An Advanced Authentication Scheme for E-evaluation Using Students Behaviors Over E-learning Platform

https://doi.org/10.3991/ijet.v15i04.11571

Yassine Khlifi
Umm Al-Qura University, Mecca, Saudi Arabia
Carthage University, Tunis, Tunisia
khlifi.yassine@gmail.com / yrkhlifi@uqu.edu.sa

Abstract—E-learning became attractive choices for academic institutions owing to their benefits, especially offering transparent and fast students' evaluation as well as innovative teaching methods. However, security issues related to e-learning have been raised by its stakeholders mainly faculty members, students, and administration. Authenticate examination takers during the electronic evaluation (e- evaluation), comprising assessment (E-assessment) and exam (E-exam), is a major challenge. In this paper, an advanced scheme is proposed to resolve this imperative challenge by introducing an efficient secure approach for supervising e-evaluation. The scheme collects information related to students and their behavior during the courses' activities and uses them for controlling unethical behavior during e-evaluation. The proposal doesn't need additional components and considered the continuous authentication using the random generation of a variable number of questions built from the collected information. The concerned student must respond to these questions which are generated periodically throughout the e-evaluation for guaranteeing his continuous authentication. Simulation experiments are conducted to validate our approach in which the obtained results show that student authentication is effectively guaranteed at a low cost whatever the student number and whatever the e-evaluation content.

Keywords—E-learning platform, e-learning security, student behavior, authentication; e-evaluation.

1 Introduction

Internet usage has been considerably rising due to the appearance of advanced applications and services including multimedia, distributed data processing, teleconferencing, and especially e-learning and distance learning. E-learning platforms become an attractive educational location where their stockholders' acceptance growths and more and more users are going to take online courses. Consequently, educational institutions have supported the implementation and the employment of e-learning platforms in teaching courses, electronic evaluation which includes assessment (e-assessment) and exam (e-exam). Electronic evaluation of the student, which is composed of e-assessment and e-exam, is an important issue in

education and one of the key activities in the learning. E-evaluation has started to take place of the traditional evaluation and changed by online procedures which offers numerous benefits such as opportunities for ultimate learning, automatic and transparent marking as well as direct feedback. In addition, e-evaluation is used to improve the educational learning environment for students and staff as well as enhance the output educational quality [1].

Typically, e-evaluation utilizes an e-learning infrastructure which used the Internet platform. This platform can be considered as a location for a set of illegal actions then e-learning infrastructure becomes exposed to several types of threats. E-learning stakeholders including university leaders, faculty members, and students as well as administration don't accept to use e-learning infrastructure in case of the presence of security issues [2]. Security requirements must be provided by assuring the following services: confidentiality, integrity, availability, and authenticity. These services must be presented to guarantee that e-learning stakeholders are safe against existing threats and risks. Nevertheless, security policies attempt to protect the e-learning environment which is composed of several resources including hardware, software, and data from potential threats. These threats try to exploit the existing weaknesses for resulting in non-legal actions using interception, interruption, and modification as well as fabrication [3].

In this case, e-learning users announce that the present platforms are not able to provide a set of accurate authentication mechanisms suitable for e-evaluation making. Therefore, providing authentication is a major challenge in deploying e-learning for interrupting and compromising security policies by unauthorized actions [4]. Moreover, user authentication offers a user's identification during the access system resources by ensuring who is granted access to which resources. For this reason, user authentication represents the main protection line of any secure system, especially over the e-learning platform. In addition, the security factor is considered as a key role in somewhat application type. Universities' leaders and faculty members are concerned about the authentication and security of the principal components of the e-learning platform, especially the learning management system (LMS) based examination. Students' unethical behavior in e-learning evaluation become a major concern [4, 5].

To our knowledge, several works have addressed the implementation of student authentication to offer a secure e-learning platform during the evaluation. In [6], authors try to examine the attitudes and experiences of a certain number of students who utilized an authentication system called adaptive trust-based e-assessment system for learning. The proposed approach used the analysis suggests a broadly positive acceptance of these e-authentication technologies by distance education students. However, the proposal is not accepted by the students due to concerns related to no secure use of personal data and the nuances of cheating and plagiarism as well as cannot guarantee their special needs. In [7], a student authentication approach has been proposed in which the relationship between online learning and e-assessment in presence of the development of institutional approaches to academic integrity has been described. The proposed approach enabled a certain number of ways to integrate technologies for and authorship checking and provide the data integrity for identifying

the specific issues that need to be resolved for the future. However, the data collected during the implementation of this approach cannot suitably enable an examination of the perspectives of e-learning stockholders on approaches to cheating and plagiarism, and on possible future orientations.

In the same frame, authors, in [8], introduced a novel approach that can predict academic cheating, based on some factors including home environment, peer pressure, school environment, academic anxiety, learning style. In this approach, the authors described the importance of the data collection to improve the security environment during e-assessment. Moreover, the approach integrated several parameters related to teacher, parents and academic integrity to secure against academic cheating. However, this approach cannot integrate suitable data during the implementation phase which increases authentication risks to cheating and its future directions. In [9], the authors discussed the different privacy and security issues associated with e-learning. Also, the design of an e-learning user authentication system has been introduced where a novel framework is proposed. This framework can provide the ability to prevent the manipulation of the students during learning, thus allowing reliable control of learning success. But this approach should integrate the suitable data during the design process for minimizing risks of student identification.

A mixed-method study has been introduced to examine the concerns and practices of a certain number of teaching staff who used the adaptive trust-based e-assessment system [10]. The proposed study showed that the results revealed some issues related to accessibility, security, privacy, and e-assessment design and feedback. Moreover, the outcome of this study provided recommendations and an audit report with results, to increase awareness about data security and privacy. An e-assessment system is developed to fully virtually assess students and to provide teachers the ability to prevent and detect from illegitimate behaviors including cheating and plagiarism [11]. An adaptive trust-based e-assessment system for Learning is used to design the developed system where several terms have been defined such as privacy and ethics, technologies, quality, and pilot design and evaluation. This system can enhance the authentication process however the relationship between assessment and student and teachers is not validated.

