Designing a Secure Exam Management System (SEMS) for M-Learning Environments

Mustafa Kaiiali, Armagan Ozkaya, Halis Altun, Hatem Haddad, Marc Alier

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. In such environments, students can easily exchange information over the network during exam time. This paper aims to identify various vulnerabilities that may violate exam security in m-learning environments and to design the appropriate security services and countermeasures that can be put in place to ensure exam security. 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, namely "the Moodbile Project".

Index Terms— Access control, e-learning, exam engine, Learning Management System (LMS), m-learning

————————————— ◆ —————————————

1 INTRODUCTION

E-LEARNING has experienced such an extraordinary growth 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. Nowadays, the success of LMSs is so great: 74% of the US corporations and educational institutions currently offering e-learning employ LMSs in their training programs [2]. In Spain, over 90% of the universities and colleges use an LMS [3]. According to [4], 29% of the organizations (banking sector, retailing sector, etc.) in Turkey have adopted e-learning applications. Globally, 79.5% of large companies were reported to be using these systems in their training programs in 2008 [5] and the market for LMS is estimated to have an annual growth rate of about 25.2% through the year 2018 [6].

The expansion of mobile devices, meanwhile, is providing new 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]. Thus, LMSs must change to adapt to new user requirements and technologies. For example, interaction with external applications, such as social networks and mobile applications, must be incorporated in LMSs [9] to facilitate personal learning demands that happen anywhere and at any time.

M-learning puts the control of the learning process in hands of the learner itself [10] and enhances collaboration and 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." The students that participated in this study expressed feelings of competence and high self-efficacy, and that they were able to learn more using their e-books. Moreover, among other technological factors impacting the future of m-learning, Rao et al. [12] asserted that cloud computing would make mobile learning more efficient in many ways, ultimately in time and cost. A web portal developed using Amazon's cloud computing service is presented in [13] whereby teachers without programming skills can implement interactive learning processes. The materials developed can be used with mobile applications on Android and iOS based devices.

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. From teachers' point of view, they could continue to use LMSs as their working platform, leaving mobile devices for students. The problem, however, is that the integration between m-learning applications and LMS is not an easy task. Indeed, LMSs do not generally contain interoperability standards

————————————————

- *Mustafa Kaiiali, Armagan Ozkaya, Halis Altun, and Hatem Haddad are with the Computer Engineering Department, Mevlana University, Turkey. E-mails: mkaiiali@mevlana.edu.tr, armaganozkaya@mevlana.edu.tr, haltun@mevlana.edu.tr, hhatem@mevlana.edu.tr.*
- *Marc Alier is with the Institute of Education Sciences at the Polytechnic University of Catalonia and a co-founder of Moodbile Project. E-mail: ludo@essi.upc.edu.*

to communicate with external applications; they are usually designed as monolithic or layered systems [9].

Moodle, as one of the mostly accepted and widely used open-source LMS, is a web-based application. It had a user base of 83008 registered and verified sites, serving 70696570 users in 7.5+ million courses with 1.2+ million teachers as of June 2013 [22]. Yet, due to the fact that it is not made to be service oriented, its services cannot be consumed through client applications other than web browsers. This has limited its scope of use to personal computers; therefore, the Moodbile Project [23] was conceived to extend the Moodle functionality to the world of mobile devices. This project aims to enable mobile learning applications to work together with the widely accepted Moodle LMS by incorporating the appropriate external web services into Moodle architecture or redesigning certain components of Moodle to be service oriented.

Even though Moodle 2.0 already had a collection of web services, these web services focused on developing an API suitable for massive batch actions like user or course creation and inscriptions. They are not, however, suitable for the integration of mobile learning applications and do not properly address security management issues. Moodle Architecture is designed following the classic three-tier architecture where the major part of business logic is located at Domain Tier as illustrated in Fig. 1. While Domain and Presentation tiers have not been changed with respect to Moodle Architecture, the Moodbile extension has created two tiers:

1. An External Tier where the actual services for mobile integration are defined. This layer can basically access methods from the standard LMS API.
2. A Connectors Tier consisting of connectors for supported web services communication protocols like SOAP and JSON-RPC. Each connector implements the translation of the services defined in the External Tier to the specific protocol. At the same time, this tier provides additional web services protocols and authentication methods more suitable for mobile devices, such as OAuth [24].
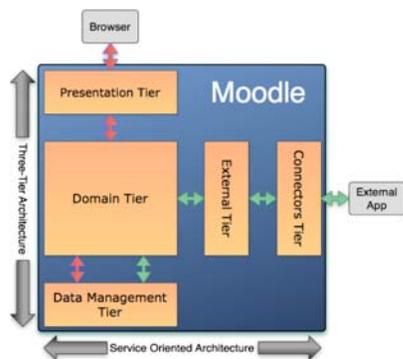

Fig. 1. Moodbile Web Services Architecture [14].

Therefore, Moodbile project is to provide an extension that would turn Moodle into a web services provider for mobile applications, with the design of a web-service layer to access most suitable Moodle features for mobile applications. However, while Moodbile serves as an excellent extension to Moodle to bring its widely adopted services, such as administration, documentation, delivery of e-learning courses or training programs, to the mobile world, it never touches the Moodle Quiz Engine which was originally coded using PHP in a way that makes it very difficult to be service oriented. Consequently, Moodle Quiz Engine can only be accessed through web browsers, not through mobile apps. Web browsers are not considered as reliable platforms to conduct exams on mobile/tablet devices; they are slow, prone to security vulnerabilities, and may shutdown for many reasons.

Security in e-learning for various environments in general has been well-considered in literature from early on [25], [26], [27]. Scholars have offered various protection measures against security threats originating from both the user side and the management side [28]. A significant component of e-learning processes is online exams. It is clearly desirable to simplify exam management such that all exam stages are performed electronically, so exams become e-exams. A number of e-exam systems for various purposes, ranging from custom adaptive systems [29] to commercial solutions [30], [31] have been developed. However, e-exams carry such unique and specific security issues that more of user-centered and technology-supported countermeasures need to be implemented [32], [33]. Frank [34] introduced a reference model based on types of risks that threaten integrity of e-exams and evaluated three commercial systems using this model.

The classical approach to perform e-exams involves providing specific exam centers equipped with machines configured with static security policy to be used only for exam purposes. This approach brings about the cost of creation and upkeep of the environment, and continuous underutilization thereof. Also, such policies cannot be applied in m-learning environments where the students' mobile/tablet devices are meant to be used for general purposes, e.g. Internet browsing or e-book reading, as well as for the sake of exams. Using students' mobile devices as exam stations offers the advantages of low cost, more exam takers at the same time, and no need for a wired network. Thus, a dynamic security policy is needed in this case with an appropriate enforcing mechanism. To the best of our knowledge, this issue has not yet been addressed by any previous work for the same environment.

Moodbile Project does not address the security and privacy issues related to conducting exams in m-learning environment, and neither does the Moodle Quiz Engine which emphasizes only on the learning process not on securing the examination process. The "Secure Exam Environment" described in [35] supports exams based on Moodle to be taken by students on laptops. The system denies access to local files and Internet, but allows the use of certain programs like Excel and Java applications. Students have to connect their laptops to the wired LAN and boot from a USB drive or DVD. Other e-exam systems developed based on mobile platforms with wireless access [36], [37] lack proper security considerations and exam management functions.

This paper aims to design a Secure Exam Management System (SEMS) that meets the distinct security require-

ments of m-learning environments and to integrate it with the current Moodle/Moodbile platform. This will result in a complete LMS that is both equipped with secure exam services and suitable for m-learning. Our intention of integrating SEMS with a well-known LMS such as Moodle is so to get the benefits of Moodle's ready-made services in other learning aspects such as course material administration, documentation, etc. which have been experienced and appreciated for the last 15 years. However, the proposed SEMS can also work as a standalone secure exam management system for m-learning environments without integration with Moodle.

