Hybrid Authentication Combining Student Behavior and Knowledge for E-Evaluation Transparency and Equity Over E-Learning Platform

https://doi.org/10.3991/ijet.v17i21.32825

Yassine Khlifi[1,2](✉)
[1]Deanship of Scientific Research, Umm Al-Qura University, Saudi Arabia
[2]Research Member Digital Security Lab., SupCom, Carthage University, Tunisia
yrkhlifi@uqu.edu.sa

Abstract—COVID-19 has forced academic organizations to migrate rapidly to distance education or online (electronic) learning (e-learning) owing to its benefits, mainly offering innovative teaching and transparent evaluation. However, e-learning stakeholders, faculties, staff, and students have evoked evaluation security concerns regarding authenticating takers during the electronic evaluation (e-evaluation) comprising electronic assessment (e-assess) and examination (e-exam). This paper presents a hybrid scheme that resolves this challenge using a dynamic authentication method for supervising e-evaluation. This approach builds an active student profile employing students' information and behavior gathered during the courses' activities and uses them for managing unethical conduct during e-evaluation. The proposed scheme ensures continuous authentication using active questions made using operational students' profiles without a need for added components and extra cost. The student answers to the set of random queries developed dynamically, in terms of time and information, to ensure real-time authentication with e-evaluation transparency and equity. A mathematical model is developed and employed utilizing students' and courses' contents to enable a dynamic authentication algorithm throughout e-evaluation. The obtained results of the simulation work show that the authentication requirements are guaranteed at a low cost regardless of student number, e-evaluation content, anytime, and anywhere.

Keywords—e-learning platform, e-evaluation, hybrid authentication, student behavior, student knowledge, mathematic model, simulation

1 Introduction

Internet utilization is vastly expanding with the appearance of advanced tools, applications, and services, mainly multimedia, distributed data processing, and videoconferencing, specifically online learning (E-learning). Several educational institutions support e-learning usage owing to the benefits, especially by offering innovative teaching and transparent and fast evaluation. Faced with COVID-19, most academic institutions are forced to rapidly migrate to e-learning platforms to ensure the continuity of the

educational system, where enabling traditional evaluation is unreachable. Due to this concern, online evaluation (e-evaluation) is starting to replace classic evaluation by triggering online assessment (e-assess) and online examination (e-exam). E-evaluation employs innovative operational methods to offer multiple benefits, particularly opportunities for the highest learning, automated and evident marking, and immediate feedback. Moreover, it can provide the academic learning demands of students and staff and improve the quality of teaching outcomes [1].

E-evaluation operates with an e-learning infrastructure using the Internet platform supposed as a vulnerable environment disclosed to a set of illegal activities, explicitly several varieties of threats. E-learning stakeholders, particularly managers, faculty members, and students, are concerned about e-learning infrastructure utilization due to the stated security issues [2]. These security concerns, especially identified during e-evaluation usage, should be resolved to provide a safer, fair, and transparent location for student evaluation. E-evaluation problems can be alleviated using different security services, notably confidentiality, integrity, availability, and authentication. These services guarantee that e-learning stakeholders are safe against threats and risks. However, security approaches try to protect the e-learning environment which is typically composed of several resources such as hardware, software, and data from potential menaces. These menaces attempt to control the existing weaknesses resulting in non-legal actions employing fabrication, interception, modification, and interruption [3].

The mentioned vulnerabilities are often alleviated and resolved using the reliable tools implemented and upgraded according to the defined requirements on the distinct access points of the employed network of the educational institution. Most e-learning stakeholders reveal that the existing platforms are not wholly secure and entirely utilize suitable mechanisms related to student authentication when operating e-evaluation. Providing authentication is a significant challenge in deploying e-learning due to interruption and compromission methods that occurred by unauthorized activities [4]. Authentication offers a student identification in the system admission, mainly the required information granted to access the authorized resources. Students' or users' authentication specifies the main security line of any infrastructure, particularly over e-learning platforms. The noted security factor represents a fundamental function in guaranteeing education equity and transparency in the evaluation techniques. The managers and faculty members of academic institutions are concerned about the authentication and security of the principal components of the e-learning platform, especially the learning management system (LMS) for enabling examination. Student unethical manners in e-learning evaluation are becoming the main topic in the educational strategy [5].

In our previous works, fixed and advanced schemes are employed to solve student authentication issues during educational evaluation [6, 7]. In [6], an innovative approach is used to ensure constant authentication and unethical behavior control using an innovative model. This method employs a practical solution combining a random question establishment guaranteeing authentication and cheating identification. It ensures continuous authentication by managing information related to students and courses during activities. In [7], an authentication scheme is used where a scalable model is employed to manage e-assessment and overcome authentication concerns. This scheme handles real-time student information with authentication to supervise

unethical behavior during e-assessment taking. The presented approach enables an applied solution joining in a random test authentication during assessment reducing exam cheating. This approach incorporates constant random authentication using the information collected and stored in the databases to confirm student presence, identity, and authentication.

The presented approaches deliver the required environment that ensures student authentication during the e-evaluation, especially e-assess and e-exam. Nevertheless, with the emergence of new services and applications over the existing e-learning platform, students try to create additional techniques to overcome the verification of their identification and authentication during different educational activities, especially during e-evaluation procedures. This concern produces a need for an innovative authentication scheme to identify the dynamic behavior of students and ensure their authentication anytime and anywhere. For this reason, the current research work investigates a hybrid student authentication to solve the newly identified and discussed concerns, including student behavior and activities management, and ensure the authentication depending on the student actions ‘types, e-evaluation content, time, and location.

This work comprises the following sections. Section 2 discussed and analyzed the current research works related to student authentication during e-evaluation. Section 3 introduced the proposed approach design, the developed analytical model, and its algorithm. Section 4 described the experimental work and discussed and analyzed the obtained results to verify the efficiency and effectiveness of the introduced approach. Finally, section 5 concludes the work.

2 Related works

Student evaluation comprises two types of online formative and summative, where the first one ensures learning improvement and provides information about their progress to show a final course impact. However, the second type defines a learning advancement and delivers intermediate feedback to enhance the learning results. With COVID-19, e-evaluation, comprising e-assessment and e-exam, is presented as a principal strategy for student evaluation covering the course material. E-evaluation can reach the effects expected or planned by faculty members and instructional institutions. It depends on a learning management system that increases security issues in the e-learning environment. Yet, the e-evaluation should achieve all the features offered by traditional paper-based exams, mainly security requirements, by enabling the appropriate scheme considering authentication issues.