In [12], a study is conducted to investigate higher education teachers' perceptions of the prevalence and types of cheating in their courses and how the use of student authentication and authorship checking systems might impact assessment practice. This study used an Adaptive Trust-based e-assessment System for Learning which offers a variety of instruments to assure student authentication and authorship checking. The study used questionnaires and interviews to evaluate activities and explore the specific areas for examining the impact of authentication. A study is conducted in which online exam user authentication methods, systems, and threats have been discussed [13]. The results of the study showed that complete authentication methods that have been used in online exam systems are classified using knowledge, possession or biometric. The online exam systems and authentication techniques are based on user identification, authentication or continuous authentication. However, the threats may occur during exam sessions and

specifically classifies impersonation threats which must be solved using the existing authentication solutions.

The authentication challenges have been investigated to online examinations, review benefits, constraints of existing authentication traits, and discuss alternative techniques [14]. A profile-based authentication framework with user-id and password for the authentication of students during online examinations have been used. The sample size will be obtained from a group of E-learning University students. Data has been analyzed through descriptive statistics where several factors have been employed to validate the authentication process during e-assessment. Similarly, authors in [15] analyzed a deniable threshold ring authentication protocol that combined the two concepts including threshold ring signature and deniable authentication. This study introduced a new approach where a non-interactive deniable threshold ring authentication protocol has been utilized. The proposed protocol tried to guarantee legal participates that generate a valid signature in case of a message containing modification attacks under certain restrictions. However, the results of this approach should be validated through an experiment work or using a statistical method.

Even though the discussed works constitute important contributions in the development of authentication schemes for e-assessment and e-exam, these approaches have not considered several challenges. Particularly, the management of student authentication is done using jointly initial and active student profiles to supervise the authentication access which may have a significant impact on protecting e-learning infrastructure against unauthorized access. Moreover, the collection of the needed data related to the student for generating the authentication questions which, decrease cheating procedures is little addressed. Therefore, there is a need for the introduction of an advanced scheme that implements the required mechanisms for student authentication during the e-evaluation based on the active student profile for ensuring authentication process over the e-learning platform.

In this work, an advanced authentication scheme has been studied to solve the discussed issue by introducing an efficient model for e-evaluation supervision. In this scheme, a novel approach is introduced for guaranteeing a continuous authentication and control of unethical behavior. The introduced approach enabled during student e-evaluation a practical solution that incorporated a random generation of questions that assured the authentication and helped to the identification of the cheating attempts. Moreover, the proposed scheme ensured a continuous authentication of a student based on the management of students' information collected, during courses' activities. Using this known information by the concerned student, a variable number of authentication questions, depending on the e-evaluation content, are generated and used to guarantee his presence and his authentication. Finally, to validate our proposal, and evaluate its performances and effectiveness, extensive simulation work is conducted where the obtained results are discussed and analyzed. These results show that the proposed scheme can solve the studied authentication problem.

The paper is organized as follows. Section 2 presents in detail the evaluation management as well as a close relationship between authentication and e-evaluation. It also introduces the orientation to a novel authentication scheme. Section 3 presents in detail the proposed scheme and, describes the modeling procedure and its

associated algorithm as well as its essential functionality. Section 4 discusses the obtained numerical results through an experiment work and details the improvement of the proposed scheme compared to the existing schemes. Section 5 describes findings analysis and discussion. Finally, section 6 concludes the paper.

2 Related Works

2.1 E-evaluation management

E-evaluation can be considered as suitable methods due to its advantages such as providing a fast and transparently evaluation of students' knowledge and learning capability identification. Several approaches have been presented for examining the knowledge achievement of students, beginning from manual methods including using paper-based exams, oral, written, practical exam, and electronic form [16]. Evaluation, as a main component of the examination, is the main theme in education; it is a major part of any curriculum using student learning outcomes, which includes measurement, feedback, reflection, and change. It is becoming commonly used and one of the main activities in the student learning process [17].

Regular evaluation of students supports them to enhance and review to guarantee knowledge acquisition. In [18], two types of assessments of student learning can be identified including summative assessment and formative assessment. In the summative assessment, one can assess the knowledge and skills acquired by the students at the end of each learning module or unit. However, the formative assessment is focused to collect information related to the students' learning progress. E-assessment is considered one of the most significant structure issues of an e-learning platform where it depends on the learning supervision system which increases security issues related to e-learning software. However, the e-exam phases complete all features that traditional paper-based exams existing also reduce time, financial costs as well as increase convenience for students. In this case, entire security requirements should be completely achieved where the design of the proposed solution should consider special care of security [19].

Based on technological developments, assessment and exam have taken benefit from the system out of classroom location into online environments. E-evaluation, including e-assessment and e-exam, is defined as the use of technology to make more effective, and transparent as well as accurate assessments and exams electronically. Using information technology for any evaluation of student activities, e-evaluation can provide several advantages compared to traditional evaluation (paper-based). The advantages include lower long-term costs, immediate feedback to students, better flexibility about the place, improved reliability, and enhanced objectivity as well as greater storage efficiency to be stored on a server compared to the physical space required for paper-based evaluation. [18, 19].

The online formative evaluation is introduced for improving students' learning and providing information about their progress which leads towards a final course mark. Thus, it is essential for a student to make a summative evaluation which contributes to

determining a learning period nevertheless the formative evaluation delivers intermediate feedback for improving the learning results. E-evaluation consists of e-assessment and e-exam including a self-assessed quiz and a homework assignment with significant weight on the overall course grade is re-graded as formative, in case of examinations cover the similar material. Therefore, with a reliable approach, e-evaluation can reach the effects expected or planned by faculty members and instructional institutions. In this case, it is important to develop a suitable measurement procedure that ensures the efficiency of the evaluation process. Moreover, the e-evaluation depends on the learning management system that increases security issues over the e-learning environment. However, the e-evaluation scheme should achieve all the features that traditional paper-based exams offer. For this reason, all security requirements should be completely achieved where the design can take special care of security issues.

2.2 Relationship between authentication and e-evaluation

Authentication is an important phase of any evaluation system to verify and prove the identity of re-evaluation takers continually and repeatedly in a learning platform [18]. According to the existing works, especially in [18, 19], we determined three authentication methods which are summarized in table 1.

In this work, we focused on the knowledge method (what you know) with the integration of the behavioral level which established on utilizing password security and authentication questions. The information related to the authentication questions is collected based on an active student profile and his behavior during course activities. In the following table, we presented the different techniques used to collect information utilized during the authentication process.

