An Adaptive Framework for Designing Secure e-Exam Systems

Mohammad T. Alshammari
md.alshammari@uoh.edu.sa
College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia

Summary
Traditional learning approaches through classrooms can be rigid, tedious and may not be suitable for all types of learners. Learning organizations usually offer e-learning systems to address the issue of traditional learning. These systems can provide an interactive learning experience with different types of learning material which can be offered anytime and anywhere and enable communication services to support learner-instructor interaction. However, a secure online examination represents a challenging issue in comparison with traditional examination procedures. In exam traditional settings, professional proctors are involved, and exams are conducted in a specified place within a timeframe. This paper aims to address this issue by proposing an adaptive framework for designing and developing secure e-exam systems. An evaluation of the framework is also offered based on a hybrid methodology involving interviews and surveys. Also, some instructional and technical recommendations are presented to supplement the proposed framework. The results of this study confirm the applicability of the framework in designing secure e-exam systems. Future directions of research are also offered.

Key words:
E-Learning; E-Exam; Security; Learner Model; Education

1. Introduction

Learning technologies are advancing and becoming more smarter to meet the requirements of learners, instructors and learning organizations [1]. By using advanced learning technologies, it is possible to deliver and create dynamic and interactive learning material which can be accessed by learners anytime and anywhere in contrast to classroom-based learning [2]. Learners may find traditional learning approaches through classrooms rigid, repetitive and unappealing which can affect learning motivation and learning outcomes [3]. The new generations of learners usually use e-learning systems in order to gain some knowledge. These e-learning systems can be used in combination with traditional classrooms or alone.

Most universities worldwide offer e-learning systems to facilitate the learning process and support their learners [4]. Some universities open their online courses to external learners to universally spread knowledge such as Harvard University and Massachusetts Institute of Technology (MIT). Since different types of e-learning systems are mainly used by learning organizations, the main challenge is to establish a secure online examination approaches to ensure that learners are assessed reliably and effectively [5]. In traditional examination approaches, exams are conducted in specific places and times; they are also professionally proctored and organized so that the process of examination is effectively managed to reduce the chances of misconduct or misbehaviors that may occur [6]. Cheating can directly be observed by exam proctors, and they can take immediate actions against any suspicion following the exam regulation of the learning organization.

However, it is still challenging to deal with online exams securely in comparison to traditional examination settings such as proctored paper-based exams [7]. These challenges involve, for example, privacy, acceptability, availability, authentication and authorization [8]. This paper aims at providing an adaptive framework for designing secure e-exam systems to address the issue of offering secure online examinations. The adaptive framework contains different components such as the interaction interface, domain model, learner model and the adaptive exam generation. Each component has a specific objective to accomplish to provide a secure online exam experience. For example, the component of the interaction interface can be designed in a way that not to permit or deactivate interface re-locating, copy-paste, minimize-maximize or taking screenshots services. Another example relates to the domain model; its main aim is to represent, store and manage questions banks. The paper also gives an evaluation of the framework's applicability to design secure e-exam systems. A hybrid evaluation methodology was conducted. The methodology consisted of expert interviews and surveys. The experts who were involved in the interviews represent the fields of education, learning technology and computer science to cover both instructional and technical challenges and to obtain deeper insights into different aspects of designing such secure e-exam systems. The survey was completed by undergraduate learners who have some experience in an online examination or at least attempted an online exam. The main aim of the survey is to understand how learners perceive online examination. The data obtained from both the interviews and surveys generated a clear picture of issues, challenges and perceptions of online examinations. Therefore, a possible solution can be offered.

The key research question of this paper is How can we design a secure e-exam system? The main approach taken in this paper to answer the research question was to explore related work and how they perform such online exams and evaluate them. Then, an adaptive framework was initially generated in view of published research, followed by a preliminary evaluation of its applicability. Based on the

Manuscript received May 5, 2020
Manuscript revised May 20, 2020

findings, further refinements were applied to the proposed framework and presented in its final form.

