Evaluation of E-exam during Covid-19

Mooad Imad Al-Shalout
Zarqa university ,Jordan – Amman – Zarqa ,mooad_sh@yahoo.com
Mohammed Rasmi
Departmint of Internet Technology ,Zarqa university ,Jordan – 13132 – Zarqa ,mmousa@zu.edu.jo
Mohammad A.Hassan
Computer Scince Departmint ,Zarqa University ,Zarqa- 13132 – Jordan ,mohdzita@zu.edu.jo

ABSTRACT:
Electronic exam's' non-reliability is one of the most critical gaps in this type of exam, whereas any electronic exam is considered entirely unreliable. In addition to that, it is not protected and free from cheat. The continuous validation that the examinee is the one who solves the questions of the electronic exam permanently and continuously is the most crucial goal of this research. Many methods and procedures will be discussed, which will protect the validity of this type of exam. For example, one of these methods matches the student's fingerprint and takes random snapshots while taking the electronic exam in more than one format. In this research, it's proposed to use student handwriting during the electronic exams to built the value of validity. This way is considered one of the rare methods in the electronic exam. The research also tackles the process of reality for electronic exams through a fingerprint during the examination period. It takes random snapshots for the student without paying attention to him or appearing those pictures to the observer or correcting the exam. The difficulty of offering a safe and high-credibility exam and reducing the phenomenon of cheating requires excellent capabilities in some countries. It also needs prior arrangements and good preparation. It also needs to develop technological capabilities continuously in a high-cost material that may reduce the cheating rates in such a kind of exam.

Keywords:
e-learning, distance education, information security, online privacy, privacy principles, network privacy, policy-based management, trust mechanisms
Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

I.Introduction

Technical development, the explosion of knowledge, and the fantastic acceleration in communication technologies have produced an environment that depends on technology in all fields, including the educational field. So, we have tests that measure the student's learning extent.

Computers designed and build exams, present them to students, administer them, correct them, submit them, and give comprehensive reports for students' educational status and the extent of their academic development.

After preparing these tests, building their equivalent forms, and reviewing them to ensure that they are free of any mistake, the tests are ready for students if the computer requests that. Before giving any of these tests, the computer will collect data for each student who will take the test to identify them and save their performance data in the trial for reference when needed.

With the advent of the technological revolution, the development of information technology, and the development of the Internet in recent years seen E-learning tools in our schools, and recently we have seen the approval of opening e-university. From this point, it was necessary to mention the e-learning tools. The most important of these tools are electronic

excellently and rapidly, the idea of designing tests on the Internet arose.

The test design began on the Internet at the beginning of the emergence of the Internet in the nineties. This matter facilitated communication and helped create tests as an easy way to evaluate the student electronically. In contrast, the teacher could quickly prepare tests to apply to students and correct them electronically and immediately, ensuring credibility and transparency in the correction. In the 1980s, electronic trials began to be used, particularly the CAT test, and Canale presented a research paper about the effectiveness of computer-prepared tests in 1986. The beginning talked about using these tests in teaching languages.[24]

In our research, we will learn about the methods are used and their effectiveness invalidation on the condition that the actual student is the one who answers electronic exams.

And the problems that may face us in the electronic exam.

1- The online exams security :

computer security, according to the NSIST guide, is defined as follows :

Protection generated to the automated information system keeps achieving the applicable goals to maintain the safety of its resources, availability, and confidentiality. Computer and network security is a set of tools that protect data stored or exchanged between computers within the network [3]. Even though significant progress includes the last system security during the past decade, there are many security system flaws and many cyber-attacks victims worldwide. Information security is a serious issue and an essential requirement in the inspection systems. This context is from the latest users' view, such as (authors - teachers - students) and the thought of security functions before content, personal security, access control, authentication, and encryption.[22]

1-1 Concept of online exam security:

This section aims to present the main security concepts for the electronic test. Here we address the security countermeasures and CIA controls against the PIA security objectives and the need for continuous authentication, and the types of identity theft threats (privacy).[1]

1-2 Security measures against E-exam cheat:

The technical standards are against the chest, and precautionary requirements must be applied in the electronic exam to ensure that lectures, students, and data will be protected from potential risks. Therefore, four technical counter-security measures can be used to ensure the security of electronic examination systems or any computer system:

Confidentiality and honesty - availability - reliability. [1-5]

Concerning procedural security measures, below are the four basic requirements that should be fulfil :

1- Security apply.
2- Security policy.
3- Security risk management plan.
4- Monitor security measures.