Table 1. Overview of authentication methods.

Method	Advantages	Disadvantages
Knowledge Method	Password security is good if it is strong enough and provided by the institution.	Password is sometimes discovered. Not ever trusted for authentication throughout e-assessment.
Possession Method	Depends on Instruments such as: dongles, keys or cards that permit for authorized students to log in e-labs.	Instruments might be passed to others; the authentication scheme will be avoided and cannot be trusted for authentication at ever.
Biometrics Method	Provide precise means of authentication. For instances: fingerprint, voiceprint, retinal design and DNA sampling. Handwriting and typing measure (keystroke dynamics).	Expensive and difficult to implement. Requires special-purpose hardware.

2.3 Existing authentication techniques

Most computer systems are protected using identification and authentication techniques. These techniques utilize the personal information of users including name, user ID, password, email and other information known by the users. The users'

information, which is called also knowledge information, can be extended by integrating the behavioral information such as voice, gait, mouse movement and keystroke as well as signature etc. Also, other authentication techniques can be enabled using biometric, token procession, location, and IP address, as well as timestamp…etc. In this work, we focus on the concern to ensure authentication using knowledge information related to students and course activities for offering a low use of system components and high authentication capability.

Whereas the discussed authentication methods can be considered as a significant contribution in the e-learning security platform, other approaches and extensions to these works can be studied for implementing advanced authentication methods. In this paper, we interest to extend the use of behavioral information for assuring the protection and achieving a better security level over the e-learning platform. For this reason, we have found it interesting to integrate jointly student knowledge and behavior information as well as course activities in our proposed authentication scheme. Then, the new technique will be able to handle an advanced authentication approach that enables the better e-assessment environment. The implementation of this scheme constitutes a final phase for the design of an advanced authentication scheme suitable for e-assessment and e-exam as well as support for a next-generation e-learning platform.

2.4 Toward a novel authentication scheme

Although authentication is a major issue in the e-learning environment, most of the existing strategies and techniques did not consider some significant aspects such as simplicity and transparency. These aspects are very important for students during the e-assessment or e-exam taking, especially during the reel time authentication. This makes e-evaluation very hard and the process of monitoring the authentication information and supervising learning outcome became out of range. Therefore, there is a need for synchronization between the students' requirements and identification, as well as the design and implementation of a security scheme over the e-learning platform.

One of the main aspects of these enhancements is the realization of an e-learning platform that can solve the university problems. The first problem consists of several courses' evaluation can be hardly processed due to the important number of students and the limited staffs' number. The second problem is the limited resources that the university has in hand which made difficult to add biometric components for ensuring the authentication during e-evaluation. Moreover, the motivation behind this idea is to enable the real-time authentication management in the different e-learning components, which significantly enhances identification and interruption of security policies compromising by unauthorized persons. In previous works, the implementation of a security management framework and an authentication scheme for e-learning infrastructure success have been addressed [20, 21, 22]. The considered approaches have been introduced for information authentication improvement and efficiently e-assessment management. However, due to the rise of innovative needs related to e-learning stockholders and e-learning platform, the current platform

becomes unable to support security needs, especially for students and institutions with variable requirements for managing e-e-evaluation.

3 Novel Authentication Scheme

3.1 Descriptions and assumptions

Online authentication can be ensured using biometric components or other kinds of components or/et techniques which imposes an added cost for the concerned learning institute. For this reason, any proposed approach must consider the present problems and solve the limits in the learning environment, especially Saudi Arabia by using other methods. Our proposal doesn't need biometric components for managing and synchronizing the different stages of information to enable e-evaluation. The proposed approach will use knowledge methods which are executed into two steps: face-to-face (F2F) and behavior. The first step included the traditional technique which managed by the instructor to monitor authentication. Whereas, the behavior step is performed in the second phase in which password, profile and challenge questions as well as activities monitoring…etc. will be integrated.

To suitably design and implement the proposed approach, several assumptions should be taken into considerations and some descriptions need to be presented. These assumptions can help for providing the e-learning platform the appropriate environment to enable formative e-evaluation systems and data flow management. These assumptions can be presented as follows:

- Student identification is performed using private information delivered by the student
- Logging on by student is enabled using a password as a private information delivered by the student
- Authentication questions are created based on student profile, course activities, and content interaction. etc.
- Parameters of student activities included information related to the modules followed by each student and assignment deadline…etc. would be utilized
- Parameters of student profile are composed of several data types such as name, date and place of birth, age, interests, and image…etc. would be used

These assumptions help to manage e-evaluation considering the nature of the learning system at UQU which characterized by separating males and females in different environments as well as the important student number in some fields. Moreover, students' registration to the e-learning system over D2L or Blackboard is made based on user name and password which will be used to carry out e-evaluation of students' authentication. Knowing that the UQU learning system enabled two e-learning platform including D2L or Blackboard which are closed systems. In addition, UQU learning systems require to provide that system is flexible in assuring students authentication in e-evaluation without depending on the instructor. For this reason, LMS of UQU learning systems requires including other methods to guarantee the

designed learning process that reflect the impact on the authentication technique used during e-evaluation.

3.2 Modeling

To investigate an accurate authentication model, it is necessary to define and describe the different parameters which are managed by the considered e-learning system. The proposed approach is going to handle two types of parameters including information related to students' profile and courses' activities. These parameters are appropriate to generate the different components of the database which will be used to randomly design the authentication questions. The authentication questions include also other factors that will be utilized to support our model such as time and number of attempted access. The considered e-learning system is composed of several entities that deal with the main system are student, instructor, administrator, and registration unit. The student is the main entity who takes the exam or e-assessment. Whereas, the instructor is responsible for supervising or tracking the process. However, the administrator is responsible for managing the whole system, and the registration unit that is related to control the admission process to each student's course.