The rest of the paper is structured as follows. Section 2 provides related work. Section 3 offers the proposed adaptive framework for designing secure e-exam systems detailing its core components. Section 4 presents the evaluation methodology followed in this paper. Section 5 delivers the results and discuss them. Section 6 provides some instructional and technical recommendations. Section 7 concludes the paper besides future research directions.

2. Related Work

Many attempts to develop e-exam systems have been found in published research [9]. The work presented by [10] focused on building an e-exam system using video cameras enabled on the client-side so that the learner's face can be captured in different intervals and stored on the server-side. They evaluated their system successfully with 450 learners studying a course on digital signals. However, the manual work of checking the stored images of each learner after the exam represents a limitation of their system. Additionally, other aspects were not covered in the system such as how the exam content are provided and how information about learners is represented.

A similar attempt is also provided by [7]; they designed and deployed a secure e-exam management system. However, the system is limited since it enables one type of question only (i.e., multiple-choice questions). Other assessment types are essential to increase the reliability of the online exam. Another approach to enhance the security of e-exam systems based on group cryptography was proposed by [5], focusing on real-time monitoring of the online exam session. Still, the approach offers the same sets of questions to all remote examinees without randomization features. Learners in this approach can easily cheat using their mobile devices via communication applications during the exam session, where they can share the answer for each question affecting the integrity of the whole exam.

A more adaptive online examination process was provided by [11], where the e-exam system automatically generates exam questions randomly from a question pool. However, an evaluation of the system was not provided in a real context. A study that focuses on supporting secure online exams through mobile devices was offered by [12]. They evaluated their mobile exam system concentrating on usefulness surveys with learners and instructors generating positive findings.

According to the published research and a recent review of the field of secure e-exam technologies [8], [9], there are some research gaps that need to be addressed. First, most e-exam systems were developed focusing on specific issues of security such as authentication or online exam generation, limiting their completeness when deployed in a real examination context. Second, the developed e-exam systems lack empirical development based on earlier attempts proposing a wide variety of different architectures of e-exam systems. Third, the e-exam systems usually focused on the technical aspects neglecting the instructional aspects and the learning and assessment theories. Hence, based on the pre-mentioned issues, the study in this paper proposes a generic adaptive framework for designing different instances of secure e-exam systems. Moreover, technical and instructional recommendations are included to supplement the proposed framework.

3. The Adaptive Framework

The proposed adaptive framework consists of different components to deliver a secure online examination via e-exam systems, as presented in Fig. 1. There are six core components, where each component has a specific job. The components of the framework consist of the interaction interfaces (learner interface and instructor interface), learner model, authentication engine, domain model, adaptive engine and exam generator.

The components of the framework are also common to the components of adaptive e-learning systems [13]. However, the proposed framework is original as it focuses on designing e-exam systems rather than delivering learning material. An integration of the framework into enhancing current systems is possible since it is flexible and adaptable.

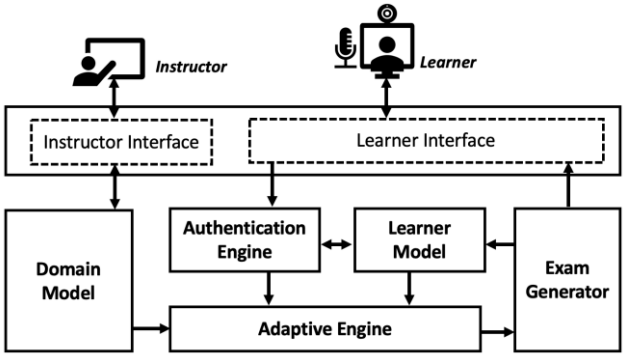

Fig. 1 The proposed adaptive framework.

The learner interface and instructor interface are simply the graphical user interfaces. Learners can interact with the learner interface in order to complete the online exam, whereas instructors can interact with the instructor interface to manage question banks. The learner model contains information related to each learner, including, for example, personal identifier, name, personal image and information related to the exams completed and their assessments.