Multiple approaches managing e-learning user security are introduced, especially in the e-evaluation procedures ensuring the control of students ‘identification and authentication [8, 9]. In [8], a new examination system is proposed for assuring user authentication using facial expression recognition. The proposed method incorporates the design of a facial database from the captured images. It also integrates artificial intelligence (AI) using a system for facial feature extraction and its classification utilizing intelligent Agents. Moreover, it contains the authentication of separate users by automatic identification of facial images. The obtained results of experimental work show that the proposed method can handle the confirmation of the authenticated

users and provide security over the e-learning platform. A novel approach to avoiding the presence of a proctor during the examination is investigated using an intelligent examination system [9]. This method is presented to enhance e-learning by employing an advanced question bank and examination system. The system is developed with diverse complexity levels included in the questions and used as a device for evaluating the student's knowledge through the teaching procedures. This system operates with just-time supervision and offers an acceptable level of security. The proposed methodology includes the question design bank stored in a database and the design of the artificial intelligence (AI) system for examination and evaluation.

In [10], the authors analyze the various security challenges identified during the usage of the e-exam procedure. The authors introduce an innovative approach based on attacks and defense tree approaches to solve the determined concerns. The attack tree scheme is enabled to specify the different risk assessments. The attack tree approach is employed to evaluate the e-exam application according to penetration test experiments over a server operating the e-exam application. A new defense tree scheme to overcome the identified attack tree is developed and utilized as a procedure to design equivalent e-exam systems. This scheme is employed to fix the existing attacks using a defense tree and ensure a secure e-exam process. The discussed technologies comprise engineering, machine learning, and psychometrics for a test security framework [11]. The examined techniques are employed to create systems and protect the integrity of test scores. This approach incorporates methods for actively and passively detecting and preventing malicious behavior using a large item bank created through an automatic establishment procedure. It includes test administration experiences containing both automated and human reviews. The proposed approach integrates various tools and techniques for maintaining the security of assessments of the score reliability, interpreting and validating the different test scores.

A comprehensive analysis using a biometric behavioral authentication system is presented, in which keystroke dynamics and neural network classifiers are used [12]. The obtained results of experimental work indicate that keystroke dynamics can deliver an acceptable level when used as a dual authentication element. The different roles of no timing and timing features are demonstrated, where the cited characteristics maintain a significant role in enhancing performance measures. The proposed model is considered the appropriate enhancements compared to the reported results given by the existing approaches. In [13], the authors investigate the impact of perceived security on e-learning acceptance among university students using the technology acceptance model (TAM). This model uses a cross-sectional design to collect and process from several university students based on an online survey. The data analysis demonstrates that perceived security positively affects the intention to use e-learning via the mediator or perceived usefulness. A positive impact is seen related to perceived security comprising the benefits and ease of usage. The obtained results give the opportunities to propose new orientations and recommendations for the e-learning stakeholders comprising managers, faculty staff, and students.

A novel approach to define the access created by the legitimate user is presented using fast identity online (FIDO) [14]. The comparison and analysis indicate that the proposed method shows that security levels stay higher than the existing methods. The presented scheme can assure the control of cheating comportment may make by

illegal or legal users. The proposed technique can enable suitable users 'usage in safer conditions over mobile and web environments. This scheme provides an appropriate platform for user authentication with the development of e-learning needs and constraints. In [15], the authors present the research results and conclusions on the usage and acceptance of e-learning systems by students in higher education. The research utilizes an extended version of the technology acceptance model (xTAM) employing structural equation modeling (SEM) and the AMOS virtual program. The proposed approach explores several external elements and emphasizes information technology (IT) security awareness as a crucial importance element of the internet infrastructure, focusing on personal data protection. The evaluation of IT security awareness reveals the behavior of students using e-learning systems.

A systematic literature review (SLR) online examination is accomplished to determine and examine online exam features that contribute to developing approaches to implement online exam solutions [16]. Various techniques, algorithms, and datasets are proposed to design multiple online exam tools. The participation of countries in online exam research is investigated where the main factors for the global usage of online exams are compared with major online exam features. This approach can select the right online exam system for a particular country based on existing e-learning infrastructure and overall cost. The introduced method provides a solid platform to identify the appropriate features comprising tools and techniques to design and implement a particular online exam solution according to the needed requirements. In [17], didactic characteristics related to the assessing operation of students are examined. The concept of learning outcomes and classification theory is utilized to automate the assessment in e-learning and distance education environments. Several approaches are employed to establish the correspondence of the completed education tasks to the learning outcomes with the distinction of variable learning tracks. A formulation of the problem of building classification and an estimation algorithm using artificial intelligence systems are developed. The obtained results permit the identification of the different conditions and limitations related to the proposed approach.

Although e-learning security, especially authentication, is a significant issue in e-evaluation, the discussed approaches and techniques describe valuable contributions. However, they did not inspect the different parameters and factors such as simplicity, transparency, and equity asked by a large part of the students. Moreover, they cannot offer realistic feedback about the educational procedure and the expected outcomes by the academic staff. The investigation of the mentioned parameters is performed to confirm the balance between students' requirements and education procedure. This orientation is analyzed and introduced during the design and implementation of the proposed security scheme over the presented e-learning platform.

The main objective of the focused improvement is to ensure e-learning usage that guarantees the requirements of educational institutes, including learning, teaching, and evaluation while providing the expected outcomes. First, with the appearance of new needs provoked by the COVID-19 pandemic, the existing e-learning platform cannot support the constraints and rules of e-evaluation. The second motivation behind this goal is to enable hybrid authentication control in the different components to manage student identification and handle resources in the case of the presence of unauthorized occurrences. The third purpose is to optimize the cost of the e-learning platform to improve

university resource usage and avoid new challenges requiring additional components, especially biometric devices, to guarantee authentication during e-evaluation. The last orientation is to make easy specific courses evaluation hardly completed due to the significant number of students and the limited academic staff.

3 Hybrid authentication scheme

3.1 Descriptions and assumptions

E-evaluation is provided using several techniques comprising biometric features and components, resulting in an additional cost for the higher academic institute. This cost introduces a load on the institutes funding to develop the education procedures and strategies. Moreover, the stakeholders of the education environment are not entirely convinced about e-learning usage in all stages of educational operation, mainly during the COVID-19 pandemic, because it can affect the learning outcomes. Consequently, the proposed approach must consider the mentioned issues and tries to solve the identified constraints in the employed e-learning platform, in Saudi Arabia, especially at Umm Al-Qura University (UQU). The introduced scheme uses student behavior and knowledge information related to the teaching processes and course contents. It also employs the data collected and stored to generate e-evaluation, comprising the different e-assess and e-exam occurrences, as depicted in Figure 1.