The different parameters of the designed approach and the notations are presented as follows:

- V: Total value of the output obtained from the average value of the answers.
- V_i: Value of the answer (s) to one of the authentication questions.
- NAQ: Number of authentication questions.
- NQA: Total number of authentication question.
- NEQ: Total number of exam questions.
- Nmodel: Total number of questions in one question group.
- AutR: Total value of authentication repeated questions.
- AutS: Students Authentication.
- NS: Number of Students.
- TS: Total Number of Students.

$$V = \frac{\Sigma_1^N v_i}{NAQ} \tag{1}$$

The above expression is stated as follows: As defined above, the authentication questions are generated during an e-evaluation in which a variable number of authentication questions are built. The number of authentication questions is depending on the evaluation content, precisely according to the number of e-evaluation questions. Knowing that the average answers' value of authentication questions related to the concerned students, which denoted by expression 1, is formulated based on the status of student response. The response status is identified using several parameters, mainly the number of attempts made by the student which is limited by an introduced threshold. This threshold defines the number of attempts that a student has for replying to an authentication question. We assume that the number of attempts is equal to three in the considered system. In this case for each

authentication question, the student has three attempts and a complete score which is equal to 1, in case the answer is correct in the first attempt. However, if the answer is incorrect for the first time due to false response or the authorized time is elapsed the score of the student related to this authentication question will be equal to 0.75, in case his response is true in the second attempt. We assume that the configured time period for each authentication question is fixed to 30 seconds. The student has another chance to answer the same question, but the multiple choices' answers will be reduced in each attempt by erasing the false choice. Therefore, if the student gives a correct answer, he will get 0.5 as a score, otherwise, the student will get a zero as a score for the wrong answer. For the shake of simplicity and for achieving a stable e-learning system, the above values of the threshold and the timer have been chosen.

$$\mathrm{NQA} = \frac{\mathrm{NEQ}}{\mathrm{Nmodel}} - 1 \tag{2}$$

The expression 2 is proved as follows: Let's recall that NEQ defines e-evaluation content which can be identified by the total number of e-evaluation questions. As described above, Nmodel defines the total number of questions related to a group of evaluation questions. knowing that this number of questions is organized in a set of groups and the whole groups have the same total number of questions which is identified by a configured number. In this case, the found value which describes the total number of all evaluation questions (NEQ) is divided by the total number of questions in one question group (Nmodel). In conclusion, one can subtract 1 from the computed formulation for attaining the total number of all authentication questions in the e-evaluation.

$$\mathrm{AutR} = \sum_{\mathrm{n=i}}^{\mathrm{nqa}} \mathrm{i}*\mathrm{V} \tag{3}$$

The expression 3 is verified and stated as follows: As described above, V defines the total value of the output obtained from the average value of the answers. Let's recall that the number of authentication questions is generation depending on the number of question groups in the e-evaluation. In this case to find AutR, one can calculate the sum of all the number of authentication questions multiplied by the total value of the output obtained from the average value of the answers. In conclusion, this expression describes the authentication strength in the case of the repeated authentication question and the strength level related to the effect of question repetition during the verification of the student identity.

$$AutS = \frac{\sum_{s=n}^{Nst} nS \sum_{n=i}^{nqa} i * \mathrm{V}}{tS} \tag{4}$$

The above expression is proved as follows: Considering the above notations, we can formulate the effect of the variation of the number of students and their impacts on the authentication scheme. Knowing that nS defines the number of students who participate in the e-evaluation. By computing the first sum and multiplying it by the total value of authentication repeated questions (AutR). After that, the obtained result is divided by the total number of students in this case the expression 4 is formulated. Finally, the obtained expression gives the impact of the students' number on the

validation of the authentication questions during the identification of the e-evaluation takers.

3.3 Algorithm

For overcoming the discussed issues, an advanced algorithm is proposed in which the information related to the student and his knowledge, as well as his behavioral during the courses' activities, is integrated. New mechanisms and parameters are introduced including two thresholds the first one is the timer and the second one is the number of attempts to respond to the authentication questions. The threshold is used to give the concerned student the opportunity to respond appropriately to the authentication questions. Whereas, the timer is used to manage the duration of the attempt for responding appropriately to the authentication question In the proposed algorithm, several expressions, formulated during the modeling, which are used to trigger the suitable mechanisms for ensuring the synchronization and supervision of the needed information during the e-evaluation.

The proposed algorithm is composed of three phases: e-evaluation phase, pre-e-evaluation phase, and post-e-evaluation. In the pre-e-evaluation phase, the e-learning platform collects the personal information of the student such as name, level, password and PIN code that contribute to personnel student authentication. In addition, the e-learning platform assembles behavioral information including information related to the student courses' activities which are used during an eventual e- evaluation phase. In the post e-evaluation phase, e-learning brings faculty staff the needed information about student behavior and grade. The proposed algorithm is integrated into the e-learning platform which synchronizes the collection information related to student authentication and enables the management of e-evaluation phase. In the following, we present the useful parameters and notations that handled by the e-learning platform during e- evaluation:

- SPIF: Student Personal Information Form
- CN: Course Name
- ET: E-evaluation title
- EG: E- evaluation Grad
- 1A1T: One Answer 1st Try
- 1A2T: One Answer 2nd Try
- EQN: E- evaluation Question Number
- PW: Password
- PIN: Personnel Identification Number
- CS: Course status
- AS: Authenticate status

```
SPIF phase
Start Form phase
```
While *CS== true*
Do

Perform Course phase
Read (PW, PIN)
If *AS== true*
Then
Store (PW)
Open SPIF
If *Student Answer All Questions*
Then
Save all SPIF Answers
Send All SPIF information to e-learning platform
Exit
Else
Back to SPIF Form
Endif
Else
Exit
Endif
Enddo
End SPIF Phase.
Post- Course activates
Start Post-E-assessment phase
Read (PW, PIN)
If *AS== true*
Register CN
Register ET
Register EG
Store (CN, ET, EG)
Send CN, ET, EG information to e-learning platform
Else
Exit
Endif
End Post-e-assessment session
E-evaluation phase
Start E-assessment phase
Read (PW, PIN)
While *AS== true*
Do
Generate SPIF
Compute 1AT1
If *1A1T = SPIF*
Send information to e-learning platform
Exit
Else
Generate SPIF
Compute 1A2T

***If** 1A2T = SPIF*
Send information to e-learning platform
Exit
Else
Read PW
Send information to e-learning platform
Exit
Endif
Endif
Enddo
End E-assessment phase.