The authentication engine is reasonable for detecting the learner's personal face during the examination by capturing their face images via the video camera and compare it with the existing image stored in the learner model for

authentication. The authentication engine also handles voices when a microphone is enabled.
The domain model involves a specific structure that enables the creation of question banks related to a specific learning domain. The adaptive engine takes into account data obtained from the other components ensuring that the learner is authenticated to complete the exam based on the learner model, to select specific questions adaptively to be offered and to monitor the examination progress continually. The adaptive engine data then feeds into the exam generator component and then the exam is delivered to the learner.
The components of the framework are detailed in the following sub-sections.

3.1 Interfaces

The interaction interface is simply the gate to interact with and manage the e-exam system. There are two interaction interfaces: the learner interface and the instructor interface. Each learner can complete the exam by interacting with the learner interface. The interface is designed to, for example, display the learner profile including his/her information, the exam that needs to be completed and present their grades. Some security features need to be considered when offering an exam. These features involve, for example, starting an exam in a fresh encrypted interface, preventing screenshots, disabling copy-paste text and maximizing-minimizing the interface.
About the instructor interface, it enables each instructor to manage their questions' banks related to their courses. It should be noted that the interfaces should usable and follow standard human-computer interaction in interface design [14].

3.2 Learner Model

The learner model cares about each learner by representing and managing their data including personal information, exams that have been offered and taken, and their assessments [15]. The information stored in the learner model is continually updated based on the learner-system interaction. The model is initiated through the registration with the system by each learner. An exam can be offered to each learner based on his/her profile. For example, different types of questions are offered, and once a learner answers each question a specific grade is assigned until the completion of the whole exam. The grades are then stored in the learner model. A set of exams can also be delivered according to the courses that the learner is enrolled in.

3.3 Authentication Engine

The authentication engine aims at ensuring that the expected learner is logged in the e-exam system via two methods. The first method uses video cameras, whereas the second method uses microphones. In the first method, the engine implicitly captures multiple images of the learner with different intervals during the exam session through the video camera. The engine can then apply some sophisticated algorithms that compare the set of captured images with the stored personal image in the learner model. The output of the engine can be classified into three cases: authenticated, holding or unauthenticated. The authenticated case means that the learner is the actual person who is taken the exam by comparing the elicited personal images from the video camera with the stored image in the learner profile. The holding case is initiated once the engine detects that the video camera is switched off or a non-human face image is found. The unauthenticated case involves the detection of a personal face image that is not related to the actual learner who is taking the exam. In the second method, the engine also records any speeches by the learner who is taking the exam and any sounds related to the learner's surrounding context. The recordings are reordered assigning the current question where the learner is trying to answer. These recordings can then be investigated.

3.4 Domain Model

The domain model can be represented to contain information related to some courses where each course has multiple objectives so that learning material and assessment content can be retrieved [16]. Each learning objective can also be augmented with different types of questions such as multiple-choice questions, true/false, short answers and fill in the blank. These types of questions can automatically be assigned a completion time and a possible point by the instructor in the creation phase so that the point is successfully achieved when correctly answered by the learner. Also, the instructor can interact directly with the model to add some features such as displaying exam description, one question at a time, randomizing the answers and force completion of the exam when the Internet connection is lost.

3.5 Adaptive Engine

The adaptive engine takes into account data stored in the learner model, the domain model and the authentication engine. The adaptive engine ensures that the output of the authentication engine in order to proceed in matching the learner profile with the domain model to select relevant questions related to a specific course or a set of learning objectives. These data can then adaptively and automatically be passed to the exam generator component. This component continually receives data from the authentication engine until the learner completes the whole exam.

3.6 Exam Generator

This component generates an exam that is offered to each learner after ensuring that the learner is authenticated and authorized to take the exam. The questions and their options can be randomized to prevent exam cheating or misuse of the exam. According to the domain model, the completion time of the whole exam is determined based on the required time to answer each question. This model can easily be modified and updated by the instructor. The exam is then passed to the interaction interfaces to display the exam to the learner.

