi-Fi, Bluetooth, and cellular communications before it starts presenting the exam questions to the student from the local repository. During the exam, ECS periodically checks whether the Wi-Fi, Bluetooth, and cellular communications are still blocked to ensure that the student has not re-enabled them manually. Once the exam is over, ECS re-enables the network communication, re-establishes the secure channel with the Exam Server, and submits the student's answers signed with ECS electronic signature to the Exam Server.

3.2 Online Exam Strategy

In this strategy, students attend the exam through a secureand online channel established with the Exam Server. Thisstrategy has more advantages over the offline one. Forexample, it allows students to access a shared library ofe-books or a set of related websites pre-specified by theteacher for an open-book exam scenario. On the other hand,enforcing exam security becomes a challenge in such anopen environment.In this case, the system has to adopt a dynamic networkaccess control through which it can create andenforce different policies for different cases. For example,if the student has no exam, then all kinds of communications,including the cellular, Bluetooth, and Wi-Fi communications,are allowed. During exam time, however,cellular, Bluetooth, and Wi-Fi communications have to beblocked except the main connection to the Server throughwhich the student is tosubmit answers to questions oraccess the exam's shared library.To enforce such policies, SEMS SA is introduced. It is asoftware agent installed on students' mobile/tablet devicesand responsible for downloading the dynamic networkaccess policies from the Exam Server and for enforcingthem on students' mobile/tablet devices.

3.3 Establishing the Secured Channel with the Exam Server

A shared key, based on which the secure channel will be established, has to be initially negotiated between the two parties. The Exam Server has to maintain a database of all shared keys with the students' mobile/tablet devices while each student's device has tomaintain its own shared key only. To securely negotiate the shared key, we propose the following protocol:

1. The student must get his/her mobile device. The student has to get his/her login credentials.
2. The student has to first log in to the system through his/her device.
3. Once the login credentials are successfully authenticated, it prompts to the next page. The student has to click on scan, from his/her mobile device. As the key is presented in a QR-code format, it is secured against any kind of shoulder surfing attack and, in addition, the burden of entering a complex key manually into the student's device has been removed.
4. Once the QR code has been successfully authenticated it prompts to the next page which asks for biometric authentication to prevent exchanging of devices during exam.
5. Once all the security levels are completed, a secure channel between the Exam Server and the student's mobile device can be established at the beginning of an exam.

Fig 3.3 Secret shared key embedded in QR code

3.4 Enforcing the Downloaded Security Policy on the Student's Devices

Another issue that has to be discussed is how the SecurityAgent is going to enforce the Dynamic Security Policy onthe student's mobile devices. Fig. 13 illustrates a high levelview of a possible solution for Android devices.

Android is built based on Linux kernel where its iptablescan be used as an effective and light weight firewall. iptables4Ais an interface developed to interact with Linux iptableson Android [58]. The script has succeeded in blocking any networkcommunication going out of the tablet except thosecommunications with the specified Server-IP.The issue with iptables4A interface is that it requires aroot access. We can handle this issue in three ways:

1. By installing a custom Android ROM bundled withSEMS' APK on all students' mobile/tablet devices.
2. By rooting all students' devices before installingSEMS' APK on them and subsequently giving SEMS' APK root access privilege on each device.
3. By using the Device Administration API whichoffers the ability to give applications specific administrative

rights without the need for any superuserpermissions; it only needs the corresponding deviceadministration rights properly defined in a resourcefile. This seems to bethe easiest and the most suitable way to grant SEMS'APK with the required privileges. Currently, however,Device Administration API does not supportaccess to iptables.

Instead of iptables, SA can create a VPN and divert alltraffic on student's mobile device through it during an exam. This way, it can choose which traffic to allow andwhich to stop through its VPN. However, it also needs tokeep checking that its VPN is in active state during exams.This approach does not require rooting and is more applicableto other smart platforms where iptables is not in-built.

4 Network Related Issues

4.1 Network Overload

In case there are many students, we can deploy specific wireless routers that can support more devices connected simultaneously. We can also deploy multiple over-lapped access points in high density areas and design the access point placement such that each device always sees two or three access points. If an access point is overloaded at any given time, the client can be load-balanced to another access point without any negative impact to the end user.