3.4 Toward a validation approach

Based on the proposed model and algorithm, our scheme provides e-learning the ability to assure an efficient authentication process. The authentication is made using students' profiles which are created based on their personnel information and behaviors collected throughout the courses' activities. Thus, the e-learning platform, upon receiving the incoming request of student e-evaluation, generates a variable number of authentication questions. These questions appeared one by one and randomly after a defined set of evaluation questions that depend on the e-evaluation content. The number of questions is computed using the expression formulated and stated in the modeling phase. Then, the student authentication phase is started and processed until the e-evaluation is achieved or completed due to the unsuccessful authentication by the e-evaluation taker. Therefore, our scheme offers the needed improvements that can solve the discussed problems, but it is indispensable to evaluate it over an e-learning platform. Moreover, these improvements solve the discussed problems, but it is indispensable to evaluate it over an e-learning platform before the integration phase.

For this reason, we opted for an experimental platform to test and validate the different components of the proposed scheme. To make sure of the experimental platform credibility, we select to design it using a well-known simulation tool. This tool provides the ability to develop programs that offer the possibility of working as in a real e-learning system. for this reason, The MATLAB tool has been selected as a suitable tool that can integrate the proposed model and algorithm to achieve significant results. Also, we found it important to design the simulation work using this tool which helps us to generalize the obtained results over a different e-learning system. Knowing that the authentication level is the main output parameter of the performance evaluation related to our proposal, which is managed through the variation of various input parameters. So, to evaluate the considered e-learning system, we are going to select the suitable input parameters depending on expressions developed and stated in the modeling phase.

4 Experimental Work

Most of the well-known e-learning platforms are a closed system; improvements cannot be integrated before a validation process of any introduced enhancements. For that reason, we have found it realistic to develop experimental work for validating our proposal. However, modeling is an effective tool for measuring the authentication level during e-evaluation over an e-learning system but to consolidate it using simulation gives more credibility for the obtained results. Therefore, simulation work is conducted to focus on the validation of our scheme using a suitable environment and appropriate parameters.

4.1 Simulation environment

To develop appropriate simulation work, it is interesting to present a clear indication of the accuracy of the developed simulation tool before presenting simulation results. The present simulation experiments are performed using the well-known MATLAB tool which gives the capability to implement a pseudo-real system like e-learning systems. The considered tool provides the ability to generalize the environment of the simulation work which is considered the principal motivation behind its usage. Moreover, the simulation model is validated using random generators that utilize the generator of pseudo-random uniformly distributed numbers RAND predefined in the MATLAB, which is verified [23]. The different input parameters are generated using the sample-size calculated which is based on a well-used statistical method. This method is going to enhance the credibility of the obtained output parameters using the developed simulation model [24]. The authentication level is considered the main output parameter which is chosen to evaluate the performance of our proposal. This parameter is managed and supervised by the different considered input parameters. Authentication question number, size of question group and student number are selected as input parameters to evaluate the impact of the simulated system on the considered input parameter.

4.2 System description

We define hereinafter the experimental system which is composed of several components such as student environment, student profile, course components, quiz parameters and activity modules as well as authentication questions.

- **Student environment:** 10 classes are considered in which the student number in each class is between 20 and 50. The considered classes belong to three different levels, level 1, level 2 and level 3. The objective behind the choice of three levels is to collect the exact status of the student behaviors during the courses' activities. Moreover, the choice of three levels is considered as an advanced phase for the design operation of an innovative authentication approach, which is going to improve the pedagogical side and student acceptance.

- **Student profile:** Two kinds of profile are handled: initial and active profiles. The initial profile is composed of useful personal information such as name, image, PIN, Facebook, address, password, education, and date of birth and email. Whereas, the active profile comprises the information related to courses' activities including courses identification, quizzes identification, and self-assessment done by the student during the courses' periods.
- **Course components:** The components that will be used during the experimental work comprise course title, course content and course status. Also, the course can be identified by several parameters such as module, quiz, and activity studied as well as done by the student. These components can be identified using the following parameters:
  - Course modules: The considered parameters related to module include quiz number and quiz title. Moreover, we focus on activity number, activity title, the activity status of each module.
  - Quiz parameters: These parameters are composed of quiz include number, title, and status.
  - Activity parameters: The chosen parameters related to activity comprise activity number, activity title, grades, and activity status using several course tools such as forums, dropbox, and self-assessment.
- Authentication questions: The considered parameters related to authentication or verification questions are composed of question number, question response, question score, and attempt number as well as timer related to each attempt.

4.3 Simulations results

In the simulation work, we assume that each student's e-evaluation is consists of N evaluation questions and p authentication questions that are created using student profiles. As described before, the authentication questions are built randomly and added one by one after a set of e-evaluation questions which defined based on the developed model. Moreover, the student has two profiles: initial or personnel profile and active or student behavior during the courses' activities. After, m number of e-evaluation question, one authentication question appears for the student who has a certain number of attempts to respond to this question. For each attempt, a timer is enabled to supervise the response entry.

In the considered system, the student status or the score is defined using two policies: threshold-based and timer-based. The threshold-based, which is equal to three, describes the number of attempts that a student must reply for an authentication question. Whereas the timer-based, which is fixed to 30 seconds, describes the authorized time to response an authentication question for an attempt. The status of student or score is equal to 1, in case the answer is correct in the first attempt. The score is 0.75, in case the response is true in the second attempt. The score is 0.5 if a response is true in the third attempt, otherwise, it is equal zero due to a wrong answer in the third attempt, but the multiple choices' answers are reduced in each attempt by

erasing the false choice. Moreover, the response is considered false if the timer-based is expired without receiving a response of the student.

We present hereinafter the achieved simulation results, which indicate how the input parameters affect the considered output parameter of our system.