The paper is organized as follows: Section 2 presents the core services and functionalities of SEMS Exam Engine. Section 3 introduces SEMS Security Agent that enforces the dynamic network access control on students' mobile devices during exams. Section 4 discusses various network issues that can affect the exam process. Section 5 is on SEMS integration with Moodle/Moodbile framework. Finally, Section 6 presents a survey conducted about SEMS.

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% 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.

2 SEMS Exam Engine Core Services and Functionalities

The Quiz Engine embedded in Moodle is not built based on Service Oriented Architecture. It is implemented as a bulk of PHP code which has to be accessed through standard web browsers that are a bit slow on mobile devices and cannot address the exam security issues that exist in m-learning environment. Moodbile services extension to Moodle does not touch the Moodle's Quiz Engine. Thus, we need to develop a new Quiz Engine that can be deployed as a service oriented application, so that its services can be consumed by a mobile application designed to cater to m-learning specific security requirements. As well, it should be integratable with Moodle/Moodbile in order to have a complete LMS which suites the m-learning environment and addresses all of its security issues. The core services of the proposed Exam Engine are discussed below.

2.1 Secure and Random Distribution of Exam Questions
This service provides the following functionalities:
1. Enabling the teacher to define a bank of exam questions and to link them to his/her subject through an appropriate interface (Subject's Ques-

tion Bank Interface). In case of objective kind of questions, each question may have a set of options. The teacher has to provide those options through the same interface and specify the correct choices among them to enable the exam engine to auto-evaluate students' answers. In case of descriptive kind of questions, a text box (or probably a sketching canvas) will appear below each question at the student device screen to allow him/her to write/draw the question's answer; those answers will be saved at server side to be further reviewed and evaluated by the teacher. In addition, each question will have a property to specify its difficulty "level" (let's say: A, B, C, D, and E).
2. Enabling the teacher to **specify a subject's exam properties** such as: Date and Time, Duration, Percentage of level A, level B, and level C questions in the exam paper, etc. through an appropriate interface (Subject's Exam Setup Interface).
3. **Securely authenticating and enrolling students**, using any of the well-known secure authentication mechanisms, into exams at the pre-defined date and time through the Exam Enrollment Interface. Multifactor authentication can be adopted for stronger security as explained in Section 2.4.
4. **Creating exam instances by random distribution of exam questions** to the enrolled students' mobile/tablet devices according to the predefined exam properties such as percentage of each question level. This means that questions are not going to reach students in the same order. Moreover, the multi-choices of each question, in case of objective questions, will be flipped randomly and delivered differently to each student. The Exam Server associates the exam questions with a message digest signed by its private key to ensure data integrity. The Exam Server also has to memorize the way it has distributed the questions to each student to be able to evaluate the correct answers once the students submit their answers back to the Exam Server. This process, illustrated in Fig. 2, guarantees that each student gets different questions order and makes cheating by "hand-signals" impossible. The prepared questions bank is reusable. Teachers can always enrich their courses' questions bank by adding new questions or upgrading old ones during the semester. At the exam time, it is the responsibility of the Exam Server to create exam instances out of the questions bank. Incorporating the "question level" concept helps the Exam Server to prepare a moderate kind of questions while selecting them out of the questions bank.
5. **Students answer the exam questions** through the Exam Client Software Interface. Their answers are then submitted to the Exam Server along with a signed message digest to ensure the integrity.
6. **Processing students' answers** to determine their grades in the test. The Exam Server has to evaluate students' answers according to the questions' correct solutions pre-defined by the teacher. Then it

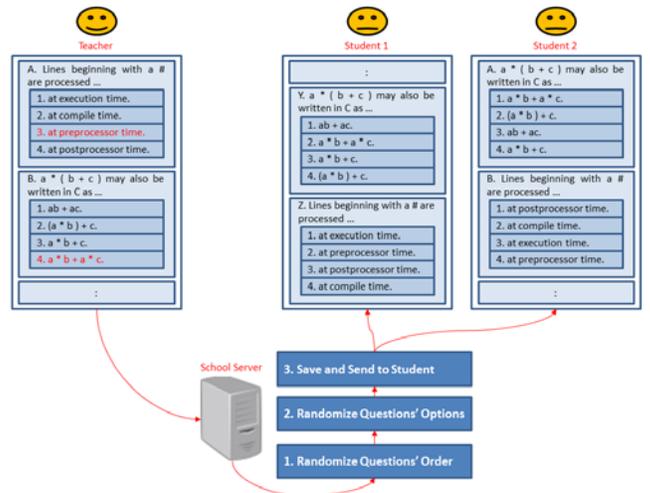has to generate the appropriate reports.

Fig. 2. Secure distribution of exam questions

7. **Reporting**: The Exam Engine has to generate a set of reports to enrich the assessment process, like:
   - Subject's Exam Report: It reflects statistical information about a particular exam (Students' Grades, Min, Max and Average Grade, etc.).
   - Student's General Report: It reflects general information about the performance of a particular student in the whole semester/year. It shows his/her scored marks in all subjects and calculates his/her GPA and other statistical values.
   - Teacher's Report: It shows the average performance of students in all the subjects given by a particular teacher.

2.2 Turbo-Mode Assessment

This service can be useful for conducting arbitrary quizzes during class time rapidly. It increases or decreases the level of the questions in a reactive manner. Assuming we have five levels of questions (A, B, C, D, and E), the Exam Server starts asking each student questions of level C. According to the student's answers, it increases or decreases the level of the questions in a reactive manner. As a result, student's level can be determined using fewer questions and in a shorter time (binary search).

2.3 Preventing the "Unattended Exam" Issue

In a Wi-Fi based network, we cannot guarantee that each student is going to attend an exam from a dedicated classroom. A student can simply sit in a nearby room and log in to the exam system through the Wi-Fi network. 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 be absent, 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 QR-Code based Strategy

This strategy is suitable for medium/large number of students where the proctor may not be familiar with all examinees. In this strategy the Exam Server has to generate a QR-code based exam access token for every student according to the following procedure:

1. The Exam Server generates an RSA public key pair specifically used to generate the exam access tokens as shown in Table 1.

TABLE 1
RSA KEY PAIR EXAMPLE

Private Key	Public Key
MIIBOQIBAAJBAMARFhSxzPrn5il4NZckWCogK DxE+XSW4QD+r2knvgCNyNXTPaWxvhUODW0 AHQxQ7djcPWL09mOu3kgp3nKOwBUCAwEAA QJAESo1v/m36QCKmFAu8egEnRcsoV5EsP++8hj Q0mQD3gal188UN+CAnGjBVyLsoTxm+GgtHPII8 230Osr2a5RyAQIhAP49pDGl2XmvCdKtOWm9zp D8ma5LPqfhK2bcsKSpapuVAiEAwWVPhWEm4J KKE1QywfxWCI4ljrzV//IPvdhXvFzWcoECIH9ryX UQmDSCY7vxEYtLk9Hap/NQxvBAzA3bobSFLGc ZAiB/CzqN+CA97oXd5LXjUQyDWj254rsCA9Xrd K9OAf6uAQIgGuYtTgJELqsE0JVR6s/1cJVJvGyYj d3p3E5gcleqdL4=	MFwwDQYJKo ZIhvcNAQEBB QADSwAwSAJ BAILwO/f1TLY mv5E10Iu50WZ TczpoOgLoRSJ dVUIOLbBFfon 6fyhpXrOTcfD8 L8MnpJzfiITovI +IRlDlWcX2eM sCAwEAAQ==

2. The Exam Server creates an exam access string for every student, as shown in Table 2.

TABLE 2
AN EXAM ACCESS STRING

Student #: 020313008, Subject: CE101, Room: A25, Seat No: 19

3. It then hashes the access string using SHA-1 to produce the message digest, as shown in Table 3.

TABLE 3
HASHED ACCESS TOKEN

206e83d0b62fe160c100f59554f9466510b0eb33

4. The Exam Server signs the access string message digest with its RSA Private Key to get a signed message as in Table 4.