4.2 Occasional Network Failures

The Exam Server creates an exam instance for every student. This instance is identified by a u unique id, let it be the corresponding student's id. The Exam Server has to keep track of the status of each established instance. If a network issue occur, secure agent must make sure that the mobile device's Wi-Fi adapter is still active. Then, SA starts sending periodic "session reconnect" requests to the Exam Server. Once the network is back, the Exam Server receives the "session reconnect" request, responses to it by restoring the tracked session, and resumes the exam directly from the failure point. SA associates the "network failure" flag along with the "session reconnect" requests to inform the Exam Server that the previous sessionhas failed due to a network issue not due to a security violation by the student.

4.3 Preventing disturbance during exam

An intruder might attempt to use a portable Wi-Fi jammer [64] that can effectively disable the Wi-Fi signal in an exam environment. There is no well-known approach available to countermeasure such attack apart from that used in some important places, such as national secret agencies where disruption of the network is a matter of national security. The procedure followed usually is:

- All Wi-Fi access points are recommended to be wire connected to the central switch. Avoiding wireless bridging helps to identify the problematic region more easily and quickly.
- Use a spectrum analyser [65] to detect the source of disturbance in the problematic region. Small attachable hardware units that turn off-the-shelf smartphone devices into low-cost, but effective RF spectrum sensors also exist [66].
- Enforce deterrent and strict laws to prevent someone from doing so.

4.4 System Architecture

To design a Secure Exam Management System (SEMS) that meets the distinct security requirements of m-learningenvironments. This will result in a complete LMS that isboth equipped with secure exam services and suitable for m-learning. Features of implemented system:

1. It has a Service Oriented Architecture.
2. Provide better security.
3. Can be access more lightly.

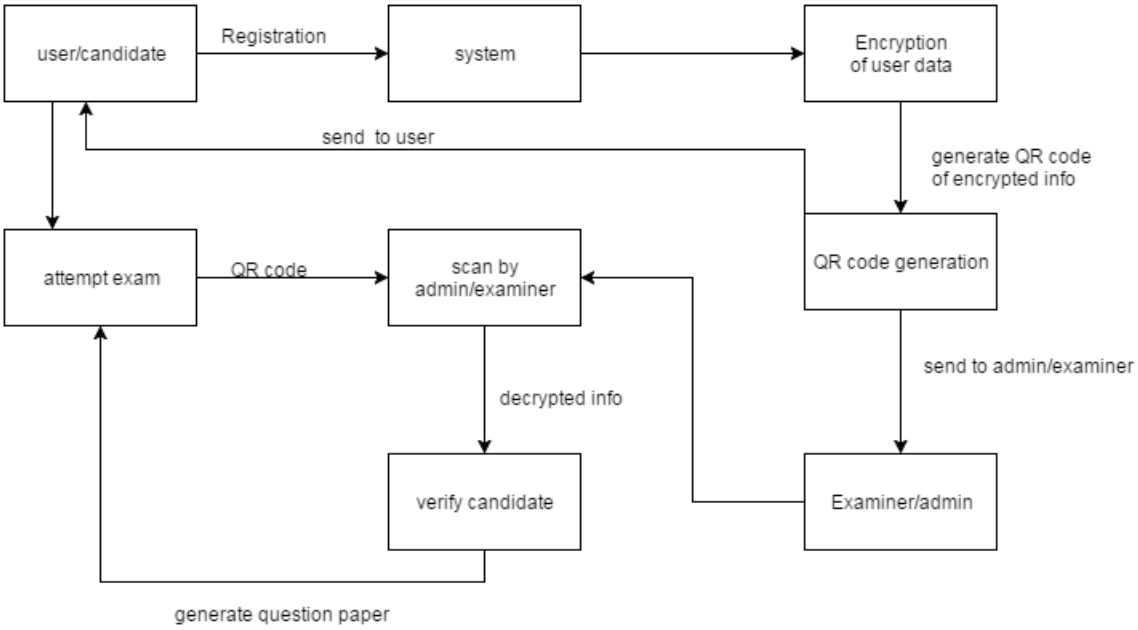

Fig 4.4 System Architecture

5 Outlook

This paper mainly concentrates on providing security while taking exam. Hence provides three level of security: Firstly only the registered students can attempt to take the exam. At the time of exam, student must login by providing his email and name, only when the provided credentials are successfully authenticated it moves to the next level. After successful login, the QR code must be scanned. When the QR code is successfully authenticated, it moves to next level where in biometric authentication is done to prevent the exchanging of devices during exam. Only after the authentication is validated the questions are generated and the timer starts. The questions are dynamically generated by the server. The questions are generated directly by the server. Once the test ends the result is generated to the student instantaneously to the student and also submitted to the server. The questions are randomly distributed and hence prevents the same questions appearing to two different students attempting the exam.