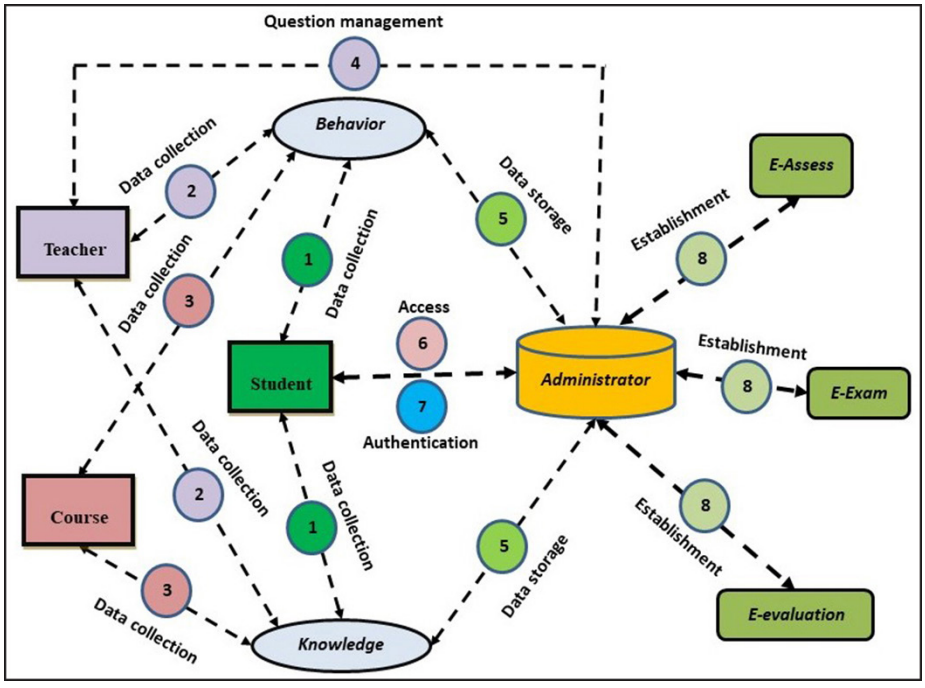

Fig. 1. Hybrid authentication system

The design and implementation of the proposed approach require the definition of some assumptions described and explained in the following. These assumptions permit considering the distinct constraints when developing the e-learning environment that conducts suitably the e-evaluation system and manages data operations. These assumptions are presented and discussed as follows:

- The students' access to the course in the e-learning platform is completed based on private information given by the concerned service in the academic institution.
- This private information concerning students is offered by the administrator managing the e-learning platform used to access the cited infrastructure.
- This information must be changed by the student at least every month during the academic year. If this information is not modified, then student access is declined.
- The student access to the e-evaluation, specifically e-assess and e-exam, is made employing another delivered secret information.
- This secret information ensures the access to evaluation is generated automatically and sent to the student before the e-evaluation and previously a limited time.
- This time is supervised by the access system and managed by the administrator.
- The continuous authentication of the student during e-evaluation is handled using a generated question that needs a response made by the student.
- The student has three opportunities to give his response concerning any authentication question.
- The number of authentication questions is managed according to the type of e-evaluation, its content, and advancement of student response during the e-evolution accomplishment.
- The authentication questions are generated automatically based on the time of response attempt depending on the data collected used to build student profiles employing behavior and knowledge.
- The time given to the student to answer to authentication question is given as extra time added to the e-evaluation interval time if the answer is provided in the first chance.
- A time-out is defined for the authentication question. However, if this time is expired, then the e-evaluation is locked.
- The behavior parameters are composed of information concerning student and teaching activities.
- The knowledge parameters comprise information relating to the learning and course events.

3.2 Mathematic model

The considered e-learning system operating with the proposed scheme needs to investigate a suitable authentication model that addresses the required parameters. The introduced or hybrid approach handles static and dynamic parameters simultaneously and manages two types of parameters that comprise information relating to the student profile and course activities. These parameters are collected, exchanged, and stored by the different components of the e-learning platform to generate an e-evaluation system. The e-evaluation design contains the authentication procedure composed of dynamic,

continuous, and random authentication questions. The built of authentication questions include the needed factors and equations utilized to support the conducted model comprising time-out to answer to authentication question, question number, attempt number to respond to authentication question, and attempt number to access, as illustrated in Figure 2. As also depicted in the mentioned figure, the e-evaluation procedure is improved dynamically using the feedback of the different components of the proposed model employing a hybrid authentication scheme that guarantee the requirements of all stockholders.

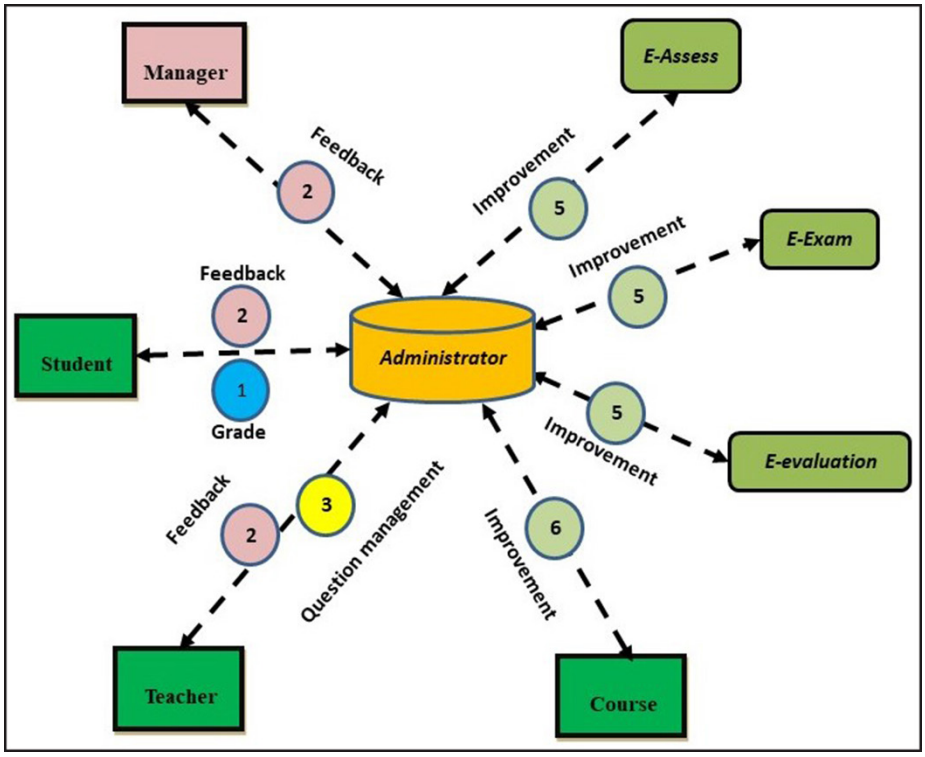

Fig. 2. Hybrid authentication model

Authentication parameters. For developing the hybrid authentication approach, several parameters and notations are needed, which are presented in the following:

- SAS: Student authentication status.
- SAT: Student authentication transparency.
- SAE: Student authentication equity.
- SAQN: Static authentication question number.
- DAQN: Dynamic authentication question number.
- SSR_j: Student static response to question i.
- SDR_j: Student dynamic response to question j.
- SN: Student number per level.