TABLE 4
HASHED ACCESS TOKEN

S9Uv5+oefDTQBP4HOn7ZHNs7vv496kv6gFBTUehs6fSWsVZWKY1H GUk4GbP/29jFATUXX791V0xM1eGIdVQ4UQ==

5. Finally, the Exam Server generates the QR-Code of the signed access string to get the exam access token as shown in Table 5.

TABLE 5
AN EXAM ACCESS TOKEN

Student #: 020313008 Student Name: XXXXXXX Subject: CE101 Room: A25 Seat No: 19	

The Exam Server repeats steps 2-5 for all students involved in the exam. All access tokens, ordered by student numbers, are printed on a special paper which can be teared easily from the dash-line as depicted in Fig. 3. The proctor is given the access token list in the exam center before the exam.
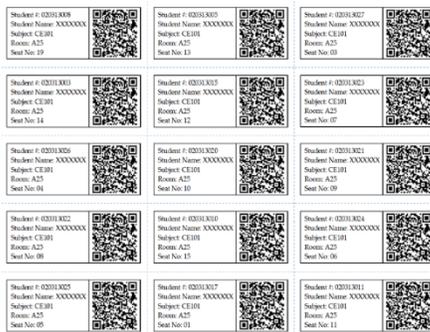

Fig. 3. List of exam access tokens.

A student gets into the dedicated exam room and obtains his/her access token from the proctor. After he/she signs into the exam system through the Exam Client Software (ECS) installed on the student's mobile/tablet device, ECS asks the student to present his/her access token in front of the mobile/tablet device camera. This process guarantees that no student can log in to the exam system from another room as access tokens are not distributed there. In case a student must leave the room for an emergency during the exam, he/she needs to submit his/her mobile device and access token to the proctor.

The process of distributing exam tokens can be auto-mated if the school can afford equipping every exam table with a Wi-Fi enabled, mini, black and white LCD screen (in the size of a hand watch screen).

2.3.3 NFC based Strategies
2.3.3.1 Network NFC Reader and NFC-Enabled Student ID Cards

In this strategy, the Exam Server signs every student's general information, such as student's number and name, using its Private Key. The generated signature is further stored on a write-once NFC-enabled ID card as the one shown in Fig. 4. On the other hand, every exam room is equipped with a simple wall-mounted network NFC Reader like the one depicted in Fig. 5.

Fig. 4. NFC-enabled ID card.

Once a student enters an exam room, he/she is supposed to swipe his/her NFC-enabled ID card on the network NFC reader of the exam room before he/she gets seated. When the student logs into the exam system, the Exam Server checks whether the exam's corresponding NFC reader has previously logged the student's signed information. This guarantees that the student is within the dedicated exam room.

Fig. 5. Network NFC reader [41].

This method, however, has a security flaw. A student may give his/her ID card to an accomplice and ask him/her to enter the class room and swipe the card over the NFC reader on his/her behalf. The accomplice may sit in the exam room idle allowing the student to log in to the system from a neighboring room (he/she will be allowed to log in because his/her card was swiped over the NFC reader). Here is the job of the proctor to ensure that every student who swipes his/her ID card over the NFC reader holds the same personal photo printed on the NFC card. The proctor may also investigate that every student in the exam room is really logged into the exam system by moving around and monitoring their mobile devices' screens.

2.3.3.2 Exam NFC Tag and NFC-Enabled Mobile Devices

In this strategy, the Exam Server generates a generic access string as shown in Table 6. It then signs the access string with its Private Key and stores the result on a write-once NFC tag as the one shown in Fig. 6. The proctor collects the NFC tag from the exam center and sticks it to a proper place in the dedicated exam room.

TABLE 6
EXAM GENERIC ACCESS STRING

Subject: CE101, Room: A25, Date: 30/04/2015

Fig. 6. NFC tag.

When a student enters the exam room, he/she will pass his/her NFC-enabled mobile/tablet device over the NFC tag. Then, ECS has to send the value read to get validated by the Exam Server before it allows the student to log in. If it is a bottleneck to ask all the students to swipe over a single tag, the Exam Server can generate 3-5 tags which can be distributed to different places in the dedicated exam room for simultaneous enrollment process.

NFC tags are extremely cheap; however, this strategy requires the students' mobile devices to be NFC-enabled. This is quite common in nowaday's mobile devices. Moreover, this NFC-based strategy does not have a security flaw unlike the previous strategy.

2.4 Providing an Appropriate Mechanism for Anti-impersonation

Student authentication for exam enrollment is a serious issue. Especially when there is a large number of students attending the exam and the proctor does not know all of them personally. A student may employ an impersonator, providing his/her credentials, to attend the exam on his/her behalf. To prevent impersonation, we recommend the adoption of a well-known biometric-based authentication technology, such as face recognition, to serve as a supplementary access key.

Authentication based on face recognition is a long standing problem that has been studied extensively and several well-established techniques have made it a very common authentication approach [30], [31], [42]. There are plenty of methods available in the literature which can be classified as template-based vs. geometric-based, appearance-based vs. model-based, holistic vs. piecemeal. Due to ever-increasing use of mobile devices, new algorithms for secure authentication on such devices attract considerable attention from research community [43], [44], [45].

Computational load imposed by the face recognition algorithms is generally one of the key issues. However, the current computational power of the mobile devices gives a pave to obtain a real-time application of face recognition. Extensive research effort is dedicated to improve the real-time performance of face recognizer by utilizing available embedded GPUs on mobile devices [46], [47], [48].

In SEMS, we plan to utilize the OpenCV library [49], which allows easier development of proven algorithms such as Eigenfaces, Fisherfaces, and Local Binary Pattern Histograms for face recognition. OpenCV supports exploiting parallel processing power of GPUs.

In the proposed system, a face recognition module will be integrated with the OAuth protocol as a second authentication factor. A student will firstly be authenticated using his/her own username and password, whereupon he/she will be prompted to take a proper pause in front of his/her mobile/tablet device camera. The software on the student's device will be responsible for capturing a proper face. Since current computational power of mobile devices allows us to implement feature extraction section of the face recognition, we propose to implement this section as a service on the mobile device. The extracted features will be sent to the Server to be compared against the student's registered face features and a confirmation will be sent back to the mobile device to approve student's identity.

Spoofing attacks are of concern with respect to face recognition security, but are taken into consideration by the research community [50], [51]. There are plenty of techniques such as liveness detection [52] and progressive authentication [53] which can be easily integrated in the face recognition module to counter-attack spoofing. Thus, we believe that face recognition is a usable, highly secure, and efficient biometric-based authentication mechanism that can be adopted as a second authentication factor.

2.5 Preventing Students from Exchanging Mobile/Tablet Devices during an Exam

Beyond all the enforced security mechanisms discussed earlier and those which are going to be discussed later on in this paper, students might still attempt to cheat by simply exchanging their mobile/tablet devices after they get authenticated by the Exam Server. To prevent this issue, ECS tries to re-authenticate the students biometrically by asking them to represent their faces in front of the mobile camera on a random basis. With this mechanism, students cannot exchange their devices during an exam after getting authenticated as the system at any point of time can ask them to represent their identity.