6 Conclusion

This paper proposes the design of a Secure Exam ManagementSystem to mitigate the unique exam security threats that exist in m-learning environments. SEMSoffers many exam services such as: secure and random distribution of exam questions, finger print based biometric authentication service for anti-impersonation, preventingstudents from exchanging their devices during anexam, conducting exam securely through online or offlinestrategies.

The paper also provides countermeasures against various network related issues such as network overload, occasional network failures, students attempting to use alternative mobile devices to exchange information during an exam, and an intruder using a Wi-Fi jammer to bring the Wi-Fi network down. Questions are dynamically generated from the server and randomizing of questions is done so that no two students has the same set of questions.

REFERENCES

[1] (May 2014). Think act—Corporate learning goes digital. Roland Berger Strategy Consultants [Online]. Available: https://www.rolandberger.com/media/pdf/Roland_Berger_TAB_Corporate_ Learning_E_20140602.pdf.
[2] (Nov./Dec. 2014). Training industry report. Training Mag. [Online]. Available: http://www.trainingmag.com/sites/default/files/magazines/ 2014_11/2014-Industry-Report.pdf.
[3] M. P. Prendes, "PLATAFORMAS DE CAMPUS VIRTUAL CON HERRAMIENTAS DE SOFTWARE LIBRE: An_alisis comparative de la situaci_on actual en las universidadesespa~nolas," Informe del Proyecto EA-2008-0257 de la Secretar_ıa de Estado de Universidades e Investigaci_on, 2009.
[4] G. Yamamoto and C. H. Aydin, "E-learning in turkey: Past, present and future," E-Learning Practices, vol. 2, pp. 961–987, 2010.
[5] S. Wexler, N. Grey, D. Miller, F. Nguyen, and A. Barnevelda, "Learning management systems: The good, the bad, the ugly and the truth," The E-learning Guild Res. 360 Rep. on Learning Manage. Syst., May 2008, Available: http://www.cedma-europe. org/newsletter%20articles/eLearning%20Guild/Learning% 20Management%20Systems%202008%20(May%2008).pdf.
[6] (Oct. 2013). Learning management systems market by users— Worldwide market forecasts and analysis 2013–2018. Marketsand- Markets [Online]. Available: http://www.marketsandmarkets.com/Market-Reports/learning-management-systems-market-1266.html.
[7] L. Johnson, S. A. Becker, V. Estrada, and A. Freeman. (2015). NMC horizon report: 2015 higher education edition. The New Media Consortium [Online]. Available: https://net.educause.edu/ir/ library/pdf/HR2015.pdf.
[8] (Jun. 2014). Ericsson mobility report. Ericsson, Inc. [Online]. Available: http://www.ericsson.com/res/docs/2014/ericssonmobility- report-june-2014.pdf.
[9] N. Sclater, "Web 2.0, personal learning environments, and the future of learning management systems," Res. Bull., vol. 2008, no. 13, Jun. 2008.
[10] S. Downes. (Oct. 2005). E-learning 2.0. E-Learn Mag. [Online]. Available: http://elearnmag.acm.org/featured.cfm?aid¼1104968.
[11] J. S. Kissinger, "The social and mobile learning experiences of students using mobile E-books," J. Asynchronous Learn. Netw., vol. 17, no. 1, pp. 155–170, Jan. 2013.
[12] N. M. Rao, C. Sasidhar, and V. S. Kumar, "Cloud computing through mobile-learning," Int. J. Adv. Comput. Sci. Appl., vol. 1, pp. 42–46, Dec. 2010.
[13] Y. Li, A. Guo, J. A. Lee, and G. P. K. Negara, "A platform on the cloud for self-creation of mobile interactive learning trails," Int. J. Mobile Learn. Org., vol. 7, no. 1, pp. 66–80, 2013.
[14] M. J. Casany, M. Alier, E. Mayol, J. Piguillem, N. Galanis, F. J. Garc_ıa-Pe~nalvo, and M. A. Conde, "Extending moodle services to mobile devices: The moodbile project," in Proc. 6th Int. Conf. Mobile Ubiquitous Comput., Syst., Services Technol., 2012, pp. 24–28.
[15] L. Naismith, P. Lonsdale, G. Vavoula, and M. Sharples, "Literature review in mobile technologies and learning," Future-Lab Report, Bristol, U.K., 2004.
[16] M. Sharples, J. Taylor, and G. Vavoula, "Towards a theory of mobile learning," in Proc. mLearn Conf., Oct. 2005, pp. 1–9.
[17] R. S. Cobcroft, S. Towers, J. Smith, and A. Bruns, "Mobile learning in review: Opportunities and challenges for learners, teachers, and institutions," in Proc. Online Learn. Teach. Conf., 2006, pp. 21–30.
[18] O. Zawacky-Richter, T. Brown, and R. Delport, "Factors that may contribute to the establishment of mobile learning in institutions—Results from a survey," Int. J. Interactive Mobile Technol., vol. 1, no. 1, pp. 40–41, 2007.
[19] M. Alier, M. J. Casa~n, M. A. Conde, F. J. Garc_ıa-Pe~nalvo, and C. Severance, "Interoperability for LMS: The missing piece to become the common place for elearning innovation," Int. J. Knowl. Learn., vol. 6, no. 2, pp. 130–141, 2010.
[20] E. R. Weippl, "Security considerations in M-learning: Threats and countermeasures," Adv. Technol. Learn., vol. 4, no. 2, pp. 99–105, Jan. 2007.
[21] Z. Ugray, "Security and privacy issues in mobile learning," Int. J. Mobile Learn. Org., vol. 3, no. 2, pp. 202–218, Apr. 2009.
[22] (2016, Jan.). Modular object-oriented dynamic learning environment [Online]. Available: https://moodle.org/.
[23] (2016, Jan.). Moodbile project [Online]. Available: https://code.google.com/p/moodbile/.
[24] E. Hammer-Lahav. (Apr. 2010). The oauth 1.0 protocol. Internet Eng. Task Force [Online]. Available: https://tools.ietf.org/html/rfc5849.
[25] R. Raitman, L. Ngo, N. Augar, and W. Zhou, "Security in the online e-learning environment," in Proc. 5th IEEE Int. Conf. Adv. Learn., Jul. 2005, pp. 702–706.

