A Novel Authentication Scheme for E-assessments Based on Student Behavior over E-learning Platform

https://doi.org/10.3991/ijet.v12i04.6478

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

Hassan A. El-Sabagh
Umm Al-Qura University, Saudi Arabia
Mansoura University, Egypt
dr.haelsabagh@gmail.com & haelsabagh@uqu.edu.sa

Abstract—E-Learning and distance education have become common choices for academic institutions. Based on advances in information technology systems, educational institutions have enabled the employment of e-learning systems as teaching courses and evaluation students. However, security issues related to e-learning systems have been raised by e-learning environment stakeholders which including faculty members, and students as well as data. In addition, e-learning opponents argue that incapability of e-learning environment to authenticate examination takers is one of the major challenges. E-assessment is an important element of LMS based e-courses, and student authentication is mostly realized as one of the major concerns for e-assessments. For this reason, the main challenge facing the security of e-assessment and the e-learning environment is how to authenticate students because unauthorized persons can access and manage information. In this work, we propose a novel security scheme that contributes in resolving this vital issue by introducing an efficient secure model for supervising online evaluation including e-assessment or e-exam. The scheme addresses this imperative problem by proposing a novel approach that integrates available databases authentication technologies in conjunction with e-learning environments for controlling unethical behavior during e-assessment process. Moreover, the proposed scheme considers the continuous random authentication using students' information stored previously in the databases that guarantee identity and authentication. To validate our proposal, and evaluate its performances and effectiveness, an extensive simulation work is conducted over e-learning platform similar to Desire to learn (D2L).

Keywords—e-learning platform; e-learning security; presence and identity authentication; e-assessment and e-exam.

1 Introduction

Over the past few decades, Internet usage has been considerably growing for the provision of advanced applications such as multimedia, distributed data processing, teleconferencing, especially e-learning and distance learning. E-learning systems become an attractive educational location where the user's acceptance progresses and more and more people are trying to take online courses. Therefore, educational institutions have supported the implementation and the employment of e-learning platforms in teaching courses, electronic assessment (e-assessment) and taking electronic exam (e-exam). Student evaluation, especially e-assessment is major concerns in education and one of the key activities in learning environment. E-assessment has started to take place of the traditional evaluation and replaced by online environments. Therefore, using e-assessments delivers several advantages including opportunities for ultimate learning, automatic marking and direct feedback. In addition, e-assessments procedures are constructed for improving educational learning environment and provide the suitable information related to the output progress of the educational process [1].

However, e-assessments are based on the use of advanced e-learning infrastructure, which is related to Internet services that become a location for a set of illegal actions, and e-learning platform becomes exposed to several types of threats. Moreover, several e-learning platforms are employed without taking into account of certain security concerns and challenges. Nevertheless, security issues are related to e-learning systems have been raised by e-learning stakeholders including faculty members and students as well as databases [2]. Security requirements can be provided by guaranteeing confidentiality, integrity, availability and authenticity that can be employed in e learning to ensure that stakeholders are safe against probable threats and risks. However, security policies try to protect the e-learning environment that contain several resources including hardware, software and data from the potential threats that attempt to exploit the existing weaknesses using the ensuing actions such as interception, interruption, modification and fabrication [3].

For this reason, e-learning users claim that the existing platforms did not have the ability to provide a set of accurate authentication mechanisms suitable for e-exam or e-assessment handling. Therefore, providing authentication is a major issue in deploying e-learning platform for identifying and interrupting compromising information security policies by unauthorized entities [4]. In addition, user authentication provides a user’s identity while trying to access system resources by ensuring who is granted access to which resources. In this case, user authentication can be considered as the principal protection line of any secure system, especially over e-learning environment. In addition, the component of security represents a key role in somewhat type of application. Faculty members are concerned about the authentication and security of LMS based examination. Students’ unethical behavior in e learning has become a major concern [4, 5].

To our knowledge, several works have addressed the implementation of authentication mechanisms in order to provide a secure e-learning platform during the student evaluation process. In [6, 7], authors assured that increased usage of new technologies recently affected negatively to the growing of the unethical behavior by students. Students' unethical behavior includes wide range of technology-enabled behaviors such as cheating during e-exam using electronic devices, engaging in e-collaboration such as chat and forums, in addition, cheating like logging with another student's username and password. These technology-enabled unethical behaviors are often unobserved by instructors in e-learning courses. In the same frame, authors, in [8], referred that the advancement of new technologies have led to increase cheating methodologies by students that impede achieving confident results of reliable assessments and its standards.

Little concern has been given on providing solutions to other students' unethical behavior such as identify of student and authentication that aid cheating during e-exams noted that detection mechanisms are necessary not only in the e-learning portal access. Moreover, they are necessary to confirm users' access in various e-learning course activities [9]. With regard to previous literature, the increased research focused on developing better ways to manage e-examination and e-learning systems. Several papers focused on various issues related to e-learning security and e-assessment as well e-exams in particular. In [10], authors discussed security challenges of e-learning environments. However, their investigation focused on protecting the technology infrastructure against unauthorized users. Current security practices in e-learning systems relay principally on the utilization of passwords authentication mechanisms.

Further research paper proposed a web based online examination system [11], the system carried out the examination and auto-grading for students' exams. The system facilitated conducting exams, collection of answers, auto design the submissions and production of reports for the test. In [12], authors presented an online website for e-examination of economic course that aimed to present a novel software tool used for online examination of the course. The researchers described a cryptographic scheme that kept security requirements, such that authenticity, anonymity, secrecy, correctness without existence of third party. The proposed protocol also provided students a delivery, and a proof of a successful submission. In addition, they integrated identity authentication that implemented a set of techniques for random test user authentication, during the students' evaluation.

With regard to the previous research, the major concern recommended that challenge questions could be considered as an effective issue to solving attacks carried out by others [13]. In the same frame, authors, in [14], proposed a profile based authentication framework as a technique is based on a multi-factor knowledge based system, which used challenge questions as repeat authentication in addition to login-identifier and password for student authentication in the online examination. They implemented text based academic, personal, favorite, contact and date questions for student authentication. Their findings suggested that challenge questions based authentication in online examinations can be an effective artifact to prevent others' attacks. Similarly, authors in [15] referred that the threats related to online examinations can lead to a negative impact on the reliability of online learning courses. They proposed a profile based authentication framework that used multi modal authentication approach to secure online examination. Additionally, a timing mechanism was used that locked out students after a determined period of time; in addition, they used challenge questions based authentication technique. The questions were designed to encounter security challenges according to certain criteria of student response time, anticipated length of answer, difficulty and clarity of questions that had considered in the question design.

Even though, the aforementioned approaches constitute important contributions in the development of authentication scheme for e-assessment, these proposals have not considered several issues. Particularly, the management of student identification is done jointly with courses parameters to supervise the access and confirmation which may have a significant impact on protecting the technology infrastructure against unauthorized access. In addition, the exchange of the needed information related to user, especially student online information management and utilization in order to decrease cheating methodologies by students were little addressed. Therefore, a more complete study need to be developed to integrate student behavior and personnel information with authentication process in e-learning platform that implements the required mechanisms for student authentication during the evaluation process.

In this work, we investigate a scalable security scheme that can contribute in resolving the discussed issue by introducing an efficient secure authentication model for guaranteeing supervision of e-assessment processes. This scheme addresses this imperative problem using a novel approach that integrates a real time databases access in conjunction with authentication technologies over e-learning environments for controlling and supervising unethical behavior during e-assessment taking. The proposed approach also suggests practical solution that can incorporate a random test user authentication during assessment taking in e-learning courses that can reduce exam cheating. Moreover, the proposed scheme will consider the continuous random authentication based on the management of students' information stored, during courses learning, in the databases that can guarantee presence, identity and authentication. Finally, to validate our proposal, and evaluate its performances and effectiveness, extensive simulation work is conducted over an open e-learning platform where the obtained results are discussed and analyzed to solve authentication problem and validate the proposed scheme.

The remaining part of this paper is organized as follows. Section 2 briefly provides the basic concepts of e-learning characteristics and evolution. It also discusses e-learning advantages and limits as well as security concerns. Then, section 3 describes in details authentication scheme and presents e-assessment management then discussing authentication methods and e-assessment, afterwards an overview of the current authentication techniques. It also introduces the orientation toward a novel authentication scheme. Section 4 presents in detail our proposed security scheme and describes modeling and its associated algorithm as well as its fundamental functionality. Section 5 discusses the obtained numerical results through a simulation work and details the improvement of the proposed scheme against the existing schemes. Section 6 presents findings analysis and discussion. Finally, section 7 concludes the paper.