1-3 Security controls:

The following security controls are necessary to protect E-learning:

1- Access control: whereas only authorized entities can access the system.
2- Encryption: It is a protection to private data from disclosure by using encryption.
3- Firewalls: filtering the exchanged data between internal and external networks.
4- Intrusion detection: Detecting attack attempts and generating an early warning.
5- Protection from viruses and spyware.
6- Digital signature: to ensure that the received content is from a specific user.
7- Digital Certificate: to check if the sent digital content is original.
8-Content filter: Prevent unauthorized parties from posting unwanted content.

1-4 The need for Continuous authentication:

More caution must be taken in the examination via the Internet, that what electronic examination systems do. As a result, it must be verified that the

examinee is the actual student. Therefore, random authentication is required secretly, and from here, the person can be certified in several ways.

-Certified attendance determines the place of the student.

- The identity that distinguishes the student from the other.

- The confirmation that proves the identity of the student.

2 - Identity impersonation threats:

One of the reasons why e-learning is not successful is that there is no completely reliable and secure electronic exam. There is also no protected electronic exam from cheat. [6-9]

A group of studies indicates that cheating in education [10,11] and others reported that about 70% of American high school students cheat on at least one test, where 95% have not been catch.

fig.1 Presence – Identity – Authentication (P-I-A)goals [13]

Twelve studies reported that 75% of university students cheat [12-6-11], and the situation became worse in electronic exams, where 73.6% of the examinees said that {cheating is easier and never discovered} [13].

Identity impersonation is one of the cheat acts that must be prevented or at least discovered in the electronic examination systems. There are threats of impersonation in the electronic exams in these systems and classified into three types.[13]

Type A, Type B, and Type C Unfortunately, these types alone cannot guarantee electronic exam sessions cheat-free, so we suggested impersonation from type D.

2-1 Threat: These types are defined as follows:

1- Type-A (caller impersonation threat). It's supposed that the observer is necessary; in this case, impersonation may occur in two cases: the observer has not discovered the impersonator.

- Or the impersonation of identity is allowed by force or sympathy for financial purposes.

2- Type B occurs when the student passes his security information to a fraudulent person to answer the exam. The security information means (username and password), and in this case, the authentication and the presence of an observer reduce this threat.

3- Type C occurs when the real student logs into the website. This type will allow the fraudster to keep taking the exams instead of the examinee; we suggest validating the fingerprint for the examinee.

4- Type D; The real examinee is in the exam, but another person helps him get the correct answers.

2-2 Methods for validating the electronic exam:

Several authentication methods have been proposed in the electronic exam. These methods can be classified into three factors:

1- Knowledge factors: using a strong password in which the unauthorized parties cannot access the user information. These factors require that the user should have something unique such as (password).

2- possession factors: so that unauthorized parties cannot access the users' information unless they obtain the required codes, and here the user must have some unique codes that others do not have, such as (keys).

3- Correlation factor: Referred to this factor as the biometric authentication approach. It is categorized into two main methods [8]: image processing and pattern recognition such as fingerprint, voice tag, face recognition, and retinal pattern. The most effective user can do these

things to continue user authentication in electronic exams such as handwriting, keystroke dynamics, and mouse pressure dynamics.

• Although some of the mentioned authentication methods are very reliable, they have some defects, as they are summarized in the following table:

	Defects of the authentication method
1- If the password is abandoned, the security policy will be canceled 2-A one-time password is required when logging in, and they are never trusted for continuous authentication	Knowledge factors
1- If the token share it to others, the scheme will be circumvent security. 2- A one-time code is requested upon login, and it cannot be trusted for continuous authentication	Possessive factors
1- It is more reliable, but it requires special hardware. 2- It is unreasonably intrusive, expensive, and challenging to implement. 3- Some validated methods are frequently repeated, but they are not entirely reliable. 4-They are never trusted if others help them	Correlation factors

Table 1 Disadvantages of User Authentication Methods in Electronic Assessment [8].

3- Existing e-Examination Authentication Schemes

3-1. Fingerprint authentication (FPA)

The FPA is implemented in many web applications. For example, to authenticate the user in the electronic exam [12-8-14]. Nowadays, the fingerprint used for users to log in, and the manufacturers produced a mouse that depends on fingerprint, whereas the thumb scanner will compress for continuous authentication. Also, reliable fingerprint servers are available with a false rejection with a rate of 0.0%, and biometric authentication is conducted as follows: [14]

1- The user ID is created, and each product's thumbnails are scanned and stored in a secure server.

2- Login happens by using the user ID and fingerprint via the scanner device when it is required.

3- The device will be disabled, and the user will be able to access sensitive data.