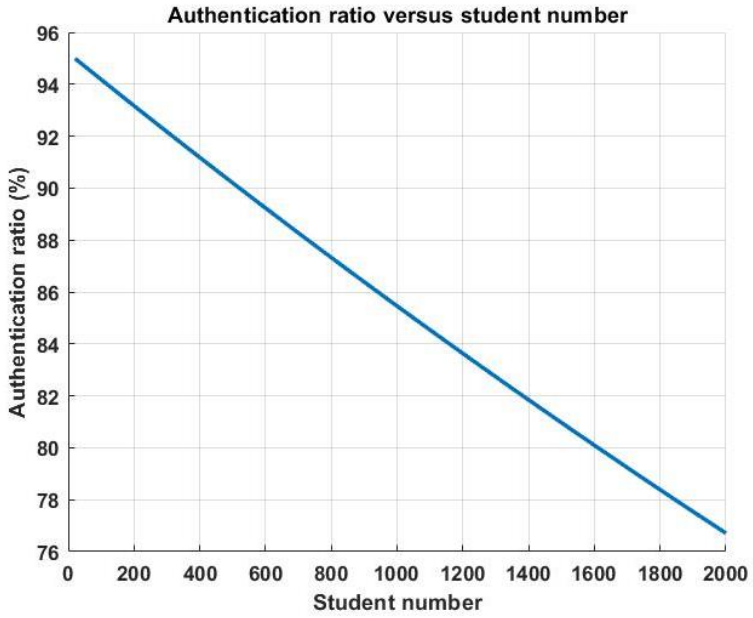

Fig. 1. Authentication ratio versus student number

Fig. 1 plots the authentication ratio versus the impact of the student number when the authentication question number is equivalent to 8. The e-evaluation question number is fixed to 40 where after each set of 5 questions an authentication question appears to the student. The student gives the response to the displayed authentication question which is supervised using two mechanisms: timer-based and threshold-based as described in the proposed algorithm. In this experimentation, the threshold is equal to 3 and timer-based is fixed to 30 seconds for providing the chance to the e-evaluation taker to give his accurate response to the authentication question. The choice of this threshold, precisely the number of attempts for responding to the authentication question, can be explained by the fact that the higher threshold provides more chance to the non-concerned student to compromise the authentication information and process an eventual cheating tentative. However, the shorter threshold cannot give the requested time to the student for realizing the authentication process. Hence, if the timer is exceeded the response to the authentication question will be considered as wrong response and the student will have the opportunity to go to the next question or to try the next attempt related to the same question.

In this figure, we observe that the authentication ratio decreases when the student number increases. This is because the growth of this number increases the presence of

a score student who has a score of less than 1. Several e-evaluations are rejected due to the non-acceptable score which is less than 0.75 nevertheless most of the evaluated student scores are greater than 0.75 and their evaluations are accepted. This figure also shows that the authentication ratio is greater than 90% when the student number is less than 200. Moreover, when the student number attained 2000 this ratio is maintained to a value equivalent to 75% which indicates a successful authentication for an important number of students. In conclusion, the proposed scheme guaranteed an accurate level of authentication for an important number of students and solves the discussed problems including a fast and transparent evaluation for many students. Using this result, the optimal number of students is less than 1600 in the e-evaluation when the authentication ratio is greater than 80% which is considered as a better ratio.

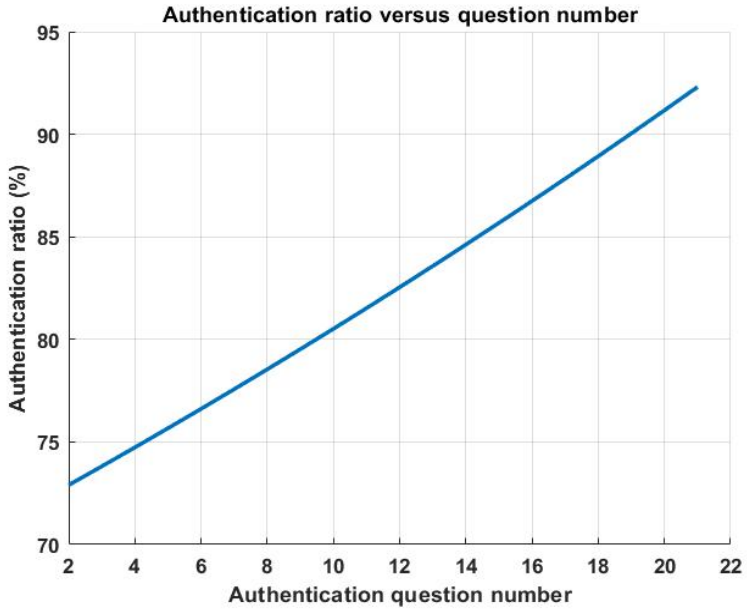

Fig. 2. Authentication ratio versus question number.

Fig. 2 presents the impact of the authentication question number on the authentication ratio when the number of students is equal to 200 and the e-evaluation question number is fixed to 40. The experiments also start with 2 as authentication number and the simulation is stooped when this number is equivalent to 21. Moreover, the same parameters are used including the threshold which is equal to 3 and timer that is fixed to 30 seconds. In this figure, we observe that the considered output parameter or authentication ratio increases with the growth of the authentication question number or the input parameter. This is because the increase of the input parameter improves the existence of information related to the two student profiles, initial or active, which are used to generate the authentication questions. This behavior has a positive impact on the authentication process, which can activate the

appropriate phase to supervise the relationship between the authorized student and e-evaluation. This figure also shows when the input parameter is less than 4 the authentication ration is less than 75% which is an unacceptable ratio, or a sensitive student score which is achieved. However, when the authentication question number is equal to or greater than 4 authentication ratio becomes equal or greater than 75%, which is an acceptable authentication ratio that assures the students' authentication and e-evaluation validation. In conclusion, the current experiment can be used to define the accurate number of the required authentication question to guarantee that the e-evaluation taker is authenticated and validate the e-evaluation.