2 E-learning technology

This section briefly presents the basic concepts of e-learning including characteristics and features. It also discusses e-learning advantages & limits. Finally, it describes security concerns and issues.

2.1 Characteristics and features

The use of information technology in currently is considered as a solution for educational institutions' planned for achieving quality issues. Based on these technologies, e learning has begun many changes in higher education, as it emerged as a new paradigm of modern education and has changed previous learning concept [16]. E-Learning in higher education has become a significant trend that increasingly used within the academic activities recently. The encouragement of learner-centered learning is leading to the privilege for revolution of pedagogical design that supports the development of 21st century skills that augment knowledge learning [17, 18].

E-Learning contributes in providing the learner rich and variety resources than the traditional education; it also overcomes the limitations of time and space of traditional environment. E-learning lets learners to learn independently, meaning that it lacks the supervision and enforcement mechanisms of traditional teaching [19, 20]. As an increasing number of institutions adopt e-learning strategies, their successes depend not only on the availability of technology but also on the extent to which faculty and students are supported as they explore and develop innovative ways to integrate technology into the learning experience [19]. Pedagogical practices becomes more important, and a reliable. Providing powerful and safe technical infrastructure should be maintained in order to use e learning effectively. In conclusion, e-learning includes all interactive procedures related to teaching and learning in the educational environment.

2.2 Advantages and limits

The use of technology has been developed in the higher education by Saudi government. It helps to improve the instructors and learners' behaviors of motivation. The evolution of e-learning environments in kingdom of Saudi Arabia has increased during the last years because of the growing claim for higher education. E-learning has been incorporated by the Ministry of Higher Education to enhance the quality of education. Most of the educational institutions have already access to learning management systems practices [21, 22]. During the last few years, Umm Al-Qura University (UQU) has been increasing the use of learning technologies for the courses delivery and quality. E-Learning Deanships at Saudi universities have a motivating role to enhance traditional learning environments. Deanship of E-learning & Distance Education at UQU was established in 2010 to support the efficiency and quality of teaching and learning process at university. The message of deanship is to reinforce Learning environments by providing high-tech tools and means that encourage faculty to make use of "eLearn" portal. In particular to university of Umm Al-Qura, Desir2Learn

(D2L) was the learning management system. The component of security represents a key role in somewhat type of application. Faculty members are concerned about the authentication and security of LMS based exam (e-exam).

2.3 Security concerns and issues

Learner security plays a vital role in e-assessments; as it ensures that only the correct students write an online test. To realize this role, the student security practices attitudes two challenges (identity and authentication) to the students. Thus, the ability of the learner to provide the correct responses will provide the security system an assurance that the correct students are taking the test. Umm Al-Qura University has utilized e-learning methods that improve learners' motivation that is based on registering and carrying out electronic examination for the students through electronic devices.

In these environments, authorized persons are required to monitor and supervise the examination process from start to finish. Non-supervised environments include distance learning examinations and on-demand tests. In these environments, the examination process might be supervised remotely; however, the exam takers are required to maintain academic honesty. One of the major challenges related to security issue is to identify exam takers, to make sure that the student who responses the exam questions is the one who is supposed to take it. Face to face exams as a traditional method ensure exam takers are capable of realizing the rules (students must not talk to each other, student must avoid cheating, following the rules, etc.), in addition, providing an opportunity to check student's identity. Similarly, the student can cheat via other existing colleague instead of him. To overcome this problem, a continuous monitoring system should be implemented so that it gives opportunity to track and check student during e-exam or e-assessment throughout the exam [14, 23].

With regard to, online testing, it requires an achieving special security concern that is considered as a significant part of e-learning security [24]. Authentication refers to a mechanism in which the authorizations provided are compared to those on file in a database of authorized users' information within an authentication server [25]. However, password based authentication did not provide strong security for the system with sensitive data. Many attackers are still able to overcome the security by different techniques. Currently used authentication mechanism security question is easily guessable and phished by the attackers. Accordingly, different goals are taken into account to ensure continuous protections such as presence and continuously authenticated presence; Identity, and authentication. All previous goals are proposed for such research purposes [26, 27].

3 E-assessment authentication scheme

In this section, we review the basic aspects relative to e-assessment management and present authentication methods and examinations. We also describe the existing authentication techniques. In addition, we discuss the motivation behind a novel authentication scheme.

3.1 E-assessment management

Examination is one of the best methods to evaluate knowledge, and ability of students learning. Several approaches have been employed in examining the knowledge achievement of students, beginning from manual methods such as, using paper-based exam, oral, written, practical exam, and electronic form that placed of paper way [28, 29]. Assessment, as a main component of examination, is a main theme in education; it is a major part of any curriculum based on student learning outcomes, which includes measurement, feedback, reflection, and change. It is becoming commonly used and one of the main activities in student learning process [30].

Regular assessment of students helps them to improve and review to ensure the knowledge acquisition. In [31], authors identified two types of assessments of student learning. First is the summative assessment, which assesses the knowledge and skills acquired by the students at the end of each learning module or unit. The other one is the formative assessment, which is focused to collect information related to the students' learning progress [32]. E-assessment management is one of the most important structure issues of an e-learning environment. The e-assessment that depends on learning management system increases more security issues than the other parts of the e-learning software. However, the e-exam scheme should achieve all features that traditional paper-based exams existing, in addition to, reduce time, financial costs and increase convenience for students. All security requirements should be completely achieved; therefore, its design should take a special care of security [33].

Influenced by technological developments, assessment has begun to benefit from technique out of classroom environment into online environments [33]. E-assessment is defined as the use of technology to digitize, make more effective, and redesign assessments and tests electronically [34]. E-assessment is the use of information technology for any assessment-related activity. It has many advantages above traditional assessment (paper-based). The advantages include lower long-term costs, immediate feedback to students, better flexibility with regard to place, improved reliability (it is more consistent than human marking, improved objectivity (it does not 'know' the students, greater storage efficiency to be stored on a server compared to the physical space required for paper-based assessments [35].

With regard to formative assessments, the online formative assessments are planned to improve students' learning and give information about their progress that lead towards a final course mark. Thus, it may be required for a student to take a summative assessment. Concerning summative assessment, it determines a learning period; however, the formative assessment provides intermediate feedback to improve the learning results. For instance, a self-assessed quiz and a homework assignment with significant weight on the overall course grade can be re-graded as formative, in case of examinations cover the similar material [30]. Consequently, with a reliable mechanism, assessment may attain the effects planned or expected by faculty members and instructional institutions. It is important to develop high-quality measurement procedures that ensure the effectiveness of evaluation process. Additionally, the e-assessment that depends on learning management system increases more security issues than the other parts of the e-learning environment. However, the e-assessment scheme should achieve all features that traditional paper-based exams offer. All security requirements should be completely achieved; therefore, its design should take a special care of security.

3.2 Authentication Methods and exams (e-assessment)

Authentication is the key part of any assessment system to identify and prove the identity of e-assessment takers continuously in learning environments [29]. According to previous literature [32, 36], we concluded the following several authentication methods that were used by the previous researchers. The authors summarized three authentication methods (techniques) as shown in the following table 1 summarize such methods or techniques.

Table 1. Overview of Authentication Methods or Techniques

Method or Technique	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.

At the current paper, we concentrated on the knowledge method or technique with integration of behavioral level in the proposed scheme, which established on utilizing password security, in addition to challenge questions that make sure student authentication according to student profile and behavior within course activities.

3.3 Existing authentication techniques

Most of computer systems or platforms are protected through the usage of identification and authentication techniques based on the use of users' information including name, user ID, password, email and other personnel information known by the users. This information which managed by users are entitled knowledge information. Knowledge information can be extended by adding behavioral information, which can include voice, gait, mouse movement, keystroke and signature…etc. However, there are others authentication techniques which are based on biometric process or procession of token as well as others mechanisms such as location, IP address and timestamp…etc. In this work, we do not interest to study the authentication techniques using biometric or physiological parameters as well as possession parameters. We focus on the issue of providing authentication using knowledge information of students and course parameters because our approach aims to offer a low materiel usage, a low operation cost and high system capability of authentication.

While the proposed authentication techniques, discussed and analyzed in the previous sections, can be reflected as an important contribution in e-learning security platform, other extensions to these works can be studied for implementing others or advanced authentication functions. In our work, we interest to integrate and extend the behavioral information in order to improve the protection and achieve a better security level over e-learning platform. For this reason, we have found it interesting to integrate mutually student knowledge and behavior information as well as course parameters in our proposed authentication scheme. Then, the objective of our proposal is to propose a new technique capable of handling toward an advanced authentication approach and enabling better e-assessment environment. The design of this scheme constitutes an intermediate phase for the design of an advanced authentication scheme suitable for e-assessment, which can be considered as a suitable support of the next-generation of e-exam platform.

