Secure Examination Management System for M-Learning (SEMS)

Akshada Abnave, Charulata Banait
Computer Department
D Y Patil College of Engineering
Savitribai Phule Pune University
Pune, India

Mrunalini Chopade, Supriya Godalkar
Computer Department
D Y Patil College of Engineering
Savitribai Phule Pune University
Pune, India

Soudamini Pawar, Vidya Nikar
Computer Department
D Y Patil College of Engineering
Savitribai Phule Pune University
Pune, India

ABSTRACT
M-learning or mobile learning is defined as learning through mobile apps, social interactions and online educational hubs via Internet or network using personal mobile devices such as tablets and smart phones. However, in such open environment examination security is most challenging task as students can exchange mobile devices or also can exchange information through network during examination. This paper aims to design secure examination management system for m-learning and provide appropriate mechanism for anti-impersonation to ensure examination security. The users are authenticated through OTP. To prevent students from exchanging mobile devices during examination, system re-authenticates students automatically through face recognition at random time without interrupting the test. The system also provides external click management i.e. prevent students from accessing online sites and already downloaded files during examination.

Keywords
E-learning, M-Learning, Online Examination System, OTP, Anti-impersonation, Authentication, Face-Recognition.

1. INTRODUCTION
E-learning or electronic learning is learning through electronic technologies such as Online Forum, Video Conference, Web or Learning Management System (LMS) to access educational course, degree or program outside the traditional classroom. Several benefits of e-learning are its cost effective and saves time, learning 24/7 anywhere.

M-learning or mobile learning is education using personal mobile devices which are further connected to Internet to obtain learning materials through mobile apps, social interactions and online educational hubs. It is flexible, allowing students to access education anywhere, anytime. Mobile learning helps educational institutes to deliver knowledge and educational contents to students on any platform and at any time. Students use mobile apps and tools to upload assignments, download course instruction and interact through online social groups to complete tasks.

Examination is an assessment to measure knowledge or skills in a given area. An examination is conducted by schools, colleges, universities to assess the understanding capability of the student. Examinations are necessary as it constraints students to learn not only the subject of interest but also the subjects that are very important in the modern world. Since a very long time, pen paper based method is used to conduct examination. Pen based examination is time consuming as time required to set examination and evaluate the paper is more and also expensive as extra material like pen, paper, pencil etc. are essential. Also chance of paper leakage are more, results are declared after some time span, and for more number of students more number of invigilators is required. Now-a-days, Mobile Learning is a growing trend. Therefore, we decided to design online examination system for Android Mobile OS.

Online Examination System is basically designed for Educational Institutes like school, universities and training centers to make an examination which saves the time as it allows number of students to give the exam at a time. It reduces the manual work as it saves the time that will take to set the examination, check the paper and prepare mark sheets. The authenticity is maintained by administrator so no chance of leakage of question papers. The system generates the result as soon as the test is finished. Administrator can insert, modify and delete the information available and can also access all the accounts of teachers and students. Teacher can view the test conducted by students and also can view their marks.

The paper is organized as follow: Section 2 discusses the related work. Section 3 presents the functionalities of Online Examination Management System for M-Learning. Section 4 discusses the design of SEMS. Section 5 and 6 discusses the mathematical model of SEMS and algorithms used. Section 7 is based on result and discussion of proposed system. Finally, Section 8 presents future scope of system and conclusion.

2. RELATED WORK
Mustafa Kaiiali and Armanan Ozkaya [1] described design of a Secure Exam Management System (SEMS). SEMS offers examination services like: secure and random distribution of examination questions, turbo-mode assessment, preventing “unattended examination” issue through proctor approval based strategy, QR-Code based strategy and NFC based strategy, also provides biometric-based authentication service for anti-impersonation, preventing students from exchanging mobile devices during an examination, conducting examination securely through online or offline strategies, and audit students activities. They also provided countermeasures for network related issues such as network overload, network failure, exchanging information using alternative mobile devices during examination, and using a Wi-Fi jammer to bring the Wi-Fi network down. SEMS is an open source and also widely accepted LMS, specifically Moodle and its Moodle service extension. The resulting design is a complete LMS with secure examination 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 a teacher towards SEMS is very favorable.