Moreover, the proctor software will have the functionality to force a particular student attending an exam to get re-authenticated by the system in case any suspicious case occurs. It can simply signal the corresponding student's ECS to re-initiate the authentication process. ECS will always respond to this signal coming from the exam's registered proctor device.

2.6 Following the Widely Accepted Industrial Standards

SEMS Exam Engine must conform to a well-known and widely-adopted set of standards and specifications developed by IMS Global Learning Consortium (IMS-GLC) [54]. IMS-GLC is a specification authoring organization comprised of distributed computer learning system vendors, publishers, digital content vendors, government agencies, universities, training organizations, and other interested parties. It is a global and non-profit member organization supported by over 190 of the world's leaders in educational and learning technology. It has approved and published some 20 standards that are the most widely used learning technology standards in higher education around the globe. These include meta-data, content packaging, enterprise services, question & test, competen-

cies, tools interoperability, sharable state persistence, vocabulary definition, and learning design. All IMS-GLC standards are available free of charge 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 results data between authoring tools, item banks, test constructional tools, learning systems, and assessment delivery systems.

The standard question types (e.g. multiple choice, fill in the blank, or true/false choice) are constructed in QTI specification using a core set of presentation and response structures, and results of questions are collected and scored by using a variety of methods. To represent these options, the QTI specification defines the 'Item'. Items contain all the necessary data elements required to compose, render, score, and provide feedback from questions. Therefore, the key difference between a 'Question' and 'Item' is that an 'Item' contains the 'Question', layout rendering information, the associated response processing information, and the corresponding hints, solutions, and feedback. Similarly, the 'test' is an instance of an Assessment. Assessments are assembled from Items that are contained within a 'Section' to resemble a traditional test. Additionally, Assessments might be assembled from blocks of Items that are logically related. These groups are also defined as 'Sections' and so Assessments are composed of one or more Sections which themselves are composed of Items, or more Sections. Collectively, these three data objects are referred to as the ASI (Assessment, Section, and Item) structures. These evaluation objects can be bundled together to create an object bank. An object bank can then be externally referenced and used as a single evaluation object. To avoid limitations associated with words like user, student, or learner the IMS QTI working 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.

As an example, to assess whether a participant knows that the capital of Turkey is Ankara, an item can be constructed to pose the simple question "What is the capital of Turkey?" and then present a list of cities as multiple-choice selections. Alternatively, the item could contain the additional information required to render a map of Turkey along with the list of cities. The participant could be asked to mark the map where Ankara is located rather than simply identify the city. In turn, a Section could be composed of many world capital multiple-choice questions. Similarly, the Assessment could consist of a set of Sections focused on assessing a participant's knowledge of geography in general. QTI specification is defined in XML to promote the widest possible adoption.

3 SEMS SECURITY AGENT

Students' mobile/tablet devices are connected to the school's Wi-Fi network through which they may illegally exchange information during an exam. Applying simple policies, such as turning the network down during exams to cut off any possible communication between students, is not a practical solution as students in different classes may not take their exams at the same time. Moreover, the network has to be up during exams in order to be able to submit students' answers to the Exam Server. A dynamic network access policy has to be generated and applied on each student's device according to predefined conditions. Employing an identity based firewall with dynamic access policy seems to be a good solution to be adopted in such a scenario. However, it has the following limitations:

1. It is a centralized software which cannot block ad-hoc Bluetooth communications between students' mobile/tablet devices, neither can it block the regular cellular communications.
2. It cannot address certain issues such as the "**unattended exam**" issue discussed in Section 2.3. For such special issues we need a protocol specifically designed for m-learning environments.
3. It cannot prevent the students from opening offline PDF files, which have been previously downloaded into students' mobile devices and can be accessed offline without the need for a network approval.
4. Firewalls can be surpassed by advanced VPN technologies such as those depending on StealthVPN [55] techniques.

SEMS proposes its Security Agent (SA) to encounter all of the aforementioned issues. It is the core secure component through which SEMS enforces the dynamic network access policy in m-learning environments. SA offers various strategies for different scenarios.

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 (discussed in Section 3.3) 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. Fig. 7 illustrates this strategy.

In case ECS finds that any of the network communication has been re-enabled manually during the exam, it will re-block, give an alarm sound, and report this situation to the Exam Server once the secure channel is re-established.
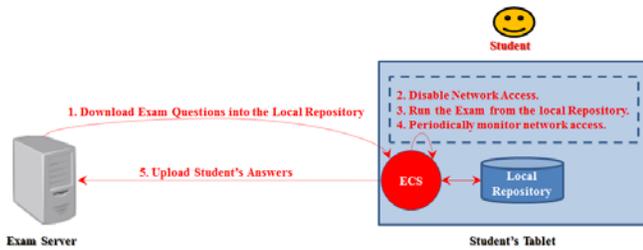
Fig. 7. Offline exam strategy.

3.2 Online Exam Strategy

In this strategy, students attend the exam through a secure and online channel established with the Exam Server. This strategy has more advantages over the offline one. For example, it allows students to access a shared library of e-books or a set of related websites pre-specified by the teacher for an open-book exam scenario. On the other hand, enforcing exam security becomes a challenge in such an open environment.

In this case, the system has to adopt a dynamic network access control through which it can create and enforce 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 be blocked except the main connection to the Server through which the student is to submit answers to questions or access the exam's shared library.

To enforce such policies, SEMS SA is introduced. It is a software agent installed on students' mobile/tablet devices and responsible for downloading the dynamic network access policies from the Exam Server and for enforcing them on students' mobile/tablet devices.

This agent is connected to the Exam Server via a predefined secure channel (discussed in Section 3.3) through which it is going to download the dynamic network access policy. To ensure that students are not going to shut this agent down in an attempt to break the enforced access policy, SA keeps sending a periodic heart-beat signal through the same secure channel to the Exam Server as illustrated in Fig. 8. Should the Exam Server stop receiving this signal for a predefined period, it logs this event and sends an immediate alert to the teacher/proctor associated with the exam to check out the issue.
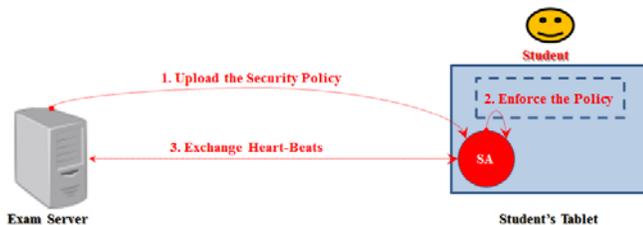

Fig. 8. Online exam strategy.

Different approaches can be adopted to implement SA in online exam strategy.

3.2.1 Separate ECS Thread

SA can be implemented as a separate thread in ECS (Fig. 9). This can guarantee that the student cannot shut SA down unless he/she shuts down ECS itself in which case his/her exam will be terminated.

This strategy eliminates the need to exchange periodic heart-beats between the Exam Server and SA, but it limits the functionality of SA to exam time only.
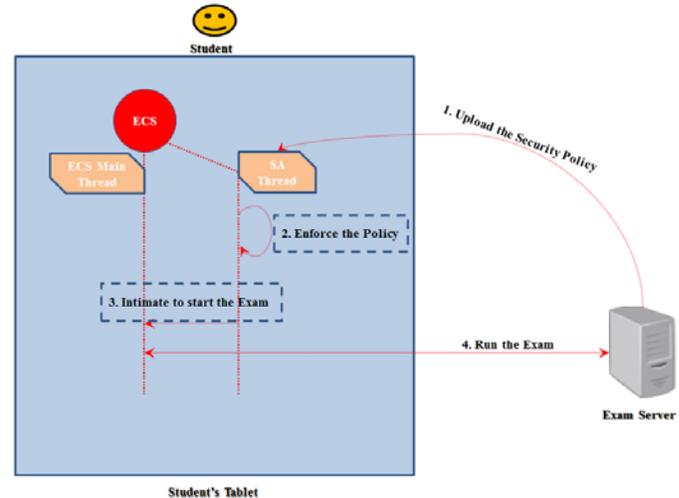

Fig. 9. SA as a separate ECS thread.