3.4 Toward a novel authentication scheme

While the existing approaches can be considered as an important contribution in e-learning security platform, especially e-assessment authentication other extensions to these works can be investigated in order to implement advanced authentication services or functions. Whereas authentication is important issues in e-learning environment, most of the proposed strategies did not take into account dynamic and reel time authentication requirements related to student of e-learning platform. This makes controlling and supervising e-assessment or e-exam very difficult for monitoring the information processing. Consequently, there is a need for synchronization between the students' requirements and identification, as well as the design and implementation of e-learning platform.

One of the main aspects of these enhancements is the realization of e-learning environment, where security services are related to students' information, which is processed during the platform exploitation stages without any restriction. The motivation behind this idea is to enable the real time authentication management in the different of e-learning components, which significantly enhances identification and interruption of security policies compromising by unauthorized persons. In our previous work, we addressed the implementation of security management framework for e-learning infrastructure success [36]. The considered approach introduced the needed improvement for data management and efficiently use of secure environment. However due to the emergence of novel needs related to users and platform, e-learning will evolve towards security measures for supporting the multiples students and e-learning courses needs with variable requirements for managing and supervising e-assessment processes.

4 Novel authentication scheme

In this section, we present the description and assumptions related to the authentication environment. We also describe the different parameters of the adopted model. In addition, we define the different components of the proposed algorithm. Finally, we discuss and analyze the obtained results.

4.1 Descriptions and assumptions

Several authentication mechanisms are able to achieve process of student authentication environment especially online. However, we depend on knowledge methods on designing the proposed scheme, because of private nature of Saudi environment and according to saving costs of other techniques (Biometrics). Our prosed model is assumed that it manages several e-assessments and assure security authentication at the same time. The scheme is supposed to include two parts of examination (F2F and Online). First part is depended on the traditional technique of exciting the instructor to monitor students' authentication, however, the online part is depended on several components such as password, profile, challenge questions and activities tracking…etc.

The authors analyzed the main assumptions of e-assessment environment especially, related to formative assessment, so that it provides the system process and data flow that depended on current scheme that can be presented as following variables:

- Student identification (ID) as knowledge based technique that based on private information delivered by the student.
- Logging on by student through certain password as knowledge based technique that based on private information delivered by the student.
- Challenges questions as knowledge based technique that based on student profile, course activities, and content interaction...etc.
- Parameters related to student activities such as last log in, modules followed by each student and assignment deadline…etc. would be used.
- Parameters such as student profile includes several types of data including name, date and place of birth, age, interests, and image…etc. would be utilized.

With regard to the previous assumption, we attempt to take into account nature of learning environment at UQU that depended on dividing males and females at different houses. Registration of students to D2L (LMS) and using only user name and password is the central method to carry out examination (e-assessment) to examine students’ authentication. Furthermore, (D2L) used by UQU is closed system. Consequently, the need to provide that system is flexible in assuring students authentication in examination and e-assessments without depending on the instructor. In conclusion, LMS is needed to integrate scheme with existing features to enhance other methods to assure the realized learning components process that reflect the impact on use of authentication technique during e-learning assessments.

4.2 Modeling

According to transition process of paper based assessment to e-assessment to promote blended learning. We attempt to detect authentication techniques that can be used in e-assessment in addition to several examples of each technique. Fig. 1 shows student authentication schemes that are categorized into three levels including knowledge, behavior and other levels. The knowledge factor involves features such as: passwords and student PIN whereas, the behavioral scheme includes factors, such as challenging questions according to several parameters which contain student profile and course activities…etc. A last, the other factors might be utilized such as determine time of attempted access.

As is seen in Fig. 2, the e-assessment system could be identified according to context diagram of proposed system. The external entities that deal with main system are student, instructor, administrator, and the registration unit. Student is the main entity who takes the exam or e-assessment. Whereas, instructor is responsible of supervising or tracking the process. However, administrator is responsible of managing the whole system, and the registration unit that is related to control the admission process to each student's course.

With regard to Fig. 3, the level zero of system or main system, the authors identified the main process of e-assessment system that includes three main processes (Pre_e-assessment, during e-assessment, post e-assessment). The diagram involved the flow of system data among the recognized sub-processes that related to regarding to data store. The pre-assessment refers to all processes that are controlled by the instructor and administrator that facilitate the following process, where is the "during e-assessment" process, it shows all relation during e-exam or e-assessment process of each student that are correlate to e-learning server, however, the "post-assessment" process are correlated to grade file store file.

As shown in Fig. 4, According to level zero of system, the authors allocated with the sub processes of (pre-assessment) that involved the following (E-Course log in by student, E-course navigation (behavior), Instructor Supervising (Tracking). According to level two of system, As shown in Fig. 5, the authors set the sub processes of (during-assessment) that involved the following (E-assessment log in by student, Password authentication, Authentication check). According to level three of system, the authors set the sub processes of (post-assessment) that involved (Recording & saving process, auto correction, adding grading, indicating the authentication, and finally the evaluation process) can be showed in Fig. 6.

As shown in Fig. 4, According to level zero of system, the authors allocated with the sub processes of (pre-assessment) that involved the following (E-Course log in by student, E-course navigation (behavior), Instructor Supervising (Tracking). According to level two of system, As shown in Fig. 5, the authors set the sub processes of (during-assessment) that involved the following (E-assessment log in by student, Password authentication, Authentication check). According to level three of system, the

authors set the sub processes of (post-assessment) that involved (Recording & saving process, auto correction, adding grading, indicating the authentication, and finally the evaluation process) can be showed in Fig. 6.

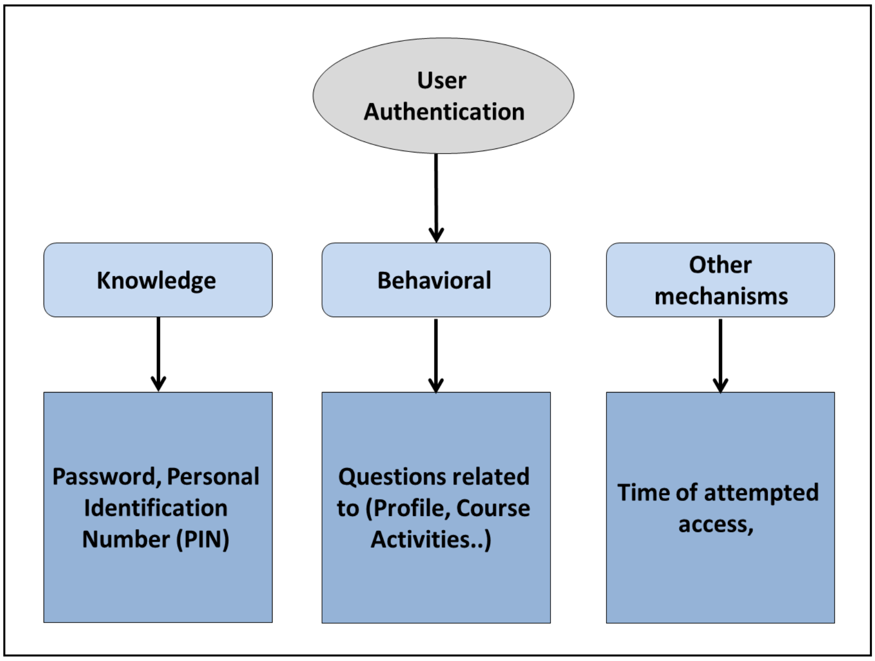
User Authentication
Knowledge
Behavioral
Other mechanisms
Password, Personal Identification Number (PIN)
Questions related to (Profile, Course Activities..)
Time of attempted access,

Fig. 1. Student authentication scheme.