George Meletiou and Ioannis Voyiatzis [2] designed and implemented e-exam system for Android platform. Their work mainly focuses on performance assessment. They claimed that for a system to be secure it should satisfy some specifications such as: physical security i.e. uninterrupted power supply, communication security i.e. user authentication, data encryption, secure OS, protection of wireless network and protection against internal attacks, code must be written in low language to easy reconstruct.

Prashant K Gupta and Manvi Madan [3] designed and implemented mobile based examination process for Android Mobile OS which consists of different modules: login module, registration module, question paper generation module, instruction module, evaluation module, score generation module, sample paper management and content management module. The authors claimed that their system has less hardware requirement so it is highly cost effective. The system is also reliable as only authenticated students can appear the test. They also included context management module for convenience of faculty members who are not tech savvy. But there is need to include features for security of the system.

3. PROPOSED WORK
The core services of proposed Secure Examination Management System for M-Learning (SEMS) are discussed below:

The users need to register themselves. The different fields of registration module are Username, Email, Mobile Number and Password. These details are stored into database which is used in future for authentication. The users are then authenticated through OTP (One Time Password) which is randomly generated password and sent to the registered mobile number or email-id for validation of single transaction. Then on successful registration users login through valid username and password.

After login, the teacher will define a set of questions and will specify set of options and correct choices and also specify examination details like Date and Time, Duration, etc. The type of questions is only multiple choices where each question consists of four options among which only one is correct answer. Also the teacher will enter list of eligible students with their id and names. Teachers have the right to view and modify all these details. Create random distribution of questions i.e. the questions will be flipped and randomly delivered to each student.

Fig 1 represents the flow for Secure Examination Management System for M-Learning. After successful login, students answer the examination questions. To prevent students from exchanging their personal devices during examination, the system re-authenticates the students automatically through face recognition at random time without interrupting the test. Students can view the different questions of test. Their answers are then submitted to the Examination Server. The Examination Server evaluates student’s answers according to the correct choices pre-defined by the teacher. Then it generates the appropriate result as soon as the test is finished, it displays total attempted questions, total current answer and percentage. The teachers can view their marks. The admin tracks the smart device usage and activities and provide external click management i.e. avoid students from accessing online sites and already stored files.

Fig 1: Flow for Secure Examination Management System for M-Learning.

4. SYSTEM ARCHITECTURE
The system enables the teacher to define examination bank through Analysis and Classification Module. Configuration Module provide set of options and also specify correct choices and specify examination properties such as: Date and Time, Duration, etc. Create examination instances by random distribution of questions. Server authenticate and enroll students and also track student’s smart device usage and activities. Students answer examination questions and their answers are submitted to application server. The application server evaluates student’s answers according to questions correct solutions pre-defined by the teacher. Then it generates appropriate result. This score then can be accessed by the institutes to evaluate student’s performance. OTP (One Time Password) is used to authenticate the user for single transaction or session. To prevent students from exchanging mobile/tablet devices after authenticated by Server, the system re-authenticates the students automatically through face recognition at random time. Fig 2 represents System Architecture for Secure Examination Management System for M-Learning.
5. MATHEMATICAL MODEL

Let \( S \) be the System where \( S = \{ s, e, x, y, F, Fc \} \)