- RTSE: Real-time student evaluation.
- CSTE: Concerned time student evaluation.
- QT: Question type.
- ESN: E-evaluation student question number.
- QTN: Question type number.
- T: Type related to the evaluation question depending on function f.
- TN: Question type related to the evaluation depending on function g.
- f: Random variable generated for providing a set of question types.
- g: Random variable generated for providing a question number per question type.

Student authentication status. The student authentication status provides the outcome obtained if the student access is done, continuously verified, and the e-evaluation performed in the typical condition. The mentioned status takes a Boolean value extracted from the obtained integer value. This status is formulated using the equation (1) denoted by eq. (1):

$$SAS = Bool\left(Int\left(\frac{\sum_{i=1}^{SAQN} \mathrm{SSR}_i}{SAQN} \right) * Int\left(\frac{\sum_{j=1}^{DAQN} \mathrm{SDR}_j}{DAQN} \right) \right) \tag{1}$$

Eq. (1) describes the authentication parameters incorporating two types of authentications employed during an e-evaluation, where a variable number of authentication questions are created. These numbers depend on the evaluation content, mainly the number of e-evaluation questions and student behavior during the evaluation. The average response value related to the static and dynamic questions of the concerned students defines the authentication status denoted by the Eq. (1) formulated using student status response. The response status depends on the number of authorized attempts and the time-out provided to the student specified by the computed threshold. The threshold characterizes the student attempts that should be composed using static and dynamic authentication questions. The number of these attempts depends on the defined time-out relating to the static and dynamic authentication treated in the equation developed in the subsection. Therefore, the reply to the question is restricted by the try number and the specified time-out.

Student authentication transparency. The student authentication transparency delivers the result reached related to the e-evaluation time completed in the typical condition. The cited status presents the ratio compared with the mean student time of evaluation. This ratio is computed employing the equation (2) indicated by eq. (2):

$$SAT = \frac{CSTE}{\left(\frac{\sum_{i=1}^{SN} RTSE_i}{\mathrm{SN}} \right)} \tag{2}$$

Eq. (2) defines authentication transparency by combining two authentication times used during an e-evaluation where a concerned student evaluation time and evaluation

time related to the student of the same course level are incorporated. These times depend on the evaluation content comprising the number of e-evaluation questions and time-out of the static and dynamic authentications that appeared during one or a set of evaluations. The mean of student time indicated by MSTE is computed for all students and compared with each student. If this time is approximately equal to one, the transparency of authentication is guaranteed. The authentication transparency represents the ratio of student time evaluation divided by the mean student time evaluation using static and dynamic questions adding the evaluation time expressed by Eq. (2).

Student authentication equity. The student authentication equity can be computed if the concerned student makes successful access, using static and dynamic authentication, and ends in an adequate case the e-evaluation. The equity is calculated compared to the student in a similar class using the equation (3) indicated by eq. (3):

$$SAE = \frac{\sum_{i=1}^{ESN} QT_i \times QTN_i}{\left(\frac{\sum_{j=1}^{SN} \sum_{k=1}^{ESN} QT_{j,k} \times QTN_{j,k}}{SN} \right)} \tag{3}$$

Eq. (2) describes the authentication equity needed to provide the student efficiency of the authentication system. The equity ensures that each student using static and dynamic authentication has the same chance as all students of the equivalent class in terms of the question type and number. These parameters define the evaluation content incorporating the number of e-evaluation questions and time-out of the hybrid authentication used during the evaluation procedure. The student e-evaluation is computed and compared with the e-evaluation of all students having the equivalent level. If the obtained value is approximately equal to one, the equity of authentication is ensured.

$$QT = T \times f(T) \tag{4}$$

$$QTN = TN \times g(TN) \tag{5}$$

The equity formulation includes two functions, entitled f, and g, utilized to develop random values for operating the question type and number relating to the concerned e-evaluation. The equations (2) and (3), indicated by Eq. (2) and (3), use the above functions to design the e-evaluation content concept. These functions employ the mentioned parameters, denoted by T and TN, for computing QT and QTN and the student authentication equity, depicted by Eq. (3). The equity is achieved by computing the question type and its number for the concerned student divided by the sum of the cited value for all students belonging to the same level for a similar course.

3.3 Hybrid authentication algorithm

The introduced hybrid algorithm manages student access in e-evaluation operating with student behavior and knowledge that combines the required information of

academic staff and course activities. The algorithm includes advanced mechanisms and new parameters covering access time-out, authentication question number, authentication question type, and authentication attempt number. The mentioned time-out represents the timer that handles the period delivered to the student for submitting his response to the concerned question of the built e-evaluation. Personnel or individual evaluation is created for each authorized student to guarantee equity and transparency. The fast building of e-evaluation and the similar assigned for a different part of evaluation ensures the expected parameters. The second timer or threshold is incorporated to guarantee the needed transparency requested by each student. The assigned time-out is utilized to supervise the student during the transfer procedure of his answer related to dynamic authentication. This variable time depends on the question number in the concerned e-evaluation part. The student must give the correct response to assure continuous authentication of e-evaluation. If this reply is valid then the time provided to the student is added to the e-evaluation period, as mentioned in Figure 3.