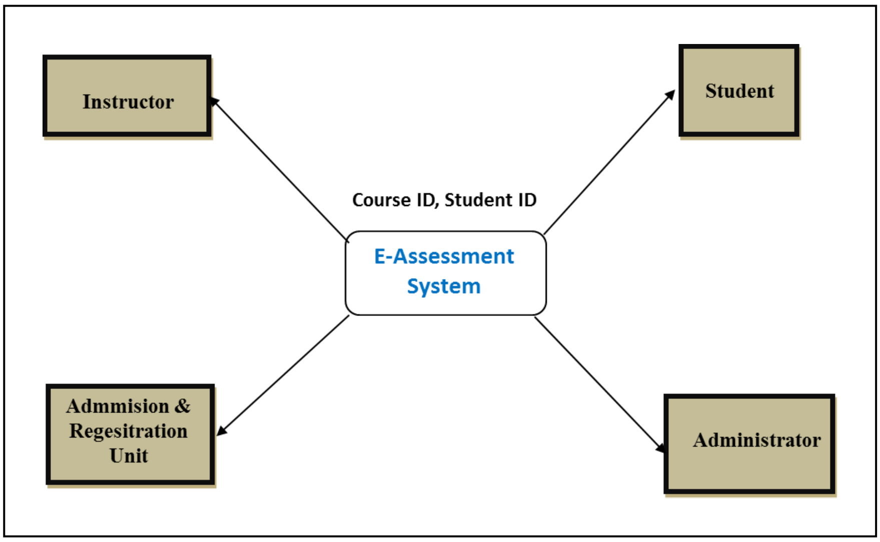

Fig. 2. Context Diagram.

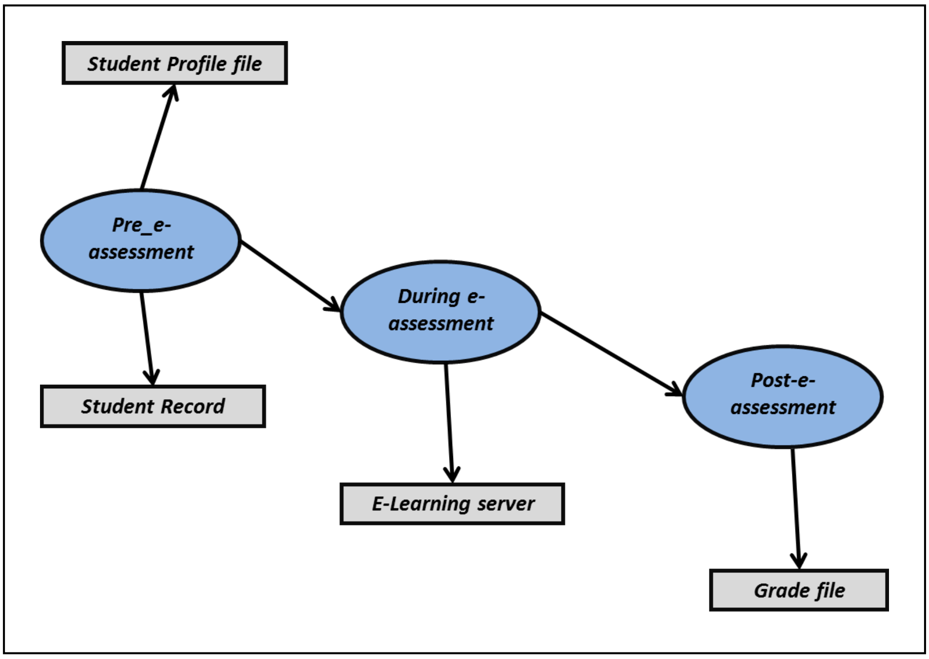

Fig. 3. Main processes of the system.

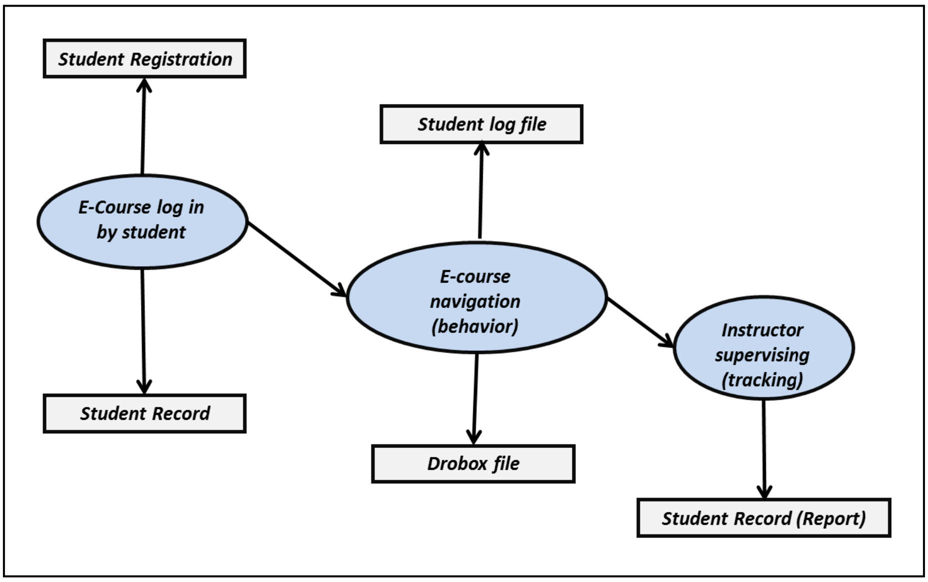
Student Registration
E-Course log in by student
Student Record
Student log file
E-course navigation (behavior)
Drobox file
Instructor supervising (tracking)
Student Record (Report)

Fig. 4. Pre_e-assessment processes.

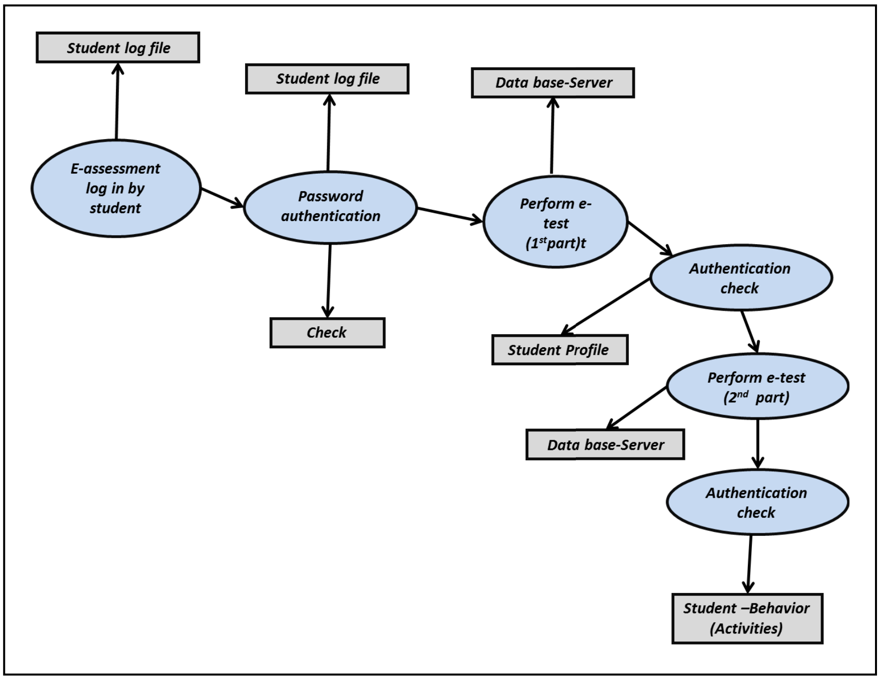

Fig. 5. During-assessment processes.

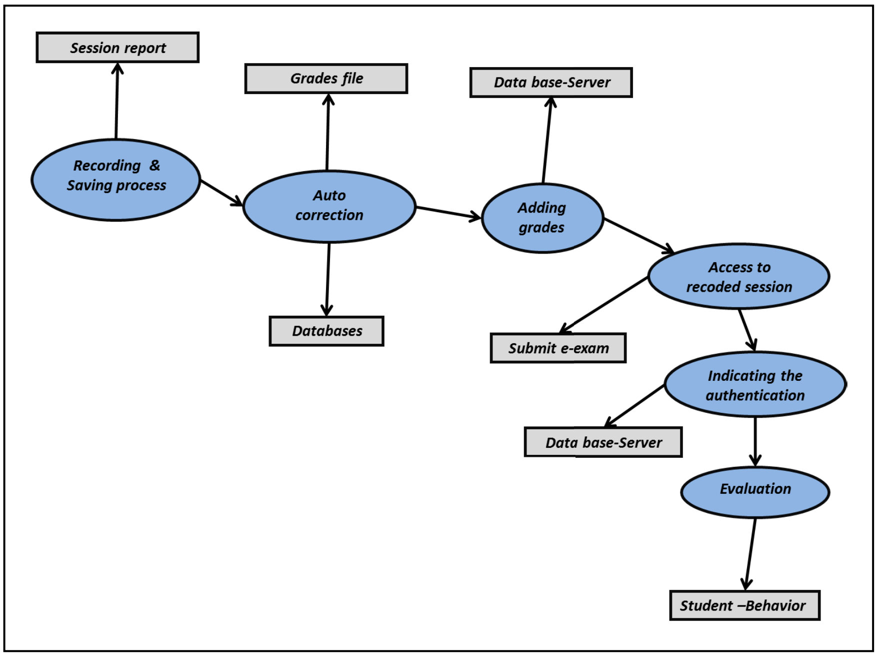

Fig. 6. Post_e-assessment processes.