3.2.2 Independent Agent Software

This approach implements SA as an independent software component (Fig. 10), i.e. as a different process from that of ECS. This requires the heart-beats to be exchanged with the Exam Server in order to ensure that the agent is operating properly. On the other hand, it offers more functionalities compared to the previous approach. SA can be designed to be a continuously running process, even outside the exam time. It can then be configured to gather important statistical information about students' different activities on their mobile/tablet devices (how long they spend on reading their courses' e-books, what kind of apps they run on their devices, what kind of websites they visit, etc.). This information helps to create a feedback for parents and teachers regarding the students' activities which facilitates analyzing the students' status better especially for those at elementary/preparatory school level. Auditing students' activity service is discussed in Section 3.5.
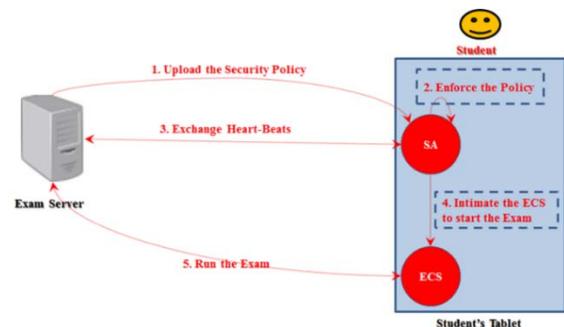

Fig. 10. SA as an independent agent software.

We suggest adding another functionality in SA that needs to be auto-activated during an exam in order to guarantee the enforcement of the downloaded dynamic security policy: a **periodic screen capture**. If such a functionality is enabled, all the student's actions on his/her mobile device during exam time can be recorded and stored at the Server (let us say for a couple of weeks after an exam) for further assessment in case of any suspicious case.

3.3 Establishing the Secure Channel with the Exam Server

A critical issue that needs to be addressed properly in the aforementioned protocol is how to establish the secure channel between the Exam Server and the Security Agent in the student's mobile device. 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 to maintain its own shared key only. To securely negotiate the shared key, we propose the following protocol:

1. The student gets his/her mobile/tablet device from the students' registration office. The device ID will be associated with the student's ID in the Server's database before delivering the device to the student. The student has to get his/her default login credentials (username/password) from the students' registration office as well.

2. The student has to first log in to the system through his/her personal computer or through a dedicated computer in the students' registration office. He/she will be prompted to change the default password and then to re-log in to the system.

3. The student's account page has a link named "Mobile Device Activation". He/she has to click on that link for the Server to internally generate a **Master Shared Key (MSK)** and associate it with the device ID of the student's mobile/tablet device in the Server's database. Then, the shared key will be embedded into a barcode presented on the student's account screen (Fig. 11 shows the shared secret key **MA4Q-EUH5-BA7U-XYZC** embedded into a barcode). Student needs to open ECS software installed on his/her mobile/tablet device, go to "Settings", select "Set up the Secure Channel", click on "Scan a Bar Code" and then use his/her mobile/tablet's camera to scan the presented barcode so that ECS software can learn MSK.

Fig. 11. Secret Shared Key embedded in a bar code

Sharing a secret key based on barcode is an industry standard used by "Google Authenticator"

and "WinAuth" implementation of the TOTP authentication protocol [56]. As the key is presented in a barcode format, it is secured against any kind of shoulder surfing attack [57] and, in addition, the burden of entering a complex key manually into the student's device has been removed.

4. Once the aforementioned registration and activation process has been completed, a secure channel between the Exam Server and the student's mobile/tablet device can be established at the beginning of an exam through the protocol depicted in Fig. 12. The figure is drawn for "**Separate ECS Thread**" scenario of SA explained earlier in Section 3.2.1. A similar one can be used for other scenarios.
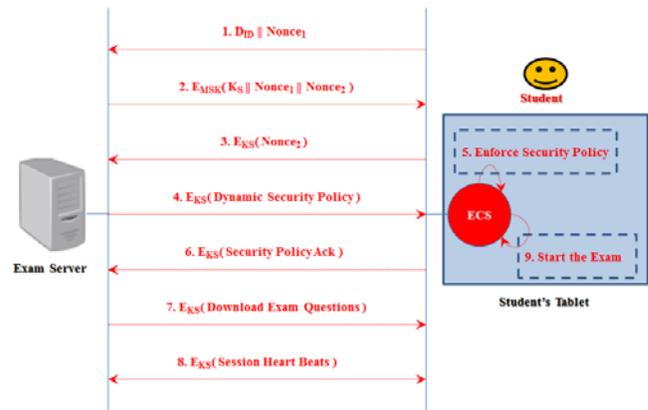

Fig. 12. Establishing the secure channel.

The first 3 steps perform the following:

- (ECS ↔ Exam Server) mutual authentication where $Nonce_i$ serves as a random challenge.
- Negotiate the specific session key (KS) using MSK.

E_{MSK} is a strong symmetric encryption function, such as AES-128, as we need to keep MSK secure enough. While E_{KS} is a medium strength encryption function, such as DES, it is going to be used solely for this exam session and there is no harm of exploiting it later on because security is needed only during exam time, not afterward. Using medium strength encryption function decreases the burden on the mobile/tablet device while exchanging the heart-beats with the Exam Server as mobile devices have limited computing power.

We could have used the standard Secure Sockets Layer (SSL) protocol, as an alternative mechanism, to create the secure session. However, SSL is generally a PKI based protocol and it is inefficient to use the public-key crypto systems to exchange periodic heart-beats on a mobile/tablet device as PKI operations are well-known to be expensive processes. However, one can apply the initial stages of SSL just to negotiate a symmetric session key. Afterwards, the heart-beats can be exchanged using symmetric crypto system. This can be done efficiently if the mobile devices are configured to accept the Exam Server's self-signed PKI certificate as a trusted certificate

for SSL protocol.

3.4 Enforcing the Downloaded Security Policy on the Students' Devices

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

Android is built based on Linux kernel where its iptables can be used as an effective and light weight firewall. *iptables4A* is an interface developed to interact with Linux iptables on Android [58]. We have tested the iptables script shown in Table 7 on Samsung Galaxy Tab 2 with Android 4.0.4 installed. The script has succeeded in blocking any network communication going out of the tablet except those communications with the specified Server-IP.
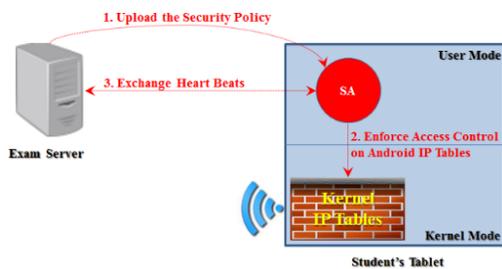

Fig. 13. Enforcing access control.

TABLE 7
ANDROID IP-TABLES SCRIPT

#iptables –A OUTPUT –d <Server-IP> -j ACCEPT
#iptables –A OUTPUT –j REJECT

The issue with *iptables4A* interface is that it requires a root access. We can handle this issue in three ways:

1. By installing a custom Android ROM bundled with SEMS' APK on all students' mobile/tablet devices.
2. By rooting all students' devices before installing SEMS' APK on them and subsequently giving SEMS' APK root access privilege on each device.
3. By using the Device Administration API which offers the ability to give applications specific administrative rights without the need for any superuser permissions; it only needs the corresponding device administration rights properly defined in a resource file like the one shown in Table 8. This seems to be the easiest and the most suitable way to grant SEMS' APK with the required privileges. Currently, however, Device Administration API does not support access to iptables.