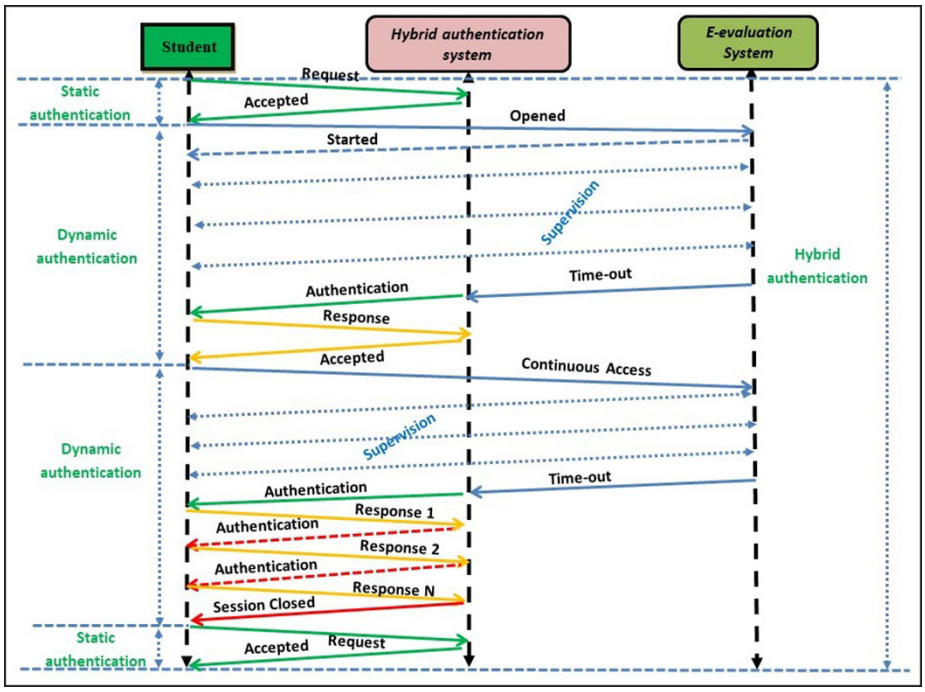

Fig. 3. Hybrid authentication method

This algorithm comprises the following five steps: data collection, data storage, e-evaluation establishment, e-evaluation feedback, and e-evaluation improvement. In the first step, the e-learning platform collects the data relating to students, staff, and course activities, comprising name, level, password, and PIN codes to build student profiles. Moreover, the e-learning platform creates behavioral information incorporating

student knowledge associated with the staff and course activities. In the data storage stage, e-learning databases store the processed data related to faculty staff and course actions to create the required information regarding student behavior and knowledge. In the e-evaluation establishment phase, the various evaluation containing e-assess and e-exam is built, reviewed, and supervised to confirm transparency and equity. The information related to e-evaluation feedback is gathered concerning e-evaluation stakeholders comprising students, staff, and managers during the e-evaluation feedback phase. In the e-evaluation improvement phase, the collected data is processed to improve the evaluation system and guarantee the needed authentication and the requested constraints demanded by diverse stakeholders of the e-learning platform. In addition to the parameters handled in the modeling, other parameters and notations are introduced in the proposed algorithm presented in the following:

- EQ: e-evaluation question.
- SSR: Static student response.
- DSR: Dynamic student response.
- EQN: e-evaluation question.
- SSAR: Sum of the static authentication response.
- SDAR: Sum of the dynamic authentication response.

Hybrid authentication algorithm

Input *(EQN). {e-evaluation question number}*
i=1. {First e-evaluation question i}
j=1. {First static access j}
k=1. {First dynamic access k}
EQ=1. {First e-evaluation question}
SSR=0. {Static student response}
DSR=0. {Dynamic student response}

```
1.      While i ≤ SN do
2.        While j≤ EQN do
            Input (SAR). {Static authentication response}
3.          While k ≤ EQN do
4.              If Response (SAR)== false
                  Exit
5.              Else
                  SAQN= SAQN +1 {Static authentication question number}
                  SSAR= SSAR +SAR.
                  SAQT= SAQT+ST.
6.              End
              k = k +1
7.            End
              Input (DAR). {Dynamic authentication response}
8.            While l ≤ EQN do
9.              If Response (DAR)== false
                  Exit
10.             Else
                  DAQN= DAQN +1 {Static authentication question number}
                  SDAR= SDAR +DAR.
                  DAQT= DAQT+DT.
```

```
11.                 End
                  l = l +1
12.               End
              SQT=SQT* QT*QTN.
              J=j+1.
13.             End
                CSDAR= SDAR +DAR.
               CSTE= ET+SAQT+DAQT.
               RTSE= RTSE+RT.
               PQT=PQT+QT*QTN.
               SSQT=SSQT+SQT.
                i = i +1
14.           End
              SAS= Bol (Int (SSAR/SAQN) *Int (SDAR/DAQN))
              SAT= CSTE/(RTSE/SN)
              SAE= PQT/(SSQT)
15.         If SAS ==True
               Output ='E-evaluation successfully done'
16.           End
17.         If SAT ==1
               Output ='E-evaluation transparency guaranteed'
18.           End
19.         If SAE ==1
               Output ='E-evaluation equity guaranteed'
20.           End
```

3.4 Toward a validation approach

The hybrid authentication scheme combines static and dynamic approaches, handling students' behavior and knowledge throughout their accesses and course activities. The data relating to the two cited methods are collected, stored, and improved during the different learning actions. If the e-learning platform receives a student demand for e-evaluation access, it enables static identification to validate the student entry. After the student's admission and according to his behavior, a dynamic authentication is activated utilizing a variable number of questions. These questions appear successively depending on a defined set of evaluation questions or time-out computed according to the e-evaluation question type. The question number and time-out are estimated based on the equations developed in the mathematical model. The usage of the mentioned parameters assures continuous authentication until the e-evaluation is completed or terminated due to the unsuccessful authentication. The proposed scheme solves the examined concerns while a validation procedure is required to show its performance and efficiency in a realistic e-learning platform or experimental environment. Due to the COVID-19 circumstances, the introduced scheme is experienced over a testing infrastructure employing a well-known simulation tool chosen to design the credible platform. This tool delivers the capability to create programs offering the potential of operating like a realistic e-learning system. The MATLAB tool represents the selected tool assuring the integration of the presented model and algorithm to reach powerful outcomes that will be generalized over the different e-learning systems comprising D2L, Blackboard, Moodle…etc. The authentication stage is the main output parameter

in the experimental work managed through the variation of diverse input parameters studied employing the outcomes of the mathematical model.

4 Validation approach

E-learning platforms can include the introduced improvements after validating and demonstrating their efficiency and efficacity. Experimental work is implemented and managed to prove the effectiveness of the modeled formulations and evaluate the different parameters related to the authentication during the e-evaluation.

4.1 Experimental platform

The simulation work is conducted employing the MATLAB tool that provides the ability to design a pseudo-real system similar to an e-learning platform. The considered tool delivers the capability to generalize the experimental environment assumed as the principal reason behind its utilization. The simulation model utilizes random generators, the generator of pseudo-random, and the uniformly distributed numbers of RAND incorporated the selected tool verified [20]. The input parameters are handled by integrating the sample size calculated by performing the well-used statistical method and the built simulation model validated in [21]. The considered output parameters to evaluate the scheme performance include authentication status, authentication transparency, and authentication equity. The input parameters are managed to verify their impacts on the cited output parameters comprising question number, e-evaluation number, and student number.