4.3 Algorithm

To solve aforementioned authentication problems, we develop an advanced algorithm that combines the student knowledge and behavioral as well as others mechanisms and parameters including time handling and questions supervision. The proposed algorithm insures a real time or online transfer of the needed information, especially during e-assessment phase to monitor significantly e-assessment and e-learning platform utilization. Our scheme is consisted of three phases including as core treatment e-assessment phase and two others phases as supporting treatment which includes pre e-assessment phase as well as post e-assessment. In the Pre-e-assessment phase, e-learning platform collects information related to personal student information such as name, level, password and PIN code that contribute to personnel student authentication. In addition, e-learning platform collects also behavioral information, which is jointly stored in the databases and will be used during an eventual e-assessment phase. In the post e-assessment phase, our scheme will give e-learning platform the opportunity to bring faculty staff the needed information about student behavior and grade. For this reason, our proposed algorithm will be performed in three different steps where the core treatment represented by e-assessment phase, however, pre e-assessment phase and post e-assessment phase will support e-assessment phase. In this case, when the e-learning platform receives information related to student authentication, it performs the proposed algorithm for monitoring appropriately e-assessment phase. In the following, we present the considered parameters handled by e-learning platform during e-assessment phase, and the useful notations:

- QR: Quiz Response,
- QE: Quiz Evaluation,
- EQN: E-assessment Question Number,
- MCQ: Maximum Challenging Question number,
- CCQ: Current Challenging Question number,
- MTN: Maximum of Tests Number,
- WT: Waiting Time
- MWT: Maximum of Waiting Time,
- PW: Password,
- PIN: Personnel Identification Number,
- AQ: Authentication Question,
- RAQ: Response of Authentication Question,
- SE: Student evaluation,
- SA: Student assessment.

- **Pre-E-assessment phase**

```
– Start Pre-E-assessment phase
– Perform Course phase
– Read (PW, PIN)
– If authenticate
    o Store (PW)
    o Perform Quiz
    o Write QR
```

```
          o  Generate QE
          o  Generate MCQ
          o  Generate AQ
          o  Compute MWT
          o  Create student behavior
          o  Save student behavior
          o  Send information to e-learning platform
        –  Else
          o  Send information to e-learning platform
          o  Exit
        –  Endif
        –  End Pre-E-assessment phase
•  E-assessment phase
        –  Start E-assessment phase
        –  Read (PW, PIN)
        –  If authenticate
          o  Generate QE
          o  Compute MWT
          o  Generate AQ
          o  Read (RAQ)
          o  While AQ=RAQ
                    •  Generate EQN
                    •  Generate AQ
                    •  Read (RAQ)
                    •  While WT<> MWT & MCQ <> CCQ
                    •  IF MWT) <> MWT & AQ<> RAQ
                            ▪  Send information to e-learning platform
                            ▪  Exit
                    •  Else
                            ▪  Compute MWT
                    •  End
                  o  Read (RAQ)
          o  End
        –  End
        –  Save student behavior
        –  Send information to e-learning platform
        –  Else
        –  Exit
        –  End E-assessment phase
•  Post-E-assessment phase
        –  Start Post-E-assessment phase
        –  Compute SE
        –  Compute SA
        –  Store (SE, SA)
        –  Send student grade information to e-learning platform
        –  End Post-e-assessment session.
```

4.4 Analysis and discussion

To design appropriately the proposed scheme, it is important to define the different parameters of implementation. In our approach, the e-learning platform needs to maintain student behaviors and information such as student evaluation and student assessment as the information related to the course including quiz number and quiz evaluation or grade, as it is described in the previous section. As seen, the proposed algorithm is performed as main service of e-learning platform, precisely during online assessment related to the concerned student, as shown in Fig. 10. The e-learning platform, upon receiving the incoming request related to student e-assessment attempts to identify the student based on student information or knowledge level including username and password. Then, it creates the e-assessment stage, updates the status of the student and relies the open session to course parameters. If student is authenticated, e-assessment phase starts and the authentication information related to the student is extracted and exchanged between e-learning platform and e-assessment phase as well as the concerned student. In this case, the student will give the appropriate response to authentication question associated to his behavior and collected information during F2F course or education activities. Let's recall that the non-authenticated student will be again until he exceeded the authorized number of response or the authorized delay threshold is reached. When the threshold is reached, the e-assessment phase is closed and information will be transmitted to the student and the concerned faculty staff. As describe above, the student behavior information is updated dynamically at each e-assessment phase related to course components including activity and quiz.

5 Simulation and numerical results

As seen before, the main characteristic of the used e-learning platform or D2L is a closed system that cannot give the ability to integrate the modifications or improvements added by our proposed scheme. For this reason, we have found realistic to develop simulation work in order to validate our proposal. In the consequence, we present the implemented simulation environment and discuss some of the most important numerical results.

5.1 Simulation environment

To design an accurate simulation work, we have found it of great interest to present a clear indication about the accuracy of the developed simulation tool before presenting simulation results. The current simulation experiments are performed through the use of the well-know MATLAB tool which gives us the capability to design and implement a pseudo real system similar to the given by D2L system. The generalization of the environment of the simulation work is the main motivation behind the usage of the considered tool. The validity of the developed simulation model is performed based on the use of random generators using the generator of pseudo-random uniformly distributed numbers RAND predefined in the MATLAB language libraries, which are well proved [37]. The generation of the input parameters, simulations experiments are conducted using the sample-size calculated using a well-used statistical method, which may improve the credibility of the developed simulation model [38]. The principal metric has been chosen to evaluate the performances of our proposal is authentication level which is handled and managed by the different considered input parameters. The following input parameters have been selected for the evaluation of considered system including quiz number, course content and activity, challenging questions and student profile.

5.2 System description

We describe hereinafter our considered system or platform, which contains several components including student class and level, student profile, course components, quiz parameters and activity modules as well challenging questions.

- Student class and level: We here consider 4 classes in which the student number is fixed to 50. The considered classes are belonged to two different levels, level 1 and level 2. The objective behind the choice of two levels is in order to have a global view about the student behavior toward e-assessment process. After that, we can generalize it with the existing levels, which are equal to 5 levels. Moreover, the choice of two levels is considered as an intermediate phase for the design operation, in the next step, of an innovative authentication approach, which has a positive impact on pedagogical side.
- Student profile: We here consider two kinds of profile such as static or initial profile and dynamic profile. The useful information related to static profile is consisted of name, image, PIN, Facebook, address, password, education and date of birth and email. The dynamic profile contains the information related to activities and quizzes or self-assessment done by the student during the course process. This information will be stored in the database after that it will be used during the initial authentication process and advanced authentication steps.
- Course components: The components related to the course used during the experimental work consist of course title, course content and course status. In addition, the course contains other parameters such as module, quiz and activity studied and done by the student which can be presented as follows:
  - Course modules: The considered parameters related to module include quiz number and quiz title. In addition, we interested to activity number, activity tile, activity status related to each module.
  - Quiz parameters: The considered parameters related to quiz include number, title and status.
  - Activity parameters: The following parameters related to activity have been chosen including activity number, activity title, grades and activity status through the use several course tools including forums, drop box and self-assessment.
- Challenging questions: The considered parameters related to challenging question consists of question number, question response, question status and waiting time as

well as the constraint related to the authorized entry for responding to the concerned question.

5.3 Simulations results

In our simulation work, we assume that each e-assessment step for each student is consists of 40 questions where each 10 assessment questions are followed by one challenging question. The student cannot have the ability to access to the second 10 question if he gives a wrong response to the challenging question. In case of the response to challenging question is right, this process is repeated for each set of questions, or 10 e-assessment questions, until the student reaches the 40th question or the last question of e-assessment phase. In addition, we also consider that a course is consisted of several modules and each module contains at least 1 quiz and 1 activity. Moreover, the maximum number of quiz and activity does not exceed 2 for each one. In this case, if we have P modules belonging to the course then the quiz number is equal to 2P as well as the activity number is also fixed to 2P. We also assume that this supposition, 2P characteristic, gives the capability to generate a challenging question from a maximum number of existing cases which will be used during e-assessment phase. We present hereinafter the achieved simulation results, which indicate how the input parameters affect the considered output parameter of our system.