TABLE 8
DEVICE ADMINISTRATION API RESOURCE FILE EXAMPLE

```
<device-admin
xmlns:android="http://schemas.android.com/apk/res/android">
 <uses-policies>
  < The Required Device Administrator Rights/>
 </uses-policies>
</device-admin>
```

Instead of iptables, SA can create a VPN and divert all traffic on student's mobile device through it during an exam. This way, it can choose which traffic to allow and which to stop through its VPN. However, it also needs to keep checking that its VPN is in active state during exams. This approach does not require rooting and is more applicable to other smart platforms where iptables is not in-built. NoRoot Firewall [59] uses a similar methodology.

3.5 Auditing Students' Activities (optional)

SA functionalities can further be extended to track students' smart device usage and activities. The agent's main task is not to spy on students but rather to analyze the efforts being made by the students and give suggestions to their teachers/parents in order to encourage students to improve their efforts so to accomplish better results.

This functionality can be more appropriate for for students of elementary school level where parents really need to keep eyes on their children while they are exploring the virtual world through their smart devices. The parameters to be monitored can differ from age to age and may have to be specified according to the national law. This service is made optional so it can be disabled as desired.

A thread of SA is registered in the system as a broadcast receiver (BR) to listen to various events occurring in the system. The receiver gets notified by the Android system if any pre-specified event occurs. It creates offline-logs about different events occurred in the system and sends them to the Server once a channel is established. The recorded events can be "course's e-book reading", "assignment writing", "internet browsing", "game playing", etc.

The Server processes the logs received whereupon it provides comprehensive reports about students' activities. This information can be exported as a PDF or an Excel document. Teachers/parents can specify the events to be monitored by the agent according to their experience. Fig. 14 illustrates the auditing service architecture.
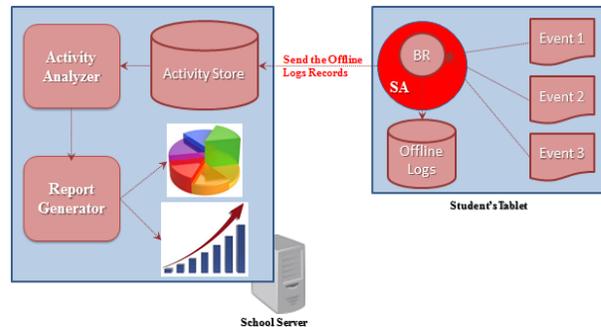

Fig. 14. Auditing student's activities.

4 NETWORK RELATED ISSUES

4.1 Network Overload

Most wireless access points can serve up to 255 devices connected at a time. This seems to be good enough to

conduct an exam. In case there are more students, we can deploy specific wireless routers that can support more devices connected simultaneously. We can also deploy multiple overlapped access points in high density areas and design the access point placement such that each device always sees two to 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. NETGEAR has given 10 design recommendations for high density areas [60].

4.2 Occasional Network Failures

SEMS has to be immune against occasional network failures. As discussed earlier, the Exam Server creates an exam instance for every student. This instance is identified by a unique id, let it be the corresponding student's id. The Exam Server has to keep track of the status of each established instance. Should a network issue occur, say the network goes down for a while, SA makes sure that the mobile/tablet device's Wi-Fi adapter is still active so the issue is not because the student has forcefully deactivated it in order to connect to another network, such as the mobile 3G network, attempting to use Internet illegally during the exam. 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 session has failed due to a network issue not due to a security violation by the student.

4.3 Using Alternative Mobile Devices to Exchange Information during an Exam

A student may bring two mobile devices, sign into the exam system using one of them and then use the other one where SA intuitively is not functioning, to exchange information with his/her colleague during exam. 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 use username and password in order to connect to the Wi-Fi network rather than using a single passphrase for all.
- Apply a security policy on the authentication server which ensures that a student can sign into the network via a single mobile device only.

We are using this policy in our university to restrict network access and maintain the bandwidth. However, a student may still communicate through another mobile device over a mobile data network, not through the school's Wi-Fi network. This violation can also be avoided by any of the following ways:

- Using a cell phone jammer [61], a device that can block cell phone signals while allowing Wi-Fi. Some countries prohibit the use of a cell phone jammer as it may cause disturbance to cell phone communications in the area nearby the exam room. However, there are mini-jammers that can block the use of cell phones within a very limited radius (e.g. 2-8 meters [62]). This kind of limited usage might become legal in many countries especially when such exam environments get more popular.
- Using a cell phone detector [63], a device that can detect the RF signature of common cell phones including LTE, AWS, PCS, CDMA/WCDMA (UMTS), GSM, EGSM, GPS, and even U.S. DECT 6.0 cordless phones, wherever cell phone jammers are prohibited.

4.4 Using a Wi-Fi Jammer to Bring the Wi-Fi Network Down

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 analyzer [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.

As far as SEMS is prepared to tackle network failures by the procedure mentioned in Section 4.2, an exam can be pursued after detecting the jam source and dealing with it.

5 SEMS INTEGRATION WITH MOODLE/MOODBILE SERVICE FRAMEWORK

Fig. 15 shows SEMS integration with Moodle framework and its service extension Moodbile. Moodle is an open source and widely accepted LMS. Integrating SEMS with Moodle helps to make use of its ready-made and well-tested services in other aspects of e-learning that are not related to exam security such as administration, documentation, tracking, reporting and delivery of electronic educational technology [67].

Moodle is designed following the classic three-tier architecture. Presentation Tier is meant for the interaction between a user and Moodle through a web browser. The majority of business logic is located at Domain Tier. Data Management Tier provides database related functionality such as storing or retrieving information.

As discussed earlier, Moodle is implemented as a bulk of PHP code that can be consumed through web browsers only. This makes it impractical for mobile client apps to access Moodle services. To make Moodle functionalities

consumable through mobile apps, Moodbile Project proposed the architecture shown in Fig. 1 [14]. Presentation and Domain Tiers have not been changed in the existing Moodle Architecture. Instead of refactoring both tiers, the External Tier was created where the actual services for mobile integration are defined.

To provide full support to the most widespread web services protocols, the Connectors Tier was designed. This tier contains specific components that adapt service specifications of the External Tier to the provided protocols. At the same time, this tier handles authentication and session management. Protocols supported are REST, SOAP, XML-RPC, and AMF among others.
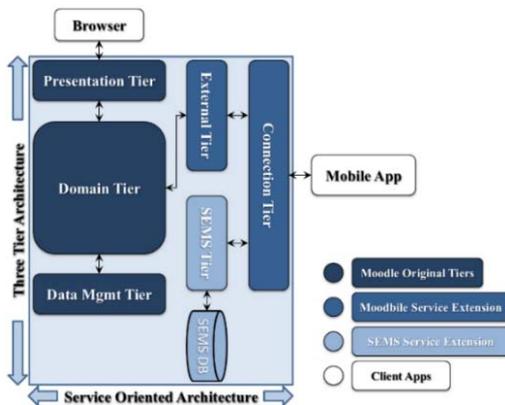

Fig. 15. SEMS integration with Moodle/Moodbile framework.

SEMS services are all to be implemented using Service Oriented Architecture so they do not need the External Tier services. For that, an independent layer is created beside the External Tier where all of the discussed SEMS services are implemented. Additionally, SEMS database is created to store and manage SEMS data.