Two measure of the security level of the fingerprint will be determined, as shown in the following equations .:[20]

1- FAR=IFA/TNIT

2- FRR=CFR/TNCT

whereas:

FAR is the false acceptance rate.

IFA indicates the percentage of fraudsters who accepted wrongly

TNIT is the total number of tested fraudsters.

FRR is the mistake.

CFR is the percentage of agents who are wrongly rejected.

TNCT is the total number of tested agents.

• FAR measures the probability of a falsely accepted fraudster, while FRR measures the probability of rejecting a valid user.

3-2. Keystroke Dynamics Authentication (KDA):

In this authentication, KDA suggests that the click speed from one key to another differs from one user to another, and this proposal has been presented with five measures to verify the identity of the user: [8]

1- Writing speed (measured in letters per minute).

2- The traveled distance between two keys, including the time the user keeps the key.

3- The time of searching on the required keystroke to search for a key before pressing it.

4- keystroke sequences which mean repeating written keys sequences.

5- Distinctive mistakes are the common mistakes that the user commits to be identified.

- Correlation is used to measure similarity among the features of the saved templates and the stroked keys, as shown in Eq. [8]

$$r = \sum_{i=1}^{n} \left(\mathrm{Ki} * \mathrm{Ti} \right) / \sqrt{\sum_{i=1}^{n} ki^2 * \sum_{i=1}^{n} ti^2 b} \quad)$$

whereas :

r: shows the correlation.

k: is the length vector.

n: the letter that saves the duration between moving from one key to another.

t is a vector of length N, which stores the travel time of the captured keys.

i-z-k-t is the duration between two keystrokes.

3-3. Algorithm Matching Video:

This algorithm was initially been proposed for the video search [15-16], but it can be used for continuous validation and automatic detection of cheating examiners. This video matched with its stored template using tree matching as shown in the figure, and the video clip is divide into several scenes in an organized tree. It consists of related snapshot groups. The matching process moves level by level and in a descending manner. Any of similarity calculated by using the color graph and snapshot pattern. Here, the algorithm uses the maximum order sum function to calculate similarity in four steps.

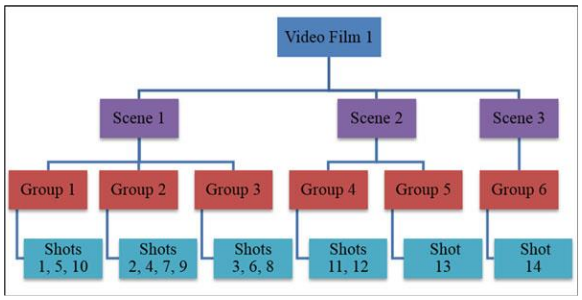

Fig.2 Structured video tree [15]

Current electronic examination certification systems:

These existing solutions to validate the electronic exam are classified into five main categories, and from here, a comparison will be made between these schemes and our schemes:

1 The Observer System: This system requires the presence of an observer or a test official to monitor the examinees during their exams, and here a study was conducted in which 200 students took the electronic exam in WEBCT computer lab [17] and three neighboring laboratories were assigned at the same time, a WebCT expert was appointed for technical support, and here the authentication was comfortable in the case that the observers were teachers of the students and they knew them well. In this study, the password and the username were given to the observers who distributed them during each session. [10]

3-4. single-modal biometrics chart.

3-5.Bimodal Biometrics Schemes :

This scheme uses a single biometric approach for authentication; for example, we use web-based face recognition authentication for student verification.

Identity with student tracking (Bio Tracker), which can track students while taking exams at home and Bio Track can be integrated with LMS where two concepts are investigated :

A- Uncooperative verification.

B- The handwriting approach is another example of this scheme where there is a tablet pen for writing the letters that are most used in multiple test questions. Typed letters are compared to templates taken before the exam. [18]

The figure below shows an example of a single handwriting letter written on a piece of paper that has been adapted to recognize electronic testing.

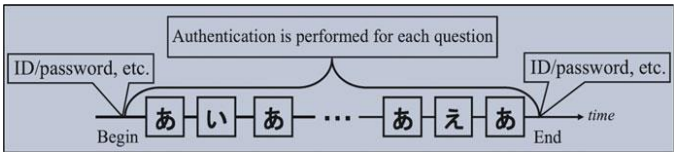

Fig.3 Handwriting authentication using LAP [18]

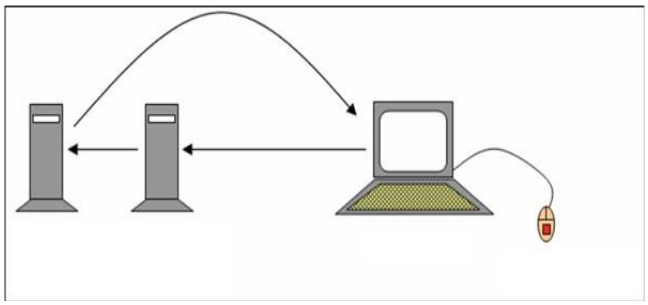

Fig.4 Fingerprint for e-Exams users' authentication [12]

This is another example that takes multiple random fingerprints for the examinee throughout the electronic exam, and this example prevents plagiarism (i.e., pretending to be another examinee).