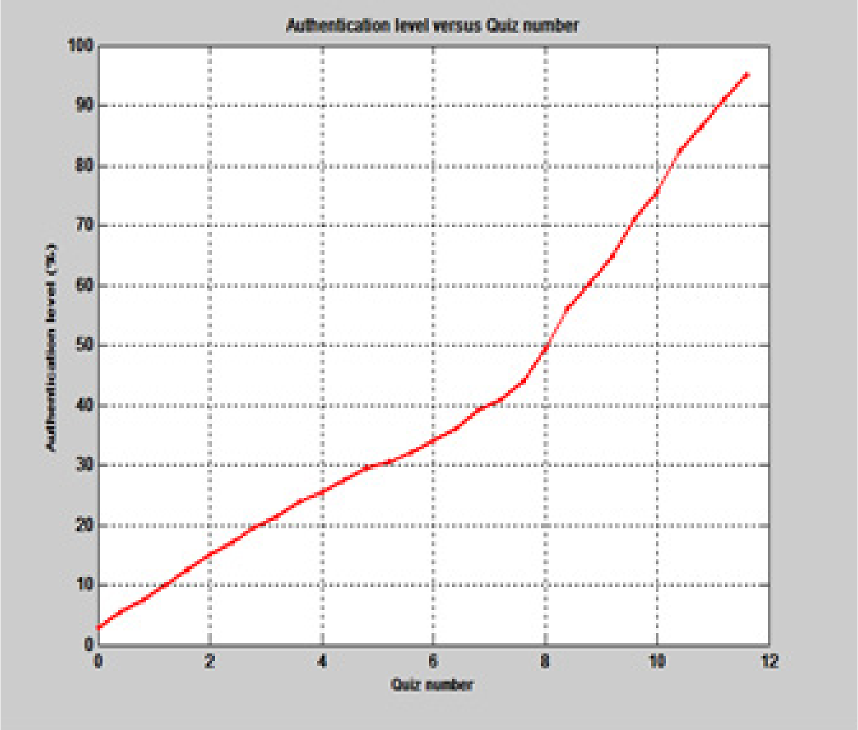

Fig. 7. Authentication level versus quiz number.

Fig. 7 plots the authentication level versus the impact of the quiz number when the activity modules are equal to 10. The challenge question is fixed to 5 questions which are given after 10 assessment questions. In this experimentation, we suppose that the maximum waiting time related to challenging question is fixed to 1 minute for providing the capability to the student to give the accurate response to the generate challenging question. Moreover, the threshold for each challenge question is fixed to 3 times. The choice of this value can be explained as follows: because, the choice of the higher threshold will provide more chance to the student to interrupt and compromise the authentication information. However, the shorter threshold cannot give the requested time to the student for realizing the authentication process. Hence, if this threshold is exceeded the e-assessment process will be closed and the existing grade will be assigned to a student and the collected information will be stored in the databases. In this Fig., we observe that, the authentication level increases with the increase of quiz number. This is because the increase of quiz number growths the presence of information related to the dynamic profile of the student which will be used in generation process of challenging questions. In this case, the student cannot have the ability to interrupt authentication process and do not the capability to compromise the response of the challenging question when the number of quizzes done by the student is high. It can be seen when the quiz number is greater than 8 the authentication level becomes greater than 50% which is an acceptable ratio of the security supervision process. However, when quiz number is less than 8 a sensitive authentication level is attained.

Fig. 8 represents the authentication level versus the impact of the activity number when number of quizzes is equal to 10, and number of the challenging questions is fixed to 5. In this simulation, the same environment used, like the previous experiment, is performed for the following constraints such as waiting time and challenging question threshold. In this Fig., we observe that, the authentication level increases with the growth of activity number. This is because the increase of activities number improves the presence of information related to the dynamic profile of the student which will be used in the generation process of the challenging questions. This behavior has a positive impact on the authentication technique, which can activate the appropriate supervising process of the relationship between the authorized student and e-assessment. In this Fig., it can be seen when the activity number is between 16 and 18the authentication level becomes greater than 50%, which is an adequate level of the security supervision procedure. However, when activity number is less than 16 a sensitive authentication level is achieved.

Fig. 9 illustrates the authentication level versus the impact of the challenging question number. In this simulation, we use the similar environment applied in the two previous experiments. In this Fig., we observe that, the authentication level or ratio increase with the growth of challenging questions number. This can be explained as follows: the increase of this input parameter improves the presence of the information related to the dynamic profile of the student. This behavior has a positive impact on the authentication procedure which can trigger the suitable supervising process of the relationship between the authorized student and e-assessment. In this Fig., it can be seen when the challenging questions number is between 4 and 5 the authentication level becomes greater than 50% which is an appropriate level of the security supervision procedure. However, when challenging questions number is less than 4 a sensitive authentication level is attained.

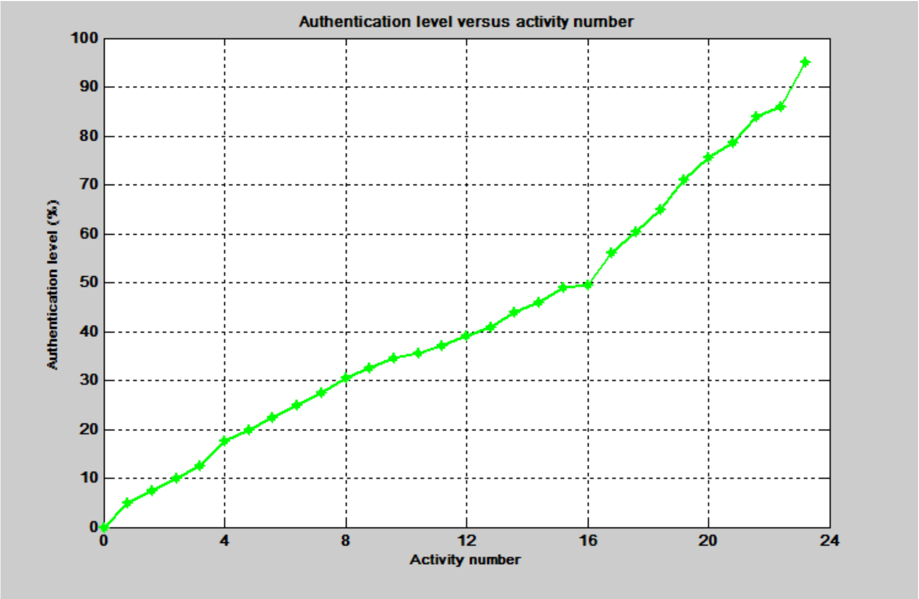

Fig. 8. Authentication level versus activity number.

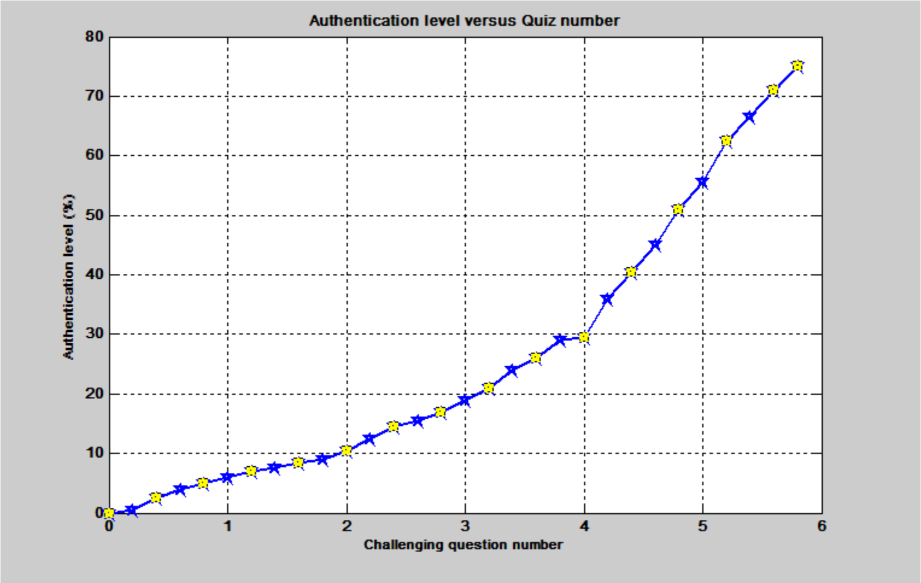

Fig. 9. Authentication level versus challenging questions number.