The final architecture, shown in Fig 15, is an open-source LMS that supports a wide range of clients, from basic web browsers to mobile apps. It includes all learning services and functionalities, from documentation to conducting exam services. It suits both e-learning and m-learning environments.

6   EXPERIENCES AND OUTLOOK

To evaluate the stakeholders' potential of interest in SEMS, two different surveys were prepared, made online, and analyzed by means of Google Docs. The surveys used a 5-point Likert-type scale, i.e. (1) Strongly disagree – (5) Strongly agree, and consisted of four questions for students and seven questions for teachers as listed in Table 9 and Table 10, respectively.

TABLE 9
STUDENTS' SURVEY

Q. No.	Q. Text
1	I would prefer using SEMS for taking an exam over a paper-based exam.
2	I would feel comfortable using SEMS.
3	My grade would be determined better by using SEMS.

4	Using SEMS would prevent cheating more effectively, hence evaluate my performance fairly.

TABLE 10
TEACHERS' SURVEY

Q. No.	Q. Text
1	I would prefer using SEMS for conducting an exam over a paper-based exam.
2	Using SEMS would be helpful in conducting exams.
3	Using SEMS would greatly improve the evaluation process.
4	SEMS's user interface is friendly and easy to use.
5	Learning how to operate the system will be easy for me.
6	The students can accept and like the system.
7	Having face recognition as a second authentication factor increases my confidence on the system.

122 students and 17 teachers provided feedbacks after having sessions about SEMS services and specifications. Due to the high percentage of positive opinions (i.e. either "Agree" or "Strongly agree") in all the items, we can conclude that the overall attitude of stakeholders is very favorable. The responses from students and teachers show that they are enthusiastic about using SEMS for exams instead of dealing with paper-based exams (Q_1). 73% of the students expressed positive opinions and similarly high percentage (76%) of positive opinions came out of teachers' response. The teachers' responses to Q_2 and Q_3, which are related to benefiting from SEMS, are such that the vast majority of them responded positively. The students think that they would feel comfortable in using SEMS and they believe their grade would be better determined, with 69% and 66% of responses being positive, respectively. Also, almost all teachers think that "the students can accept and like the system". 75% of teachers stated that having face recognition as an additional authentication factor would increase their confidence on the system. Teachers seem to have liked SEMS specifications, feeling little apprehension towards learning to use the system (Q_4 and Q_5).

Fig. 16 and Fig. 17 depict the survey results. The highly positive attitude of the stakeholders overall indicates that SEMS will be readily accepted for use in m-learning.
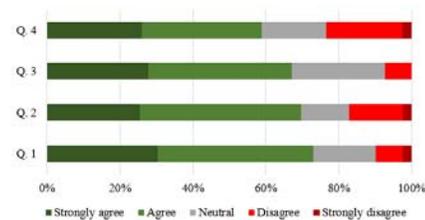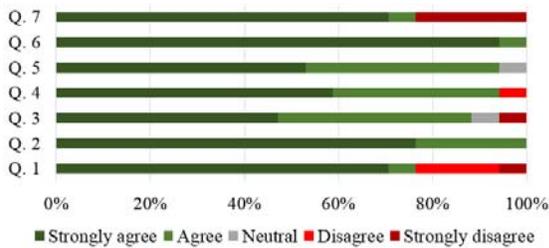

Fig. 16. Students' responses.

Fig. 17. Teachers' responses.

7 CONCLUSION

This paper proposes the design of a Secure Exam Management System (SEMS) to mitigate the unique exam security threats that exist in m-learning environments. SEMS offers many exam services such as: secure and random distribution of exam questions, turbo-mode assessment, prevention of the "unattended exam" issue, biometric-based authentication service for anti-impersonation, preventing students from exchanging their devices during an exam, conducting exam securely through online or offline strategies, and auditing.

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.

SEMS is integrated with an open source and widely accepted LMS, namely Moodle and its Moodbile service extension. The resulting design is a complete LMS with secure exam services that can be consumed by legacy systems through web browsers as well as by m-learning systems. Finally, a survey conducted reveals that overall attitude of students and teachers towards SEMS is very favorable.

REFERENCES

[1] "Think Act - Corporate Learning Goes Digital," *Roland Berger Strategy Consultants*, https://www.rolandberger.com/media/pdf/Roland_Berger_TAB_Corporate_Learning_E_20140602.pdf. May 2014.

[2] "2014 Training Industry Report," *Training Magazine*, http://www.trainingmag.com/sites/default/files/magazines/2014_11/2014-Industry-Report.pdf. Nov/Dec 2014.

[3] M.P. Prendes, "PLATAFORMAS DE CAMPUS VIRTUAL CON HERRAMIENTAS DE SOFTWARE LIBRE: Análisis comparativo de la situación actual en las universidades españolas," *Informe del Proyecto EA-2008-0257 de la Secretaría de Estado de Universidades e Investigación*, 2009.

[4] G. Yamamoto and C. H. Aydin, "E-Learning in Turkey: Past, Present and Future," *e-Learning Practices*, vol. 2, MidaseBook, 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*, May 2008.

[6] "Learning Management Systems Market by Users - Worldwide Market Forecasts and Analysis 2013 – 2018," *MarketsandMarkets*, http://www.marketsandmarkets.com/Market-Reports/learning-management-systems-market-1266.html. Oct. 2013.

[7] 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.

[8] "Ericsson Mobility Report," *Ericsson Inc.*, http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-june-2014.pdf. Jun. 2014.

[9] N. Sclater, "Web 2.0, Personal Learning Environments, and the Future of Learning Management Systems," *Research Bulletin*, vol. 2008, no. 13, Jun. 2008.

[10] S. Downes, "E-learning 2.0," *e-Learn Magazine*, http://elearnmag.acm.org/featured.cfm?aid=1104968. Oct. 2005.

[11] 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.

[12] 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.

[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 Learning & Organisation*, vol. 7, no. 1, pp. 66-80, 2013.

[14] 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.

[15] L. Naismith, P. Lonsdale, G. Vavoula, and M. Sharples, "Literature Review in Mobile Technologies and Learning," *FutureLab Report*, 2004.

[16] M. Sharples, J. Taylor, and G. Vavoula, "Towards a Theory of Mobile Learning," *Proc. mLearn Conf.*, pp. 1-9, Oct. 2005.

[17] R.S. Cobcroft, S. Towers, J. Smith, and A. Bruns, "Mobile learning in review: Opportunities and challenges for learners, teachers, and institutions," *Proc. Online Learning and Teaching (OLT) Conf.*, pp. 21-30, 2006.

[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 Technologies*, vol. 1, no. 1, pp. 40-41, 2007.

[19] M. Alier, M.J. Casañ, M.A. Conde, F.J. García-Peñalvo, and C. Severance, "Interoperability for LMS: The Missing Piece to Become the Common Place for Elearning Innovation," *Int. J. Knowledge and Learning*, vol. 6, no. 2, pp. 130-141. 2010.

[20] E. R. Weippl, "Security Considerations in M-learning: Threats and Countermeasures," *Advanced Technology for Learning*, vol. 4, no. 2, pp. 99-105, Jan. 2007.

[21] Z. Ugray, "Security and Privacy Issues in Mobile Learning," *Int. J. Mobile Learning and Organisation*, vol. 3, no. 2, pp. 202-218, Apr. 2009.

[22] Modular Object-Oriented Dynamic Learning Environment, https://moodle.org/.

[23] Moodbile Project, https://code.google.com/p/moodbile/.

[24] E. Hammer-Lahav, "The OAuth 1.0 Protocol," *Internet Engineering Task Force (IETF)*, https://tools.ietf.org/html/rfc5849. Apr.

2010.