- \( s \) = Initial state i.e. Successful registration and login with username and password.
- \( e \) = End State i.e. Subjects Examination Report.
- \( x \) = Set of Input Value = \{\( x_1, x_2 \)\}
  - \( x_1 \) = Users details for registration and login.
  - \( x_2 \) = Teachers define examination question bank and set of options.
- \( y \) = Set of Output Value
  = Subject’s Examination Report.
- \( F \) = Set of functions = \{\( f_1, f_2, f_3, f_4, f_5, f_6, f_7 \)\}
  - \( f_1 \) = Registration
  - \( f_2 \) = Authenticate (OTP)
  - \( f_3 \) = Encryption & Decryption (MD5)
  - \( f_4 \) = Login
  - \( f_5 \) = Re-authenticate (Face recognition Using Python and OpenCV)
  - \( f_6 \) = Report generation.
- \( Fc \) = Failure Case = Exam is interrupted due to any external click event or if face re-authentication fails.

6. ALGORITHMS

6.1 One Time Password (OTP) Generation for Authentication

One Time Password (OTP) is a numeric or alphanumeric string of characters which is automatically generated for authenticating users for single session. It provides simple and secure access to systems.

Step 1: Fetch length and type value of password.

Step 2: Three things Combination: Upper Case Letters, Lower Case Letters and Digits.

Step 3: Random Number is used to fetch character from combination of characters or only numbers as per user.

Step 4: While loop is used to avoid repetition.

Step 5: Unique Random OTP is generated.

6.2 Message Digest (MD5) for Encryption and Decryption

Step 1: Append padding bits

The message is padded so that its length is congruent to 448 mod 512.

Padding is performed – A single “1” bit is appended to message and then “0” bits are appended so that the length in bits of padded message becomes congruent to 448 mod 512.

Step 2: Append length

At this point resulting message has a length i.e. exact multiple of 512 bits.

Step 3: Initialize MD Buffer

A four word buffer A, B, C, D each of 32-bit register is used to compute message digest. These registers are initialized to following values in hexadecimal.

- word A 01 23 45 67
- word B 89 ab cd ef
- word C fc dc ba 98
- word D 76 54 32 10

Step 4: Process message in 16 word blocks

Four functions are defined from which each function takes an input of three 32 bit words and produces a 32 bit word output.

\[
\begin{align*}
F (X, Y, Z) &= XY \text{ or not } (X) Z \\
G (X, Y, Z) &= XZ \text{ or } Y \text{ not } (Z) \\
H (X, Y, Z) &= X \text{ xor } Y \text{ xor } Z \\
I (X, Y, Z) &= Y \text{ xor } (X \text{ or not } (Z))
\end{align*}
\]

Step 5: MD5 produces an output in A, B, C, D i.e. Start with lower order byte of A and end with higher order byte of D.

6.3 Face Recognition Using Python and OpenCV[4]

6.3.1 Database:

Usually Yale Face Database is used that contains multiple images of each individual.

6.3.2 Implementation:

Step 1: Import required modules -

- cv2 – It consists of functions required for face detection and recognition.
- os – It is used to extract image names in database and then the individual number is extracted from these names which are used as label for face in that image.
- Image – As OpenCV does not support gif format images so Image module from Python Imaging Library (PIL) is used to read image in grayscale format.
- numpy – images are stored in numpy arrays.

Step 2: Load face Detection Cascade –

OpenCV contains pre-trained classifiers for face, smile, eyes, nose etc. These XML files are stored in /data/haarcascades/
folder. Actually, haar cascade is used to detect face based on features.

Step 3: Create Face Recognizer Object –

Face recognizer object has functions such as:

- FaceRecognizer.train() is used to train the recognizer while
- FaceRecognizer.predict() is used to recognize the face. Here
- Face Recognizer used is Local Binary Patterns Histograms
- Face Recognizer. The function is as

createLBPHFaceRecognizer().

Step 4: Preparing training set –

- A get_images_and_labels() is passed with path of database directory which is function used to prepare training set. It assigns label for each recognized image. Label for image is image name and extension. The function used to detect faces in image is CascadeClassifier.detectMultiScale() i.e. used to detect skills of eyes, nose, lips.