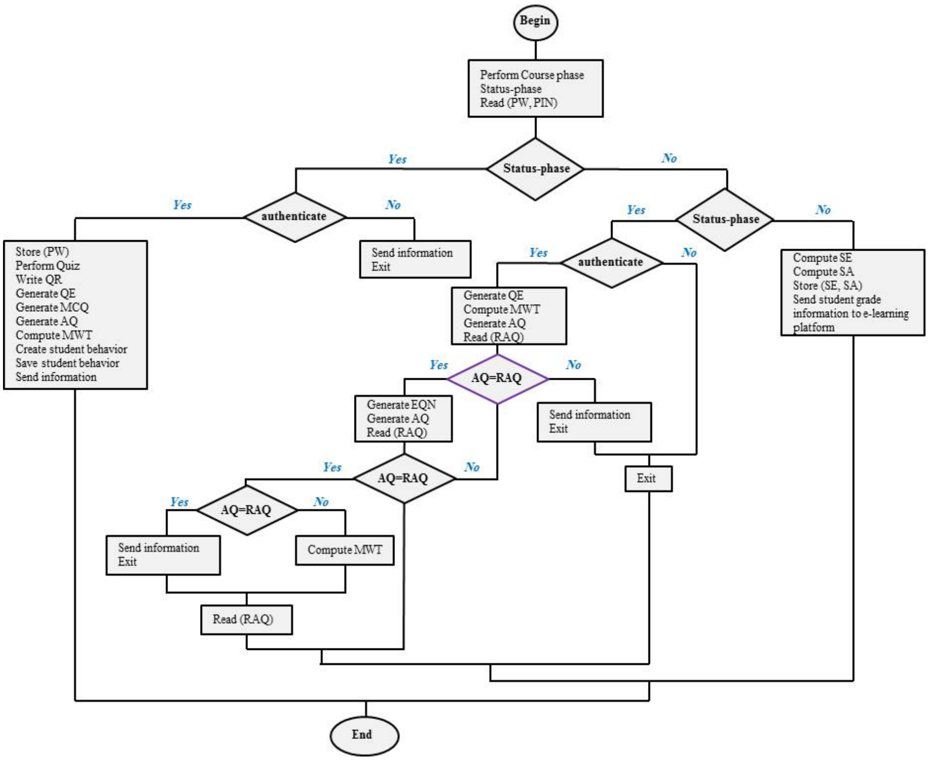

Fig. 10. Algorithm of the proposed authentication scheme.

6 Analysis and discussion

According to the previous findings, security of e-assessment is a significant process to ensure success of e-learning environment especially summative assessments that would be an important measure toward final course mark. A summative e-assessment system is supposed as secure, when realizing the students' identity and authentication security goals. With regard to the existing LMS of D2L based on e-assessment security model at UQU, we found the following assessment tools similar to quizzes, self-assessment are depended on username/password access by students which it might be discovered or passed from student to other easily during assessment process in the academic year. Therefore, the proof is achieved if the student accessed correctly. Additionally, the instructor should guarantee usually the presence and identity of each student before performing the e-test at lab. However, the instructor can find a huge difficulty to authenticate students' identity if he attempted to execute the test online away from the university campus. So, our research investigation assigned towards supervised and non-supervised environment.

In the same frame, previous literature have indicated that detecting an appropriate authentication of students through e-assessments is a stimulating problem and a major issue [13, 14, 15, 26]. In response, this paper explored the need to identify a suitable authentication technique specific to the e-learning environment (D2L portal). We used the knowledge technique due to increased cost of biometric techniques, the cultural nature of students at UQU. At the beginning, we suggested structure of authentication model via analyzing the current context diagram of the system "e-assessment". The main system included three key sub-processes as pre-e-assessment, during e-assessment process, post-e-assessment. It included all processes that are controlled by the instructor and administrator that facilitated the next process, where is the "during e-assessment" process, it presented all relation during e-assessment processes of each student that are linked to e-learning server, in addition to, data flow between each process. While, the "post-assessment" processes are linked to data store represented to grade file of the student.

Based on the system analysis, we developed an advanced algorithm that combined the knowledge and behavioral of the student as well as others mechanisms and parameters including time handling and questions supervision. The e-learning platform, upon receiving the incoming request related to student e-assessment attempted to identify the student based on student knowledge level including username and password. Then, generating the e-assessment stage updates the status of students based on the course parameters. If student is authenticated e-assessment phase starts and the authentication information related the student is switched between e-learning platform and e-assessment phase as well as the concerned student. In this case, each student provides the appropriate response to the authentication question related to his behavior and collected information during learning activities. The non-authenticated student is being recalled until he exceeds the authorized number of response or the authorized delay threshold is reached. When the threshold is reached, the e-assessment phase is closed and information is be transmitted to the student and the concerned faculty member. Accordingly, the student behavior information is updated dynamically at each e-assessment phase related to course components including activity and quiz.

The validity of the developed simulation model is performed. The generation of the input parameters, simulations experiments are conducted using a well-used statistical method, which may improve the credibility of our simulation model. The principal metric has been chosen to evaluate the performances of our proposal is authentication level which is handled and managed by the different considered input parameters. The proposed scheme is based on various parameters of implementation. The current e-learning platform needs to maintain student behaviors and information such as student assessment as the information related to the course including quiz number and quiz evaluation or grade.

With regard to the previous research, numerous investigators dealt with the authentication problem from several aspects, the main related issue related to our research topic rely on using the challenge questions as a knowledge method. Challenge questions were used to authenticate online examination students. The advantage was it is easy to implement without need for additional hardware.

Consequently, our approach is depended on constructing a novel scheme that based on unusual techniques for achieving reliable learning results. In addition, assuring the guarantee of each student's performance and his real knowledge acquisition can achieve quality assurance related to criteria of the instructional programs. Results of the current paper support the previous research and studies that dealt with Knowledge factor based on authentication for instance. With regard to the earlier research [2, 13, 14, 15, 36], they indicated that authentication have been addressed from different aspects, the related issues to our research topic that rely on using challenge questions as a method, via a proposing a new approach known as profile based authentication framework (PBAF). Challenge questions were used to authenticate online examination students. The advantage was it is easy to implement without need for additional hardware. Results of our paper agree with that suggested PBAF, which used a timing mechanism that locks out students after a fixed period. However, our authentication scheme is related to challenge questions as an effective technique, the questions were designed well to meet security challenges. The challenge questions are based on student profile, learning activities process over D2L environment that involves main tools for e-course such as content, communication and student management as well as assessments. The main components of system simulation included the following student class and level, student profile, course components, quiz parameters and activity modules as well challenging questions. The considered parameters related to challenging question consisted of question number, question response, question status and waiting time as well as the constraint related to the authorized entry for responding to the concerned question. Consequently, our approach is to build a novel scheme that based on unusual techniques for achieving reliable learning results. In addition, the guarantee of each student's performance and his real knowledge acquisition can achieve quality assurance related to criteria of the instructional programs.

Finally, the current paper appears different to the earlier research, especially to the considered papers, because it covers three main stages or contributions including system modeling, algorithm design and simulation experiments. The three stages cooperated for offering a complete and efficient scheme for a safe authentication of e-assessments based on student behavior over e-learning platform. In the first contribution, we have developed an appropriate model suitable for the student evaluation by means of information knowledge and behavioral as well as dynamic access management. In the second contribution, we have developed a dynamic algorithm that combines two data collection methods including course data and student behavior. This algorithm is consisted of three phases including as core treatment e-assessment phase and two others phases as supporting treatment which includes pre e-assessment phase as well as post e-assessment. The last contribution is about simulation experiments in which the authentication level is provided based on use of the challenging questions, quiz parameters and activity constraints. A simulation experiments has been performed to evaluate the efficiency of the offered authentication and validate the proposed scheme. The simulation results demonstrated that the proposed scheme could effectively enhance the authentication level for e-assessment. We provide through the simulation work that the proposed model is a flexible solution suitable for handling the varying student behavior and course parameters. Moreover, the results of our paper added to learning management system need to authenticate at e-learning activity level for summative e-assessments using suitable authentication strength to ensure the identity of the remote student. Then, the proposed approach oriented e-assessment and authentication can be extended to provide advanced level of security provision, which will introduce other security parameters such as confidentiality, integrity and availability over a dynamic e-learning platform.

7 Conclusion

The advances of information technology systems have supported the e-learning systems usage by the educational institutions in teaching and evaluation including e-assessment and e-exam. However, e-learning users such as faculty members and students as well as data have raised security issues related to e-learning systems. In this paper, we have mainly addressed the issue of the students' authentication problems because the current existing model is insufficient within e-learning platform related to e-assessments. For this purpose, we proposed a novel security scheme that contributes in resolving the e-assessment authentication problem due to threats of e-assessment could lead to a negative impact on the credibility of online learning users that make use of summative e-assessments. E-assessment involves an intermediate phase on the design of an advanced e-exam authentication scheme. This scheme addresses this authoritative problem by proposing a novel approach that incorporates available databases authentication technologies in conjunction with e-learning environments for controlling unethical behavior through evaluation of e-learning environment.