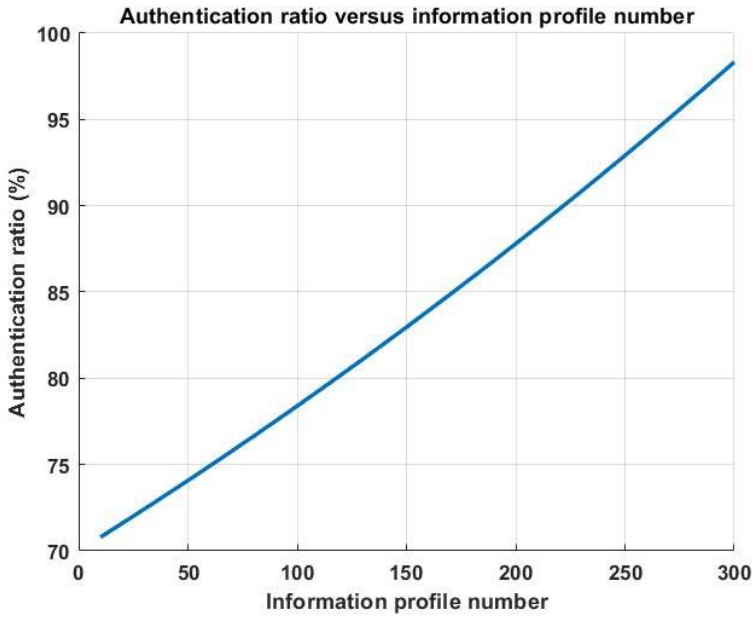

Fig. 3. Authentication ratio versus information profile number

Fig. 3 illustrates the authentication ratio versus the information profile number when the number of students is equal to 200 and the e-evaluation question number is fixed to 40. The experiments also start with 10 as the information profile number and the simulation is finished when this number is equivalent to 300. Moreover, the used threshold is equal to 3 and the utilized timer is fixed to 30 seconds. This figure shows that the considered output parameter with the growth of the information profile number or the input parameter. Knowing that the information profile number consists of the number of information related to the initial and active profile collected during the courses' activities. Therefore, the growth of authentication ration according to the size of information collected has a positive impact on the authentication process, which can disable the tentative of cheating and enable supervision of the association between the authorized student and e-evaluation. We also observe that when the input parameter is less than 10 the authentication ration is less than 75% which is an

unacceptable ratio, or a sensitive student score which results in a rejection of the e-evaluation. However, when the information profile number becomes greater than 60 the authentication ratio will be greater than 75%, which is an adequate authentication ratio that guarantees the students authentication. In conclusion, the present experiment can be utilized to identify the accurate number of the required information profile that assures the e-evaluation taker authentication as well as the e-evaluation validation.

5 Validation of the Proposed Scheme

The discussed approaches show that e-evaluation security is an important issue to assure e-learning platform success especially providing a transparent and fast evaluation as well as improving learning outcomes. UMM AL-QURA university (UQU university) is using LMS of D2L and Blackboard which enabled evaluation tools based on the student profile or personal information. This profile is considered as a static profile that is utilizing a username and password access by students that can be compromised or passed from student to others easily before or during e evaluation. Moreover, the academic staff participated in ensuring student identification before performing e-evaluation. However, the academic staff can find a huge difficulty to supervise students' authentication, especially when in the presence of an important number of students. So, the present research is introduced to solve the problem of the non-supervised and online environment. For this reason, we used the behavior technique due to the increased cost of biometric techniques, the cultural nature of students at UQU.

First, we formulated the different expressions that are used to define and analyze the suitable parameters of the studied system. Based on the system analysis, we developed an advanced algorithm that joint the knowledge and behavioral of the student as well as other parameters including threshold and timer supervision to manage the authentication questions. In this case, the student provides the response to the authentication question which generated using his behavior and the collected information during course activities. The student is authenticated based on his score which computed using the formulations made during the modeling phase. The different expressions used the two important parameters: the threshold or the number of attempts and the timer or the authorized time given for the student to enter the response for the generated authentication questions. The simulations experiments are conducted using a well-used statistical method, which may improve the credibility of the simulation model. The principal metric has been chosen to evaluate the performance of our scheme is authentication rate which is handled using the several important input parameters including authentication questions' number, information profile number, and student number.

6 Conclusion

The rapid developments in information and communication technology have encouraged educational institutions to implement and exploit e-learning platforms in

training and teaching as well as in the online evaluation. However, the e-learning platform does not been accepted by its stakeholders, faculty members and students, as evaluation support because there are some security issues related to authentication that does not be solved until now. For that reason, authenticate e-evaluation takers covering e-assessment and e-exam is considered as the main challenge. In this paper, an advanced security scheme has been proposed for contributing to resolving the authentication problem during e-evaluation due to threats or unethical behavior. These problems could lead to a negative impact on the credibility and acceptance of the e-learning platform. The proposed scheme collects information related to students and their behavior during the courses' activities and uses them for guaranteeing the authentication during e-evaluation. This scheme does not require added components and considered the continuous authentication using the random generation of a variable number of authentication questions made based on the collected information. The concerned student is authenticated using the initial profile and active profile.

The initial profile utilizes student personal information whereas the active profile is enabled using the authentication questions integrated into the evaluation according to its content. These questions are generated after a set of e-evaluation questions for guaranteeing continuous authentication. Knowing that e-learning platforms are a closed system, improvements cannot be integrated before a validation procedure. For this reason, experimental work has been developed for validating our proposal and evaluating its performances and effectiveness. The obtained results show that the authentication is effectively guaranteed at a low cost whatever the student number and whatever the e-evaluation content. The results of this work contribute to defining behavior knowledge and have several implications within the authentication field for the future development of e-learning platform. In conclusion, the study outcome can provide a significant model and approach that can be applied to achieve student authentication within e-evaluation for education policymakers so that it affects positively on the learning quality.

7 References

[1] Hillier, M. & Fluck, A. (2013) "Arguing again for e-exams in high stakes examinations", 30th ascilite Conference 2013 Proceedings, Macquarie University, Sydney, 385-389.

[2] Gathuri, J. W., Luvanda, A., Matende, S., Kumundi, S. (2014) "Impersonation Challenges Associated with E-Assessment of University Students", Journal of Information Engineering and Applications, 4 (7).