4. Evaluation Methodology

A hybrid evaluation methodology is employed in this research in order to refine and validate the applicability of the proposed framework in designing secure e-exam systems. The main aim of this evaluation is to build up a robust foundational approach before deploying such e-exam systems. This evaluation involved interviews and survey methods. The interviews were conducted with experts in the fields of education, learning technology and computer science. Experts from these three fields can contribute to the evaluation of the framework because of their relevance to this research project and to their technical and instructional experiences. The interviews were conducted with twelve experts in the pre-mentioned fields. Each field is represented by four experts. All the experts agreed to participate in this research voluntarily. Four group interviews were conducted, where each group consisted of three experts (i.e., one expert form each field). The four groups were not familiar with each other. This is to avoid any knowledge or views sharing and to gather independent opinions and responses from each group. The main procedure was to ask pre-defined questions to each group before presenting the framework. Then, the framework was shared and explained to them followed by other questions. Each group interview lasted for about 90 minutes with seven main questions. The interview questions are presented in Table 1.

Table 1: Interview questions.

No.	Interview question
Before presenting the framework	
1	Is it possible to conduct a secure online examination?
2	What are the educational challenges to conducting a secure online examination?
3	What are the technical challenges to conducting a secure online examination?
4	Do we need some pre-defined guidelines to conduct online examinations?
After presenting the framework	
5	Do you think the framework is comprehensive in addressing all instructional and security challenges?
6	If an e-exam system is built based on the framework, would you use it for your course exams?
7	How would you improve the framework?

After accomplishing the group interviews and recording the responses, a survey was then administered with 120 undergraduate learners who had some experience in online examinations to evaluate how they perceive online examinations. All the learners completed the survey and responded to all the survey items. The survey consists of 17 items, as presented in Table 2, with a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

Table 2: Survey items.

No.	Survey item
1	I am more comfortable when doing an online exam than paper-based exams
2	I can comfortably concentrate on the questions when doing an online exam
3	I would select the option of doing an online exam rather than paper-based exams
4	Online exams are appropriate for my subject area
5	Online exams can help in assessing my recall, understanding and application skills
6	Online exams can be more accessible than paper-based exams
7	Technical problems can make online exams impractical
8	It is okay for me If I am monitored during formal online exams via webcams or microphones
9	I am more confident with computer (automatic) marking than instructor marking
10	Based on my experience, the current technology in the online examination is reliable
11	Online exams can be more secured in comparison to paper-based exams
12	My grades when completing online exams are secure
13	Cheating can be easier on online exams off-campus than with paper-based exams
14	Using login information (username & password) can offer acceptable security to online exams
15	Online exams can do things paper-based exams cannot
16	Online exams can contribute to my learning
17	Current e-learning systems support secure online exams

5. Results and Discussion

The results are organized, discussed and provided into two sub-sections. The first part is related to the findings of the interviews. The second part reports on the survey results.

5.1 Interviews

There were four group interviews where each group involved three experts representing the fields of education, learning technology and computer science. The findings are organized based on each interview question.

The first phase of the interview involved four questions and was asked before presenting the proposed framework to the interviewees. This is to ensure that the group members are not affected by the framework and the main idea was to have their answers in the first phase primarily based on their

experience. The first interview question in this phase was, *Is it possible to conduct a secure online examination?* All four independent groups agreed to suggest that conducting a secure online examination is possible. Nevertheless, it is challenging to build such systems, and the current systems need significant improvements.

The second question was *What are the educational challenges to conduct a secure online examination?* The groups mentioned some critical educational challenges questioning the ability of online exams to examine different types of knowledge, skills and abilities of learners. Also, cheating is raised as a notable concern to instructors so that the fairness of the grading process may not be guaranteed.

The third question was *What are the technical challenges to conduct a secure online examination?* The groups revealed some significant technical challenges including security, exam monitoring, scalability to handle a large number of learners, reliable network connectivity, availability when needed and accessibility. Security represents a vital issue of online exams and involved many security aspects: learner authentications, authorization to take a specific exam, privacy of learners and cyber-attacks.

The fourth question was *Do we need some pre-defined guidelines to conduct online examinations?* The groups confirmed the need to have such guidelines and precise requirements that need to be carefully fulfilled when deploying e-exam systems. These should include both instructional guidelines and technical guidelines. When designing such systems, they need to follow the guidelines to ensure the reliability and effectiveness of e-exam systems.