[26]. L. Johnson, S. A. Becker, V. Estrada, and A. Freeman, "NMC Horizon Report: 2015 Higher Education Edition," *The New Media Consortium,*
https://net.educause.edu/ir/library/pdf/HR2015.pdf. 2015.
[27]. "Ericsson Mobility Report," *Ericsson Inc.*, http://www.ericsso n.com/res/docs/2014/ericsson-mobility-report-june-2014.pdf. Jun. 2014.
[28]. N. Sclater, "Web 2.0, Personal Learning Environments, and the Future of Learning Management Systems," *Research Bulletin*, vol. 2008, no.
13, Jun. 2008.
[29]. S. Downes, "E-learning 2.0," *e-Learn Magazine*, http://elearn mag.acm.org/featured.cfm?aid=1104968. Oct. 2005.
[30]. J. S. Kissinger, "The Social & Mobile Learning Experiences Of Students Using Mobile E-Books," *J. Asynchronous Learning Networks*, vol. 17,
no. 1, pp. 155-170, Jan. 2013.
[31]. N. M. Rao, C. Sasidhar, and V. S. Kumar, "Cloud Computing Through Mobile-Learning," *Int. J. Advanced Comput. Sci. and Applications*, vol.
1, pp. 42-46, Dec. 2010.
[32]. Y. Li, A. Guo, J. A. Lee, and G. P. K. Negara, "A Platform on the Cloud for Self-Creation of Mobile Interactive Learning Trails," *Int. J. Mobile*
Learning &Organisation, vol. 7, no. 1, pp. 66-80, 2013.
[33]. M. J. Casany, M. Alier, E. Mayol, J. Piguillem, N. Galanis, F. J. García-Peñalvo, and M. A. Conde, "Extending Moodle Services to Mobile
Devices: The Moodbile Project," *Proc. The Sixth Int. Conf. on Mobile Ubiquitous Computing, Systems*, Services and Technologies, pp. 24-28,
2012.