[25] R. Raitman, L. Ngo, N. Augar, and W. Zhou, "Security in the Online E-learning Environment," *Proc. 5th IEEE Int. Conf. on Advanced Learning*, pp. 702-706, Jul. 2005.

[26] E. Weipple and M. Ebner, "Security & Privacy Challenges in E-Learning 2.0," *Proc. E-Learn*, pp. 4001-4007, Nov. 2008.

[27] N.H.M. Alwi and I. S. Fan, "E-Learning and Information Security Management," *Int. J. Digital Society*, vol. 1, no. 2, pp. 148-156, Jun. 2010.

[28] Y. Chen and W. He, "Security Risks and Protection in Online Learning – A Survey," *Int. Rev. Res. Open Distance Learn.*, vol. 14, no. 5, pp. 108-127, Dec. 2013.

[29] M. Yagci and M. Ünal, "Designing and Implementing an Adaptive Online Examination System," *Procedia - Social and Behavioral Sciences*, vol. 116, pp. 3079-3083, Feb. 2014.

[30] Webassessor & Kryterion Online Proctoring, *Kryterion Inc.*, http://www.kryteriononline.com/.

[31] Securexam & Remote Proctor, *Software Secure Inc.*, http://www.softwaresecure.com/.

[32] E. Marais, D. Argles, and B. Solms, "Security Issues Specific to e-Assessments," *8th Ann. Conf. on WWW Applicat.*, Bloemfontein, Sep. 2006.

[33] K. M. Apampa, G. Wills, and D. Argles, "User Security Issues in Summative E-assessment Security," *Int. J. Digital Society*, vol. 1, no. 2, pp. 135-147, Jun. 2010.

[34] A. J. Frank, "Dependable Distributed Testing – Can the Online Proctor be Reliably Computerized?," *Proc. 2010 Int. Conf. on e-Business*, Athens, pp. 22-31, Jul. 2010.

[35] G. Frankl, P. Schartner, and G. Zebedin, "Secure Online Exams Using Students' Devices," *IEEE Global Eng. Education Conf. (EDUCON)*, Marrakech, pp. 1-7, Apr. 2012.

[36] G. Meletiou, I. Voyiatzis, V. Stavroulaki, and C. Sgouropoulou, "Design and Implementation of an E-exam System based on the Android Platform", *16th Panhellenic Conf. on Informatics*, pp. 375-380, Oct. 2012.

[37] P. K. Gupta, M. Madan, K. Puri, and A. Gulati, "Student Oriented Mobile Based Examination Process," *Int. Conf. on Parallel, Dis-tributed and Grid Computing*, pp. 280-284, Dec. 2014.

[38] Android Market Share, http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

[39] Open_Handset_Alliance, https://en.wikipedia.org/wiki/Open_Handset_Alliance.

[40] Fatih Project, https://en.wikipedia.org/wiki/Fatih_project.

[41] FunkyGate-IP NFC, *SpringCard Inc.*, http://www.springcard.com/en/products/funkygate-ip-nfc.html.

[42] A. Gioeli, "Biometrics and the future of enterprise ID management," *Biometric Technology Today*, vol. 3, pp.8-10, 2015.

[43] MOBIO - Mobile Biometry, Secured and Trusted Access to Mobile Services, *European Funded Project (FP7-2007-ICT-1)*, http://www.mobioproject.org/.

[44] R. Amin, T. Gaber, G. ElTaweel, and A. E. Hassanien "Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues," *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*, Springer, pp. 423-446, 2014.

[45] Z. Xu, T. Zhang, Y. Zeng, J. Wan and W. Wu, "A Secure Mobile Payment Framework Based On Face Authentication," *Proc. Int. MultiConference of Engineers and Computer Scientists* (IMECS), Mar. 2015.

[46] S. Yi, I. Yoon, C. Oh, and Y. Yi, "Real-time Integrated Face

Detection and Recognition on Embedded GPGPUs," *IEEE 12th Symp. on Embedded Syst. for Real-time Multimedia* (ESTIMedia), pp. 98-107, Oct. 2014.

[47] G. Wang, Y. Xiong, J. Yun, and J. R. Cavallaro, "Accelerating Computer Vision Algorithms using OpenCL Framework on the Mobile GPU - a Case Study," *IEEE Int. Conf. on Acoustics, Speech, and Signal Process.* (ICASSP), May 2013.

[48] A. El-Mahdy and R. Elsersy, "A Large-Scale Mobile Facial Recognition System Using Embedded GPUs," *Proc. 22nd High Performance Computing Symposium,* pp. 23, Apr. 2014.

[49] FaceRecognizer - Face Recognition with OpenCV, http://docs.opencv.org/modules/contrib/doc/facerec/facerec_api.html.

[50] N. Evans, S.Z. Li, S. Marcel, and A. Ross, "Guest Editorial: Special Issue on Biometric Spoofing and Countermeasures," *IEEE Trans. Information Forensics and Security,* vol. 10, no. 4, pp. 699-702, Apr. 2015.

[51] D.F. Smith, A. Wiliem, and B.C. Lovell, "Face Recognition on Consumer Devices: Reflections on Replay Attacks," *IEEE Trans. Information Forensics and Security*, vol. 10, no. 4, pp. 736-745, Apr. 2015.

[52] A. F. Sequeira, J. Murari, and J.S. Cardoso, "Iris Liveness detection Methods in Mobile Applications," *Proc. Int. Conf. on Comput. Vision Theory and Applicat.* (VISAPP), Jan. 2014.

[53] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive Authentication: Deciding When to Authenticate on Mobile Phones," *USENIX Security Symp.*, pp. 301-316, Aug. 2012.

[54] IMS Global Learning Consortium, http://www.imsglobal.org/.

[55] StealthVPN, http://wiki.astrill.com/index.php/Astrill_Setup_Manual:VPN_Protocols_supported_by_Astrill#StealthVPN.

[56] D. MRaihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," *Internet Engineering Task Force (IETF)*, https://tools.ietf.org/html/rfc6238, May 2011.

[57] Shoulder surfing, https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security).

[58] IP Tables for Android, https://play.google.com/store/apps/details?id=jp.ymatsumoto.iptables2.

[59] NoRoot Firewall, https://play.google.com/store/apps/details?id=app.greyshirts.firewall.

[60] "Best Practices for High Density Wireless Network Design in Education and Small/Medium Businesses", *NETGEAR Inc.*, http://www.netgear.com/images/pdf/High_Density_Best_Practices.pdf.

[61] Handheld Cellphone Jammer TG-120B-PRO, *Tangreat Inc.*, http://www.tangreat.com/en/product-detail-57.html, 2015.

[62] Mini Portable Cellphone Jammer J-260A, http://www.jammer4uk.com/mini-portable-cellphone-jammer-j260a-p-5.html.

[63] Wolfhound-PRO Cell Phone Detector, https://www.bvsystems.com/product/wolfhound-pro-cell-phone-detector/, 2015.

[64] Wi-Fi and Bluetooth Jammer TG-120C-PRO, *Tangreat Inc.*, http://www.tangreat.com/en/product-detail-58.html, 2015.

[65] AirMagnet Enterprise, *Fluke Networks Inc.*, http://www.flukenetworks.com/enterprise-network/wireless-network/AirMagnet-Enterprise, 2015.

[66] T. Zhang, A. Patro, N. Leng, and S. Banerjee, "A Wireless Spectrum Analyzer in Your Pocket", *Proc. 16th Int. Workshop on Mobile Computing Systems and Applications*, pp. 69-74, Feb. 2015.

[67] R.K. Ellis, "A Field Guide to Learning Management Systems,"

ASTD   Learning   Circuits,   https://www.td.org/~/media/Files/Publications/LMS_fieldguide_20091, 2009.