The second phase of the interviews involved presenting and explaining the proposed framework to the interviewees. The main aim was to share the views of the researcher based on the framework and to map their views from the first phase to the second phase of the interview. The interviewees were then asked to answer the other interview questions. In response to the fifth question (*Do you think the framework is comprehensive to address all instructional and security challenges?*), all groups confirmed the framework's comprehension since it covers their key instructional and technical concerns which can be handled in e-exam systems when deployed according to the framework.

The sixth question was *If an e-exam system is built based on the framework, would you use it for your course exams*? Three groups out of four groups agreed to use the system assuming that it is completely secure and reliable based on the proposed framework. One group had the view that final exams must be conducted via paper-based examination. They would, however, use the e-exam system off-campus based on the framework for some quizzes and short-tests. They believe that some people may suffer from technology anxiety and illiteracy. However, the three groups who would use the e-exam system argued that technology nowadays is seen as an essential skill to have so some learning would contribute to bridging the knowledge gap.

The seventh question was *How would you improve the framework?* All groups had some ideas to improve the framework. First, they suggested to enable the instructors to authenticate and manually authorize learners to take an online exam if learners do not have video cameras or for any reason during the online examination. They claimed that instructors might need some control over the e-exam system. It is believed that since instructors will eventually have the final data about the performance of each learner, they can then evaluate the situation and decide upon accepting, modifying or rejecting the data. Second, the groups recommended using voice detection mechanisms besides enabling video cameras in order to analyze any verbal cheating that the camera cannot detect. This was a reasonable suggestion, and the framework was enhanced to cater for this suggested feature. Third, the feature of allowing the instructors to be available as proctors would be an advantage to observe the online examination.

5.2 Survey

The survey was completed by 120 undergraduate learners majoring in computer science and engineering. The sample involved 72 male learners (60%) and 48 female learners (40%). The age of the participants was between 20 and 23 years old.

About the overall survey results, the majority of learners are *neutral* in their responses (39.60%) about having online examinations followed by learners who would *agree* on online examination (21.96%), and then learners who *strongly agree* (17.05%). The percentages of learners who *disagree* or *strongly disagree* with having online examinations are 14.75% and 6.61%, respectively. Fig. 2. presents a chart plotting the frequency of each option from *strongly agree* to *strongly disagree* summarizing the overall survey findings.

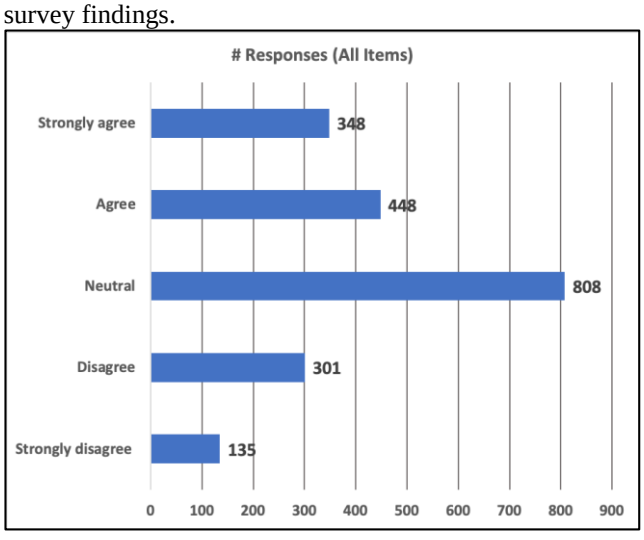

Fig. 2. The overall survey results.

It can be observed that the majority of learners would have online examinations rather than paper-based examinations. According to these findings, the positive perception of learners toward online examination emphasizes the need for such frameworks and guidelines to design secure e-exam systems. However, there is a need to investigate each item of the survey to obtain deeper insights into online examinations. Fig. 3. summarizes the results for each item of the survey. According to these results, most learners would be comfortable doing online exams and they have no issues of concentration on questions during online exams. They also believe that online exams are appropriate to their subject area (i.e., computer science and engineering). Learners also favor automatic marking rather than manual marking by instructors, and somewhat agree on the accessibility of online exams.