4.2 Platform description

The experimental system integrates and manages diverse information related to incorporating students, teachers (academic staff), courses, activities, knowledge, and behavior.

- Student: A profile assures the student identification, where this profile contains static and dynamic information. The static incorporates personal input comprising name, image, birth date, father name, mother name, PIN, …etc. The dynamic includes information related to the student activities comprising course, e-assess, e-exam, self-assessment, and feedback accomplished by the concerned student during the academic year according to his level. Five levels are examined presented as follows: 1, 2, 3, and 4, in which each one comprises a variable range of student numbers varying between 20 and 50. The objective behind the choice of five levels is to gather the precise situation of the students' behaviors and opinions during the course activities. Moreover, the level number provides an advanced stage for an innovative authentication approach design and operation, enhancing student acceptance and pedagogical conditions.
- Teacher or academic staff: A teacher profile is managed identically to the student profile comprising static or fixed and dynamic or active information. Like the

student, a static profile includes personal information. The dynamic profile contains data related to the course activities and e-evaluation feedback belonging to the class, level, and student during the academic year. The feedback improves the e-evaluation content, educational outcomes, and student transparency and equity.

- Course: The education elements include information relating to course modules, E-assess, and E-exams presented as follows:
  - Course modules comprise course title, content, quiz number, and quiz mark.
  - E-assess contains its number, title, mark, and feedback.
  - E-exam comprises its number, title, mark, and feedback.
- Activities: This information is related to the student activity built utilizing the data collected from the course module, E-assess, and E-exam.
- Knowledge: This information corresponds to the student knowledge created by employing the data assembled during the course module. The cited data comprises a response content to the question, attempt numbers, and response timer of a particular attempt.
- Behavior: This information relating to student behavior is produced based on the data collected from the course module concerning student academic staff. This information comprises question number, question response, question score, attempt number, the timer of individual attempts, student feedback, and teacher feedback.

4.3 Experiment results

The experimental work considers that student e-evaluation comprises a group of evaluation questions and a set of authentication questions. These authentication questions divide into static and dynamic, ensuring taker authentication using student knowledge, behavior, and feedback relating to student and teacher. The authentication questions are made and inserted in the e-evaluation based on mentioned parameters adding time-out as developed and described in the analytical model. The student behavior during the e-evaluation is also employed to define and enhance the build of authentication questions. The feedback provided by students and staff improves the usage of authentication questions by incorporating static, dynamic questions, time-out, and attempt numbers to respond to the authentication questions. The behavior during the different evaluations is employed to improve the time-out configuration and authentication question usage to ensure authentication efficiency, transparency, and equity. The static question appears after a set of dynamic ones if the number of attempts to respond to these equations is equivalent to a configured threshold time-out.

The experimental work evaluates the impact of three output parameters using two fundamental input parameters. The input ones comprise the parameters that can affect the different formulations developed in the mathematic model, containing the evaluation authentication question number presented by the authentication question ratio. This ratio is computed by dividing the authentication number by the e-evaluation question number. The considered output parameters incorporate the following parameters: student authentication status, student authentication equity ratio, and student authentication transparency ratio.

Figure 4 depicts the authentication status versus the authentication question ratio. The experiment starts with an input parameter equal to 1% and increases until it gets a 30%, and the output parameter decreases with the growth of the input parameters. This cited figure presents two curves where the first combines the mean of the results related to levels 1 and 2, and the second shows the outcomes obtained for students' classes 3 and 4. The obtained results for levels 1 and 2 are equivalent, and comparable outcomes are achieved by levels 3 and 4. The obtained authentication status for levels 3 and 4 is optimum than the one reached with the student with levels 1 and 2. The output parameter becomes similar for all student classes when the authentication question ratio achieves 30%. Then, the students of classes 3 and 4 can respond accurately to authentication questions and authenticate rapidly to assure e-evaluation questions continuity. In addition, the students of classes 3 and 4 manage their behaviors suitably during the courses and with the concerned teachers. The students of levels 1 and 2 find problems with supervising their behaviors and activities. In conclusion, the actions of these students, precisely classes 1 and 2, can be improved using the feedback provided during the different e-evaluation executed over their future academic years.

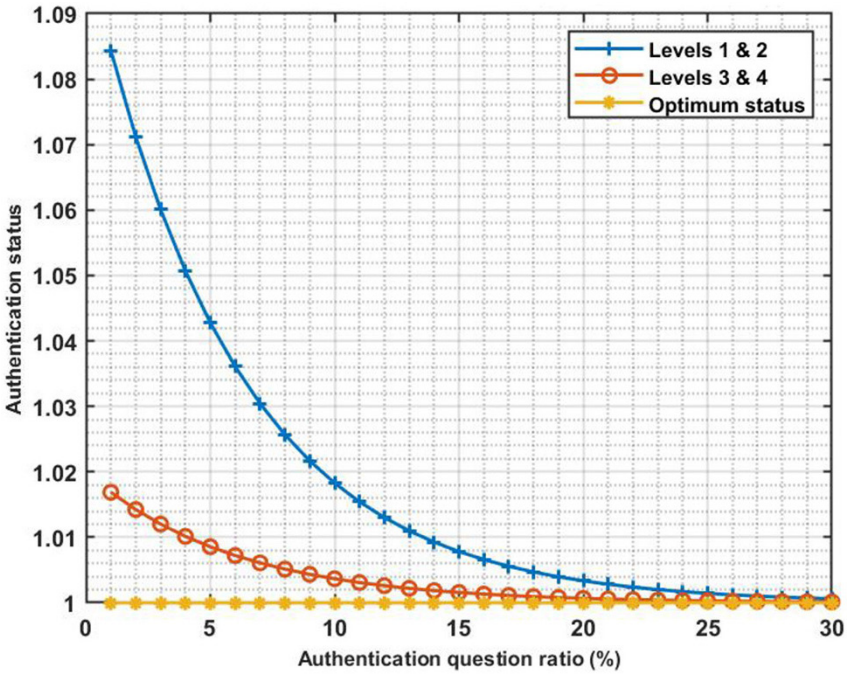

Fig. 4. Authentication status versus authentication question ratio

Figure 5 presents the authentication equity versus the authentication question ratio, and the simulation starts with an input parameter equivalent to 5% and growths until it becomes 30%. The output parameter diminishes with the progress of the input parameters, and this figure shows two curves similar to the orientation employed in Figure 4. The first curve combines the results of levels 1 and 2, and the second integrates the

outcomes of classes 3 and 4. The obtained authentication equity for levels 3 and 4 is optimum than the achieved by students with levels 1 and 2. The output parameter becomes more than 80% for all student classes when the authentication question ratio attains 30%. Based on the depicted curves, the students in classes 3 and 4 provide cooperative feedback utilized by academic staff and e-learning administrators to improve the e-evaluation content and authentication process. In addition, the students of classes 3 and 4 control their behaviors suitably during the improved courses and teachers' manners. However, the students of levels 1 and 2 deliver limited feedback creating several issues for them during the supervision of their behaviors and actions. In conclusion, the activities of these students, specifically class 1 and 2, decrease their equity during the different e-evaluation procedure and reduce the authentication validation.