Perform training– FaceRecognizer.train() function is used to perform training.

6.3.3 Testing the Face Recognizer:

FaceRecognizer.predict() is used to predict image.

7. EXPERIMENTAL RESULT

There are many online examination software’s existing in market. Onlinetestplus, Exam 9 product, Exam-Pro Software, Sify-itest, and iSummation Technologies are the widely used online examination software’s today.

Onlinetestplus is computer based software available at reasonable price. Onlinetestplus offers various examination services like Multiple choice questions, True-False type questions, Add pictures/videos to the questions, Question bank with unlimited questions, Categorize questions, Secure and password protected, Time based, Random questions, Add/import students, Instant results, Negative marking, Set unlimited exams, Administrative control and Automated grading. It is secure as while giving test student cannot go outside window.

Exam Pro is also and computer based online examination. It also administers the examination in conventional method by printing the question papers. Any type of questions can be assigned audio, video, multiple-choice, and true false. The program allows creating your own eLearning study material, quizzing for academic development of students.

Moodle is used to create private websites with online courses for educators and trainers to achieve learning goals. Moodle offers many features such as Bulk course creation and easy backup, Manage user roles and permissions, High interoperability, Simple plugin management, Multimedia Integration, Detailed reporting and logs etc. The limitations of Moodle are no external click event management i.e. previously downloaded documents can be accessed and also other online sites during examination is accessible. No appropriate mechanism for anti-impersonation.

In iSummation exam management system, in built Question database for exam questions are provided. User can access this application from anywhere and at any time. Administrator loads the exam bank into the database. Then the examinations are generated automatically as per student selections. Administrator can delete, edit and re-use the examination and questions anytime. In this system, discussion board feature is also provided so that the students can discuss problems that challenge them. And also user can add answers hints. Such online exams are delivered through any browser, and no additional software is required.

In sify-itest exam management system various types of assessments are conducted such as, Skill & Assessment Suite, Admission Management Recruitment Management, Employee Skill Assessment, Practice Test Solutions, Online Registration Engine, Sify-itest is also one of the exam management system used for Indian Institute of banking and finance. This exam management system needs its sify-itest browser for delivery of application. Additional software is required to run this system.

The proposed system i.e. Secure Examination Management System for M-Learning (SEMS) eliminates the drawbacks of the existing online examination software’s. The proposed system is Android driven examination system while all the existing systems are Web based. Moreover it has no extra hardware requirement and also eliminates the human resource required to set the examination and evaluation so we can say that proposed system is more cost effective. Since only authenticated users can take the examination so the proposed system is reliable and it re-authenticates students at random time to prevent from exchanging mobile devices during examination through face recognition. It authenticates the users through OTP. It provides 90% of good impact for security related to existing online examination software’s. It also prevents students from opening previously downloaded documents and accessing other online sites during examination. It also tracks smart device usage and activities. If any of invalid flow occurs then appropriate error message is send to user to do the needful. It provides good flexibility as whole application is designed and implemented using independent modules so that changes done in one module will not affect the other one and even new modules can be added easily to increase the functionality. The application is user friendly as least efforts are needed to operate. It provides good performance 80% of positive impact related to existing systems i.e. quick scheduling, immediate results and solutions.
8. CONCLUSION
Mobile Learning is a growing trend which leads to security issues. Hence to overcome the security issues, Secure Examination Management System (SEMS) is designed to handle unique examination security threats that exist in m-learning environment. This system is designed and implemented mainly to focus on the various security issues that could occur during online examination. It is an Android driven examination system, more number of students can apply the test at a time as now-a-days each student carries an android system with him/her. All examination stages are reviewed and identified the different security properties. SEMS provides several examination services such as: Authenticate the user through OTP, random distribution of questions, automatically re-authenticate students biometrically through face recognition at random time without interrupting the test, track student’s smart device usage and activities and also prevent students from accessing online sites and already downloaded files.

9. REFERENCES