However, learners were not sure about the ability of online exams to assess their different skills and abilities of their knowledge, understanding and applications. This can be justified since those learners may have some experience with a specific e-exam system, and that they did not investigate the system themselves or feel that the system was not usable. Also, the learners were cautious when it comes to technical problems during online examinations. They might believe that these technical problems may affect their performance or attending to the online exam so their trust can be decreased. Some learners may think deeply about solving the technical problems rather than focusing on their exams which may increase exam anxiety.

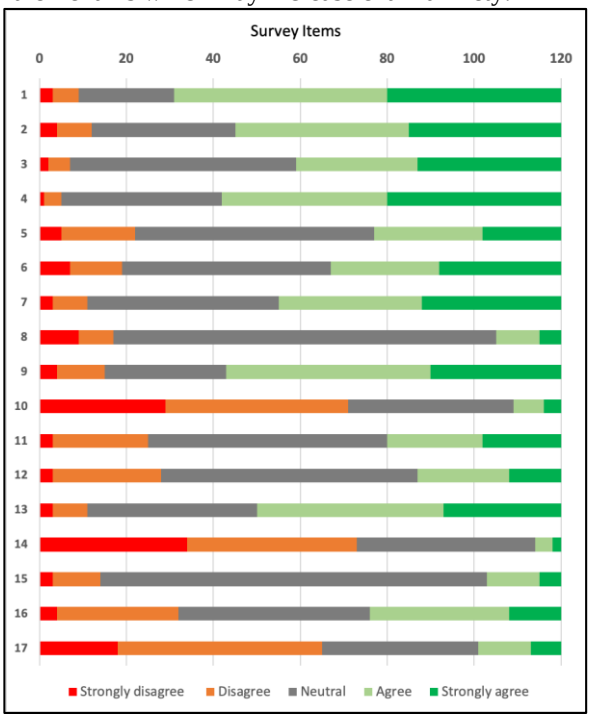

Fig. 3. The results of the survey items.

Regarding the learners' perception towards the security of online exams in comparison to paper-based exams, learners might think that e-exam systems can be exposed to cyber-attacks resulting in system failure. However, most responses about security on online exams have a neutral tendency. That means the learners may consider that even physical storage of exam papers can be threatened the same as online exams. This issue is also applied when learners are thinking about the security of their stored grades. These issues justified their responses to be on the neutral side about security. That does not mean the current e-exam systems should not be improved. Instead, developers of such systems need to be very careful and take every small details and security aspects into account.

Regarding the acceptance of learners in being monitored via video cameras or microphones during online exams, they were mostly neutral in their responses. This seems acceptable to them since they might have some experience in online learning and regularly use different social media platforms such as Facebook and Twitter. Therefore, exposing their virtual identities through formal and trustable policies from their universities seem reasonable.

Most learners strongly believe cheating in online exams off-campus is much easier than when having traditional paper-based exams. They may suppose that they could search the Internet to find the proper answers, read some books or learning resources during the online exam, have some group communication or asking someone else to complete their exams. These obstacles are challenging in paper-based exams. Learners also disagreed with having login information such as username and password only to have full security on e-exam systems. They would expect more sophisticated features of security. Also, they emphasized that the current e-learning systems they have experience with do not support secure online exams. Therefore, significant improvements are needed.

6. Recommendations

The paper presented an adaptive framework that can be used to design different instances of e-exam systems. Also, an evaluation of its applicability through reviews with experts in the domain of education, learning technology and computer science was provided. That was also supported by a survey with actual learners to investigate learners' perceptions of online examinations. According to the findings of this study and as elicited from published research, there are several recommendations for providing secure online examinations when the proposed framework is considered. These recommendations are classified into two classes: instructional recommendations and technical recommendations.