[3] Neila, R., Rabai, L., (2013) "Deploying Suitable Countermeasures to Solve the Security Problems within an E-learning Environment", Proceedings of the 7th International Conference on Security of Information and Networks, NY; USA, Association for Computing Machinery. https://doi.org/10.1145/2659651.2659721

[4] Senthil Kumar A. V., (2019) "Keystroke Dynamics: A Behavioral Biometric Model for User Authentication in Online Exams", Biometric Authentication in Online Learning Environments. DOI: 10.4018/978-1-5225-7724-9.ch008. https://doi.org/10.4018/978-1-5225-7724-9.ch008

[5] Feras Al-Hawari, Alshawabkeh, Haytham Althawbih, Omar Abu Nawas, (2019) "Integrated and secure web-based examination management system" Computer Applications in Engineering Education, https://doi.org/10.1002/cae.9.
[6] Alexandra Okada, Denise Whitelock, Wayne Holmes, Chris Edwards, (2018). "e-Authentication for online assessment: A mixed-method study", British Journal of Educational technology, Vol. 50, Issue 2, pp. 861-875, https://doi.org/10.1111/bjet.12608
[7] Roumiana Peytcheva-Forsyth, Harvey Mellar, Lyubka Aleksieva. (2019) "Using a Student Authentication and Authorship Checking System as a Catalyst for Developing an Academic Integrity Culture: a Bulgarian Case Study", Journal of Academic Ethics, pp. 1-25. https://doi.org/10.1007/s10805-019-09332-6
[8] Sarita & Dahiya, R. (2015) "Academic cheating among students: pressure of parents and teachers", International Journal of Applied Research, 1(10), 793-797.
[9] Byeong Ho Kang and Hyejin Kim (2015). "E A Design of E-learning User Authentication System" International Journal of Security and Its Applications, Vol.9, No.1 (2015), pp.45-50, https://doi.org/10.14257/ijsia.2015.9.1.05.
[10] Okada, A., Noguera, I., Aleksieva, L., Rozeva, A., Kocdar, S., Brouns, F., et al. (2019) "Pedagogical approaches for e-assessment with authentication and authorship verification in higher education". British Journal of Educational Technology, https://doi.org/10.1111/bjet.12733.
[11] Noguera, I., Guerrero-Roldán, A.-E., & Rodríguez, M. E. (2017). Assuring authorship and authentication across the e-assessment process. In D. Joosten-ten Brinke & M. Laanpere (Eds.), Technology Enhanced Assessment, 2017 (pp. 86–92, communications in computer and information science). Springer International Publishing. https://doi.org/10.1007/978-3-319-57744-9_8.
[12] Mellar, H., Peytcheva-Forsyth, R., Kocdar, S., Karadeniz, A., & Yovkova, B. (2018). Addressing cheating in e-assessment using student authentication and authorship checking systems: Teachers' perspectives. International Journal for Educational Integrity, 14(1), 2. https://doi.org/10.1007/s40979-018-0025-x.
[13] Karim, N. A., & Shukur, Z. (2015). Review of user authentication methods in online examination. Asian Journal of Information Technology, 14(5), 166–175.
[14] Gathuri, J. W., Luvanda, A., Matende, S., Kumundi, S. (2014) "Impersonation Challenges Associated with E-Assessment of University Students", Journal of Information Engineering and Applications, 4 (7), 2014.
[15] Tzu-Chun Lin, Ting-Yi Yeh, Min-Shiang Hwang, (2019) "Cryptanalysis of an ID-based Deniable Threshold Ring Authentication", International Journal of Network Security, Vol.21, No.2, PP.298-302, 2019 https://doi.org/10.6633/IJNS.201903 21(2).14.
[16] Marija Brkic Bakaric, Maja Matetic "Design and Implementation of Anonymized Social Network-based Mobile Game System for Learning Mathematics" International Journal of Emerging Technologies in Learning, https://doi.org/10.3991/ijet.v13i12.8762, Vol. 13, No. 12, 2018. https://doi.org/10.3991/ijet.v13i12.8762
[17] Sagar, K., Waghmare, V. (2016) "Measuring the Security and Reliability of Authentication of Social Networking Sites", Proceedings of International Conference on Communication, Computing and Virtualization (ICCCV), 79, 668-674. https://doi.org/10.1016/j.procs.2016.03.085
[18] Jingtai Ran, Kepeng Hou, Kegang Li, Niya Dai, (2018) "A High Security Distance Education Platform Infrastructure Based on Private Cloud", International Journal of Emerging Technologies in Learning, https://doi.org/10.3991/ijet.v13i10.9450, Vol. 13, No. 10, 2018. https://doi.org/10.3991/ijet.v13i10.9450

[19] Meyers et al., (2016) "Impact Results of the eMINTS Professional Development Validation Study", Educational Evaluation and Policy Analysis, vol. 38 no. 3, 455-476. https://doi.org/10.3102/0162373716638446

[20] Yassine Khlifi and Hassan A. El-Sabagh "A Novel Authentication Scheme for E-assessments Based on Student Behavior over E-learning Platform" International Journal of Emerging Technologies in Learning, Vol. 12, No. 4, April 2017. https://doi.org/10.3991/ijet.v12i04.6478

[21] Yassine Khlifi and Adel bessadok "A Novel Information Security Scheme for E-Learning Infrastructure Success Based on TRI Model", Open Access Library PrePrints, 2, e1424. doi: http://dx.doi.org/10.4236/oalib.1101424, pp. 1-18, Apr. 2015. https://doi.org/10.4236/oalib.1101424

[22] Yassine Khlifi, Mohammed M. Allehaibi "Information Security Services and Requirements for E-learning Infrastructure Success", 2014 World Congress on E-Learning, Education and Computer Science (WCEECS'2014), Hammamet, Tunisia, June 2014.

[23] Obaidat, M.S. and Papadimitriou, G.I. (Eds.), (2003) "Applied System Simulation: Methodologies and Applications", Kluwer, MA, USA, 2003.

[24] Pawlikowski, K., Jeong, H. D. J. and Lee, J. S. R. (2002)"On credibility of simulation studies of telecommunication networks", IEEE Communications Magazine, vol. 40, no. 1, pp. 132-139. https://doi.org/10.1109/35.978060

8 Author

Yassine Khlifi received M.S. degrees and Ph.D. in information and communications technologies from High school of communication (Sup'Com) of Tunisia. He is Assistant professor in Telecommunications at Carthage University, Tunisia, where he is a researcher at the Digital Security (DS) Laboratory. He is currently Assistant professor at Umm Al-Qura University, KSA, where he is currently an academic consultant and research & development director at IT deanship. He has authored / co-authored of several conferences and journals papers as well as a chapter in computer networks handbook. His active area of research is in optical networks, focusing on the design and analysis of optical label/packet/burst switched network architectures, optical protocols including signaling, switching, routing, grooming and QoS provision as well as networks protection and security.

Article submitted 2019-08-25. Resubmitted 2019-10-14. Final acceptance 2019-10-14. Final version published as submitted by the authors.