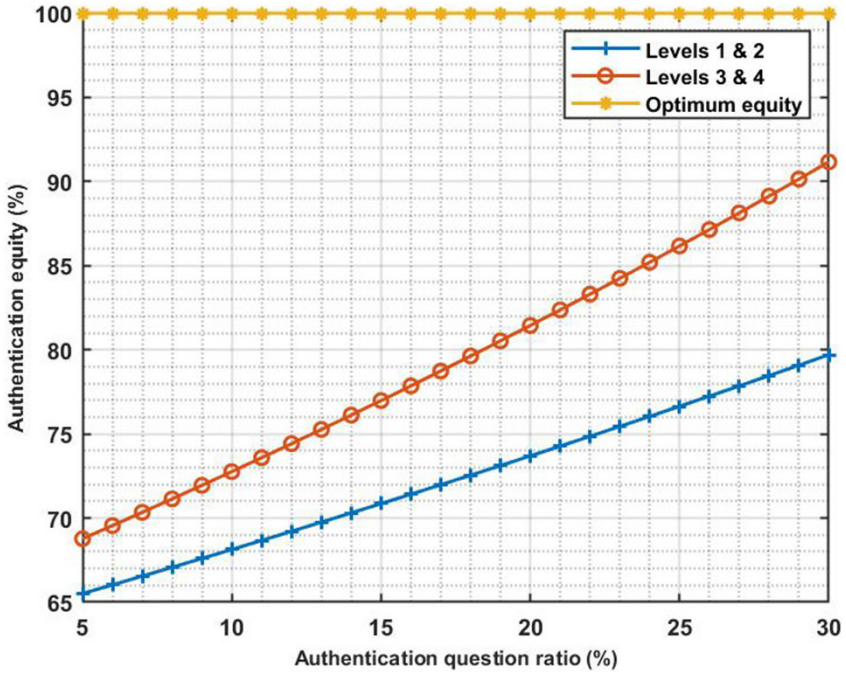

Fig. 5. Authentication equity versus authentication question ratio number

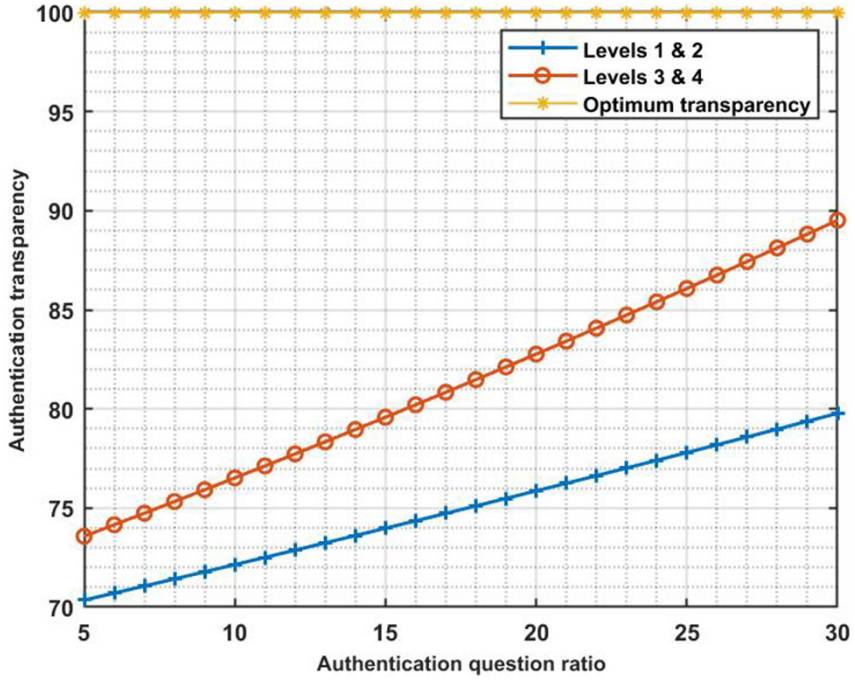

Fig. 6. Authentication transparency versus authentication ratio number

Figure 6 illustrates the authentication transparency versus the authentication question ratio, where the experimentation begins with an input parameter equal to 5% until 30%. This figure displays that the output parameter decreases with the growth of the mentioned input parameter. Figure 6 provides two curves using similar directions operated with Figure 4 and Figure 5, where the first curve combines the impacts of levels 1 and 2, and the second includes the results of classes 3 and 4. The authentication transparency for levels 3 and 4 is optimum than that completed by levels 1 and 2. But, the output parameter relating to classes 1 and 2 becomes equivalent to 80%, representing acceptable transparency. Using the curves in the mentioned figure, the students in classes 3 and 4 provide collaborative feedback used by academic staff and e-learning administrators to enhance e-evaluation content and authentication procedure. In addition, the students of classes 3 and 4 control their behaviors appropriately during the enhanced courses and teachers' methods. However, the students of levels 1 and 2 give limited feedback for solving the current issues over e-learning platforms. In conclusion, the actions of these students, specifically class 1 and 2, decrease their transparency during the different e-evaluation strategy and diminish the authentication validation.

5 Conclusion and future work

COVID-19 caused a rapid migration of academic institutions to e-learning platforms to overcome new education issues and guarantee teaching and evaluation continuities. This orientation creates a set of concerns, mainly evaluation security regarding

authenticating takers, transparency, and equity of e-evaluation. This paper introduces a hybrid authentication scheme to solve security challenges utilizing jointly static and dynamic approaches to handle suitably e-evaluation. This scheme manages an active profile built using student and behavior information collected during the courses' activities to supervise unethical conduct during e-evaluation. The proposed scheme guarantees continued authentication employing dynamic questions created depending on e-evaluation advancement and time-out without additional material and extra cost. The introduced approach assures real-time student authentication and guarantees student e-evaluation transparency and equity. Advanced mathematic models and algorithm are designed to handle information related to students, courses, and staff data and activities. Experimental work is developed where the achieved outcomes indicate that authentication level and e-evaluation transparency and equity are guaranteed continuously at a lower cost.