About the instructional recommendations, it is essential to integrate learning theories and models when generating

exam questions linked with learning objectives. One of the most popular models is the Bloom's Taxonomy [17]. This model can be applicable to K-12 instructors, college and university professors to support their teaching, learning and assessment. Bloom's Taxonomy consists of six key levels: remember, understand, apply, analyze, evaluate and create. Developers of e-exam systems based on the framework should take these levels into account when designing the domain model (i.e., a component of the framework which represents questions banks). For example, for each learning objective, different assessment levels can be associated with that objective delivered as online questions.

By using such learning models, the learners can meet the learning requirements and improve their knowledge, skills and abilities. Moreover, each question's difficulty level should be determined to generate reliable sets of questions according to each learner's level. Instructors should use the e-exam system for quizzes and short tests during the semester to familiarize their learners with the system before attempting to any final examination.

About the technical recommendations, it is critical to achieving high levels of security, reliability and effectiveness of online exams through e-exam systems. There are several vital points to take into account when designing such systems [18]. These points include, but not limited to, authentication, authorization, accessibility, usability, availability, controllability, privacy and monitoring. These concepts or points are described and presented in Table 3 as technical recommendations for designing reliable and secure online exams. In addition, other technical aspects should be taken into accounts such as randomizations of questions in online exams, force completion and submission of exams when an Internet connection is lost, providing a proper description of each exam, specifying the start and time of the exam, presenting a question at a time, disabling back-to-question feature, beginning an online exam in a new encrypted browser window, disabling copy-paste, minimize-maximize and screenshot features. Learners should also be encouraged to use reliable and unshared Internet connection during online examinations.

Table 3: Technical recommendation for secure and reliable online exams.

Concept	Explanation
Authentication	The e-exam system must ensure that the permitted learner is taking the exam through image detections and voice recognition methods.
Authorization	The e-exam system must provide secure login methods through an encrypted Internet connection, username and password to authorize the learner to access the online exam.
Accessibility	The e-exam system must be accessible in different operating systems, Internet browsers and devices.
Usability	The e-exam system must be easy to use and follow human-computer interaction standards for both instructors and learners to provide a better assessment experience.
Availability	The e-exam system must be available for instructors and learners when needed through careful considerations of server hardware & software and active support.
Controllability	The e-exam system must provide management tools to instructors and admin teams to control the system's components when an issue occurs. Flexible logged amendments can be offered via the system as an important tool.
Privacy	The e-exam system must enable events logging mechanisms so that any misuse, manipulation or viewing of data related to the grades of learners and online exams other than the authorized people can be tracked.
Monitoring	The e-exam system must provide proctoring features in online exam sessions for instructors or authorized people.

7. Summary

This paper contributes to the current body of knowledge by providing an adaptive framework for designing e-exam systems and a hybrid evaluation (interviews and surveys) that involved experts and actual university learners. The interviews were conducted with experts to evaluate the applicability of the proposed framework. The surveys were taken by university learners to explore how they perceive online examinations. The results of the findings given published research allowed us to generate the adaptive framework and offer some relevant recommendations when designing e-exam systems based on that framework. The recommendations were classified into two classes: instructional and technical and presented in this paper.

Each work must have some limitations. Since the survey sample was conducted mainly with university learners majoring in computer science and engineering, the generalizations of the survey findings cannot be generalized confidently to other learners with different subjects. However, the results of the survey offered an initial insight into how the big picture will be. Besides, it is planned to conduct more studies focusing on a larger sample, different subjects and cultures.

It is necessary to highlight that the framework does not only help in designing e-exam systems but can also allow other researchers to focus on its different components including the learner model, the domain model and the adaptive model. The framework can open different directions of

research. For example, a researcher may focus on the representation of domain models while another may explore the development of learner models.

About future research, an e-exam system will be built according to the proposed framework taking into account the instructional and technical recommendations presented in this paper. The system will then be evaluated in terms of its usability, security and reliability. Another direction could be to enhance current learning management systems such as Blackboard, Moodle and Canvas with some aspects of the framework to provide better security.

References

[1] M. Ally, "Foundations of educational theory for online learning," *Theory and practice of online learning*, vol. 2, pp. 15–44, 2004.

[2] H. Xie, H.-C. Chu, G.-J. Hwang, and C.-C. Wang, "Trends and development in technology-enhanced adaptive/personalized learning: A systematic review of journal publications from 2007 to 2017," *Computers & Education*, vol. 140, p. 103599, 2019.