Moreover, the proposed scheme considers the continuous random authentication using students' information stored during the course in the databases that guarantee their identity and authentication during the assessment process. The proposed scheme is evaluate during a simulation work in which virtual e-learning platform similar to D2L has been designed. Simulation results have shown that the proposed approach can effectively improve the authentication process using course components and students information with respect of providing the requested pedagogical features. The results of the current paper contributes particularly to the body of knowledge, and have several implications within the field of authentication for the future development of e-learning system. Moreover, the outcome of our study could provide a significant model that could be applied to assure and achieve student authentication within e-assessment for education policy makers so that it effect positively on the quality of learning process.

8 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 Confer-

ence on Security of Information and Networks, NY; USA, Association for Computing Machinery.

[4] Levy, Y. & Ramim, M., (2007) "A Theoretical Approach for Biometrics Authentication of e-Exams", Nova Southeastern University.

[5] Kennedy, K., Nowak, S., Raghuraman, R., Thomas, J., & Dacis, S. (2000) "Academic dishonesty and distance learning: student and faculty views" College Student Journal, 34(2), 309-315.

[6] Pillsbury, C. (2004). "Reflections on academic misconduct: An investigating officer's experiences and ethics supplements", Journal of American Academy of Business, 5(1/2), 446-454.

[7] McLafferty, C. L., & Foust, K. M. (2004) "Electronic plagiarism as a college instructor's nightmareprevention and detection: Cyber dimensions", Journal of Education for Business, 79(3), 186-190. https://doi.org/10.3200/JOEB.79.3.186-190

[8] Sarita & Dahiya, R. (2015) "Academic cheating among students: pressure of parents and teachers", International Journal of Applied Research, 1(10), 793-797.

[9] Levy, Y. & Ramim, M. (2009) "Initial Development of a Learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM)", Interdisciplinary Journal of E-Learning and Learning Objects, 2009, (5), 380-396.

[10] Sung, Y.T , Chang, K. E. & Yu, W. C. (2011) "Evaluating the reliability and impact of a quality assurance system for E-learning courseware," Computers & Education, 57 (2), 1615-1627. https://doi.org/10.1016/j.compedu.2011.01.020

[11] Rashad, M., Kandil , M., Hassan, A. & Zaher, M. (2010) "An Arabic Web-Based Exam Management System", International Journal of Electrical & Computer Sciences IJECS-IJENS, 10 (1), 48-55.

[12] EL-Emary, I, & Al Sondos, J. (2006) "An Online Website for Tutoring and E-Examination of Economic Course", American Journal of Applied Sciences 3 (2), 1715-1718. https://doi.org/10.3844/ajassp.2006.1715.1718

[13] Schechter, S., Brush, A., Egelman, (2009) "Measuring the Security and Reliability of Authentication via". In 30th IEEE Symposium on Security and Privacy. CA, USA: IEEE.

[14] Ullah A., Xiao H., Lilley M, (2014) "Evaluating security and usability of profile based challenge questions authentication in online examinations", Journal of Internet Services and Applications, December, 5:2. https://doi.org/10.1186/1869-0238-5-2

[15] 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.

[16] Dominici, G., & Palumbo, F., (2013) "How to build an e-learning product: Factors for student/customer satisfaction", Business Horizons, 56, 87-96, 2013. https://doi.org/10.1016/j.bushor.2012.09.011

[17] Kong, S., Chan, T.-W., Griffin, P., Hoppe, U., Huang, R., Kinshuk, et al. (2014) "E-learning in school education in the coming 10 years for developing 21st century skills: Critical research issues and policy implications", Educational Technology and Society, 17(1), 70-78.

[18] Scott, C. L. (2015) "The Futures of Learning 3: What Kind of Pedagogies for the 21st Century?, United Nations Educational", Scientific Cultural Organization (UNESCO).

[19] Bichsel, J., (2013) "The State of E-Learning in Higher Education: An Eye tword Grwoth and Increased Access (Research Report)", Louisville, Co: EDUCASE Center for Analysis and Research, available from http://www.educase.edu/ecar.

[20] Navimipour, N. & Zareie, B., (2015) "A model for assessing the impact of e-learning systems on employees' satisfaction", Computers in Human Behavior, 53, 475-485. https://doi.org/10.1016/j.chb.2015.07.026

[21] Alkhalaf, S., Drew, S. AlHussin, T., AlGhamdi, R., & Alfarraj, O. (2012) "E-learning Systems in Higher Education Institutions in the Kingdom of SaudiArabia: Attitudes and Perceptions of Faculty Members", Procedia-Social and Behavioral Sciences, 47, 1199-1205. https://doi.org/10.1016/j.sbspro.2012.06.800

[22] El-Sabagh, H. A. (2015) "Evaluation of Blended Courses Design for Quality Assurance and Continuous Improvement at Umm Al-Qura University", 4th – International Conference For e-learning & Distance Education, Riyadh, KSA, 2015. available online, http://eli.elc.edu.sa/2015/sites/default/files/144.pdf.

[23] Al-Saleem, S., Ullah, H., (2014) "Security Consideration and Recommendations in Computer-Based Testing", Scientific World Journal. https://doi.org/10.1155/2014/562787

[24] Huszti, A., and Petho, A. (2008) "A Secure Electronic Exam System", Informatika felsőoktatásban. 1-7.

[25] 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

[26] Apampa, K., Wills, G., & Argles, D. (2010) "An approach to presence verification in summative e-assessment security", Information Society (i-Society), International Conference on, London, 647-651.

[27] Sabbah, Y., Saroit & Kotb, A. (2012) "A Smart Approach for Bimodal Biometrics in Home-exams (SABBH model)". CIT Int. Biometrics Bioinf, 4, 32-45.

[28] Adebayo, O. & Abdulhamid, S. (2010) "E- Exams System for Nigerian Universities with Emphasis on Security and Result Integrity", International Journal of the Computer, the Internet and Management (IJCIM), 18 (2).

[29] Barik, N., (2012) "Security Issues Related to E-Assessment: A UML based Approach", International Journal of Advanced Research in Computer Science, 3 (2).

[30] Rui C. Paiva1, Milton S. Ferreira1, Ana G. Mendes, and Augusto M. J., (2015) "Interactive and Multimedia Contents Associated with a System for Computer Aided Assessment", Journal of Educational Computing Research, 15 (2), 224–256. https://doi.org/10.1177/0735633115571305

[31] Anderson, L. W. and Krathwohl, D. R., et al. (Eds..) (2001) "A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Allyn & Bacon. Boston, MA (Pearson Education Group).

[32] Abdelkarim, N., Shukur, Z. (2015) "Review of User Authenyication Methods in Online Examination", Asian Journal of Information Technology, 14 (5), 166-175, Online Available from: https://arxiv.org/ftp/arxiv/papers/1402/1402.0921.pdf

[33] Meyers et al., "Impact Results of the eMINTS Professional Development Validation Study", EDUCATIONAL EVALUATION AND POLICY ANALYSIS, vol. 38 no. 3, 455-476, 2016. https://doi.org/10.3102/0162373716638446

[34] Redecker, c. (2013) "The Use of ICT for the Assessment of Key Competences, Luxembourg", Publications Office of the European Union, 2013, doi:10.2791/87007.

[35] Marais, E., Argles, D. and von Solms, B. (2006) "Security Issues Specific to e-Assessments". In, 8th Annual Conference on WWW Applications, Bloemfontein, 08 - 06.

[36] Ullah A., Xiao H., Lilley M, (2012) "Profile Based Student Authentication in Online Examination", International Conference on Information Society, 2012.

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

[38] 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

9 Authors

Yassine Khlifi received M.S. degrees and Ph.D. in information and communications technologies from High school of communication (Sup’Com) of Tunisia in 2002 and 2007 respectively. 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 especially signaling, switching, routing, grooming and QoS provision as well as networks protection and security.

Hassan A. El-Sabagh received Ph.D. degree in the field of Educational Technology from Dresden University of Technology, Germany, in 2011. Since 1999, he works mainly at Computer Department, Faculty of Specific Education, Mansoura University, EG. H. El-Sabagh is currently an Assistant Professor of e-Learning at Umm Al-Qura University Makkah, KSA. His current research interests include eLearning Environments Design, LMS based Interactive Tools, Design Personalized & Adaptive Learning Environments, Quality & Online Courses Design, and Security issues of eLearning Environments.

Article submitted 01 December 2016. Published as resubmitted by the authors 11 February 2017.