6 Acknowledgements

The author would like to thank the Deanship of Scientific Research at Umm Al-Qura University for its continuous support. This work was supported financially by the Deanship of Scientific Research at Umm Al-Qura University (Grant code: 22UQU4340518DSR03).

7 References

[1] G. Jagadamba, R. Sheeba, K. N. Brinda, K. C. Rohini and S. K. Pratik, "Adaptive e-learning authentication and monitoring," 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 277–283, 2020, https://doi.org/10.1109/ICIMIA48430.2020.9074955

[2] F. D. Salimovna, Y. N. Salimovna and I. S. Z. ugli, "Security issues in e-learning system," International Conference on Information Science and Communications Technologies (ICISCT), pp. 1–4, 2019, https://doi.org/10.1109/ICISCT47635.2019.9011971

[3] M. Ghizlane, B. Hicham and F. H. Reda, "A new model of automatic and continuous online exam monitoring," International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS), pp. 1–5, 2019, https://doi.org/10.1109/SysCoBIoTS48768.2019.9028027

[4] A. Ben Amor, M. Abid and A. Meddeb, "Secure fog-based e-learning scheme," in IEEE Access, vol. 8, pp. 31920–31933, 2020, https://doi.org/10.1109/ACCESS.2020.2973325

[5] M. Kaiiali, A. Ozkaya, H. Altun, H. Haddad and M. Alier, "Designing a secure exam management system (SEMS) for m-learning environments," in IEEE Transactions on Learning Technologies, vol. 9, no. 3, pp. 258–271, 1 July–Sept, 2016, https://doi.org/10.1109/TLT.2016.2524570

[6] Y. Khlifi and H. 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, pp. 62–89, April, 2017, https://doi.org/10.3991/ijet.v12i04.6478

[7] Y. Khlifi "An advanced authentication scheme for e-evaluation using students behaviors over e-learning platform" International Journal of Emerging Technologies in Learning, vol. 15, no. 4, pp. 90–111, Feb, 2020, https://doi.org/10.3991/ijet.v15i04.11571

[8] F. Khan and S. R. Alotaibi "Design and implementation of a computerized user authentication system for e-learning" International Journal of Emerging Technologies in Learning, vol. 15, no. 09, pp. 4–18, May, 2020, https://doi.org/10.3991/ijet.v15i09.12387

[9] A. A. Alghamdi, M. A. Alanezi and F. Khan "Design and implementation of a computer aided intelligent examination system" International Journal of Emerging Technologies in Learning, vol. 15, no. 01, pp. 30–44, Jan, 2020, https://doi.org/10.3991/ijet.v15i01.11102

[10] Y. Rosmansyah, M. H. Ritonga and A. B. Hardi, "An attack-defense tree on e-exam system" International Journal of Emerging Technologies in Learning, vol. 14, no. 23, pp. 251–260, Dec, 2020, https://doi.org/10.3991/ijet.v14i23.11088

[11] G. T. LaFlair, T. Langenfeld, B. Baig, A. K. Horie, Y. Attali and A. A. von Davier, "Digital-first assessments: A security framework" Journal of Computer Assisted Leaning, pp. 1–10, Mar, 2022. https://doi.org/10.1111/jcal.12665

[12] A. Salem and M. S. Obaidat, "A novel security scheme for behavioral authentication systems based on keystroke dynamics" Journal of Security and Privacy, vol. 2, no. 2, April, 2019, https://doi.org/10.1002/spy2.64

[13] A. Farooq, F. Ahmad, N. Khadam, B. Lorenz and J. Isoaho, "The impact of perceived security on intention to use e-learning among students," IEEE 20th International Conference on Advanced Learning Technologies (ICALT), pp. 360–364, 2020, https://doi.org/10.1109/ICALT49669.2020.00115

[14] A. Leea and J. Han, "Effective user authentication system in an e-learning platform" International Journal of Innovation, Creativity and Change, vol. 13, no. 3, May, 2020, https://doi.org/10.1049/gtd2.12181

[15] A. Tick, "Evaluating e-learning acceptance and usage motivation including IT security awareness amid Z establishment hungarian students with xTAM" IEEE 23rd International Conference on Intelligent Engineering Systems (INES), pp. 000137–000142, 2019, https://doi.org/10.1109/INES46365.2019.9109506

[16] A. W. Muzaffar, M. Tahir, M. W. Anwar, Q. Chaudry, S. R. Mir and Y. Rasheed, "A systematic review of online exams solutions in e-learning: Techniques, tools, and global adoption," in IEEE Access, vol. 9, pp. 32689–32712, 2021, https://doi.org/10.1109/ACCESS.2021.3060192

[17] V. V. Timchenko, S. Y. Trapitsin, K. V. Kaisheva and M. V. Zharova, "Optimization of the student assessment algorithm based on classification methods," International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), pp. 864–868, 2021, https://doi.org/10.1109/ITQMIS53292.2021.9642801

[18] H. Ibrahim, S. Karabatak and A. A. Abdullahi, "A study on cybersecurity challenges in e-learning and database management system," 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–5, 2020, https://doi.org/10.1109/ISDFS49300.2020.9116415

[19] L. Zhao et al., "Academic performance prediction based on multisource, multifeature behavioral data," in IEEE Access, vol. 9, pp. 5453–5465, 2021, https://doi.org/10.1109/ACCESS.2020.3002791

[20] K. Wei et al., "Federated learning with differential privacy: Algorithms and performance analysis," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3454–3469, 2020, https://doi.org/10.1109/TIFS.2020.2988575

[21] S. H. Song et al., "Developing and assessing MATLAB exercises for active concept learning," in IEEE Transactions on Education, vol. 62, no. 1, pp. 2–10, Feb, 2019, https://doi.org/10.1109/TE.2018.2811406

8 Author

Yassine Khlifi has received M.Sc. and Ph.D. in information and communications technologies from the higher school of communication (SUP'Com), Carthage University, Tunisia. He is a researcher in the Digital Security (SecNum) Laboratory at Carthage University. He is an associate professor and development consultant of vice president of postgraduate studies and scientific research at Umm Al-Qura University, KSA. His research works focus on optical and all-optical network architectures, protocols, QoS provision, dimensioning and optimization as well as network and e-learning platform security. E-mail: khlifi.yassine@gmail.com

Article submitted 2022-06-23. Resubmitted 2022-08-10. Final acceptance 2022-08-11. Final version published as submitted by the authors.