[3] N. B. A. Normadhi, L. Shuib, H. N. M. Nasir, A. Bimba, N. Idris, and V. Balakrishnan, "Identification of personal traits in adaptive learning environment: Systematic literature review," *Computers & Education*, vol. 130, pp. 168–190, 2019.

[4] J. Hammad, M. Hariadi, M. H. Purnomo, N. Jabari, and F. Kurniawan, "E-learning and Adaptive E-learning Review," *International Journal of Computer Science and Network Security*, vol. 18, no. 2, pp. 48–55, 2018.

[5] I. Y. Jung and H. Y. Yeom, "Enhanced security for online exams using group cryptography," *IEEE transactions on Education*, vol. 52, no. 3, pp. 340–349, 2009.

[6] J. W. Gikandi, D. Morrow, and N. E. Davis, "Online formative assessment in higher education: A review of the literature," *Computers & Education*, vol. 57, no. 4, pp. 2333–2351, 2011.

[7] F. Al-Hawari, M. Alshawabkeh, H. Althawbih, and O. Abu Nawas, "Integrated and secure web-based examination management system," *Computer Applications in Engineering Education*, vol. 27, no. 4, pp. 994–1014, 2019.

[8] M. Kuikka, M. Kitola, and M.-J. Laakso, "Challenges when introducing electronic exam," *Research in Learning Technology*, vol. 22, 2014.

[9] A. E. Fluck, "An international review of eExam technologies and impact," *Computers & Education*, vol. 132, pp. 1–15, 2019.

[10] K. C.C. and C. C.D., "Secure Internet examination system based on video monitoring," *Internet Research*, vol. 14, no. 1, pp. 48–61, Jan. 2004.

[11] M. Ya\ugci and M. Ünal, "Designing and implementing an adaptive online examination system," *Procedia-Social and Behavioral Sciences*, vol. 116, pp. 3079–3083, 2014.

[12] M. Kaiiali, A. Ozkaya, H. Altun, H. Haddad, and M. Alier, "Designing a secure exam management system (SEMS) for M-learning environments," *IEEE Transactions on Learning Technologies*, vol. 9, no. 3, pp. 258–271, 2016.

[13] M. T. Alshammari, "Design and evaluation of an adaptive framework for virtual learning environments," *International Journal of Advanced and Applied Sciences*, vol. 7, no. 5, pp. 39–51, 2020.

[14] K. Orfanou, N. Tselios, and C. Katsanos, "Perceived usability evaluation of learning management systems: Empirical evaluation of the System Usability Scale," *The International Review of Research in Open and Distributed Learning*, vol. 16, no. 2, 2015.

[15] K. Chrysafiadi and M. Virvou, "Student modeling approaches: A literature review for the last decade," *Expert Systems with Applications*, vol. 40, no. 11, pp. 4715–4729, Sep. 2013.

[16] M. Simko and M. Bielikova, "Lightweight domain modeling for adaptive web-based educational system," *Journal of Intelligent Information Systems*, vol. 52, no. 1, pp. 165–190, Feb. 2019.

[17] T. Scott, "Bloom's taxonomy applied to testing in computer science classes," *Journal of Computing Sciences in Colleges*, vol. 19, no. 1, pp. 267–274, 2003.

[18] A. M. Gabor, M. C. Popescu, and A. Naaji, "Security Issues Related To E-Learning Education," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 17, no. 1, p. 60, 2017.

Mohammad T. Alshammari received his B.S. degree in Computer Science Education from the University of Ha'il, Saudi Arabia, in 2007, and the M.S. and Ph.D. degrees in Computer Science from the University of Birmingham, UK, in 2011 and 2016, respectively. From 2008 to 2016, he was a Teaching Assistant with the College of Computer Science and Engineering (CCSE), University of Ha'il, Saudi Arabia. Since 2016, he has been an Assistant Professor with CCSE. His research interests include human-computer interaction, user modeling, adaptive & intelligent systems and educational technology.