3-6. Video monitoring:

Video monitoring of students' activities during the electronic exam is also applied using the web camera [8]. This type requires a password to log in and random or rare footage taken during the exam to be reviewed by the observer after the exam. It also requires additional effort to watch the video clips. The figure below illustrates the structure of the electronic test diagram, which has three primary interfaces:

a- The administrator interface: (it is the one that manages the user accounts and the received video)

b- The faculty members interface: (which records the exams, shows the results, and displays the captured footage)

c- Student interface [21]

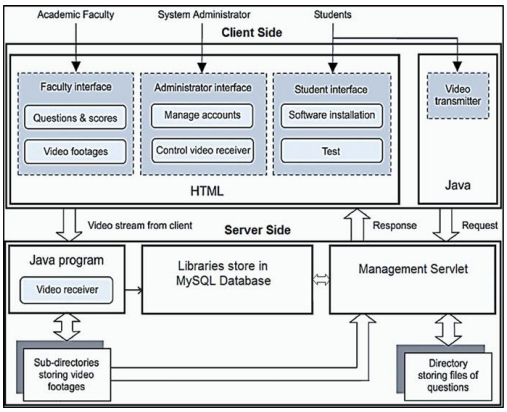

Fig.5 Structure of e-Test scheme [21] adapter

3-7. Biometrics authentication and webcam monitoring:

This system combines fingerprints and real-time video monitoring. The figure below shows the illustration:

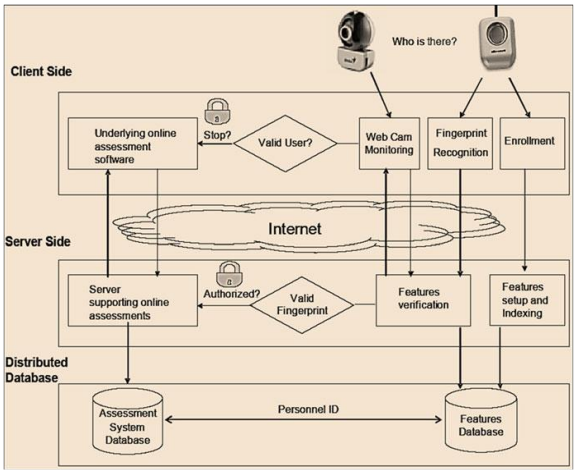

Fig. 6 Structure of combined fingerprint and video-monitoring in e-Examination [20]

When the connection is established on the server, the examinee is asked to scan his fingerprint. If it matches the store, he can continue the exam, and

when the test begins, the webcam sends the video to the server to monitor the examiner. In case of non-compliance, the exam is interrupted and reprocessed.

4- proposed schemes :

In the light of safety that the research mentioned previously to protect the electronic exams, the researcher suggests another thing that is called safety questions in which some secret questions answered by the examinee in the exam have existed in the electronic exam. These questions have been stored with their answers which the examinee answered earlier on the server and during the exam, one or two questions of these questions have appeared to the student in an average time of five seconds after that it has been compared the answers of these questions with the presented answers earlier. In this way, it can be validated that the real student is the one who does the exam not another student. Unfortunately, several problems may face us, including:

The student may not know the answers to the secret questions that he answered earlier and this is one of the most common methods that the student writes scattered words and does not see the importance of the protection questions.

The student is not able to answer within the specified period or he apologizes because his device used is slow regarding a problem on the Internet.

But this is one of the methods that must be applied due to its importance in addition to the process of tracking the keystroke.

The two figures below represent a suggestion of some types of presented security questions.

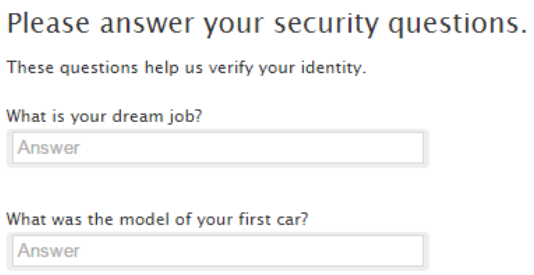

Fig. 7 security question (scheme q 1)

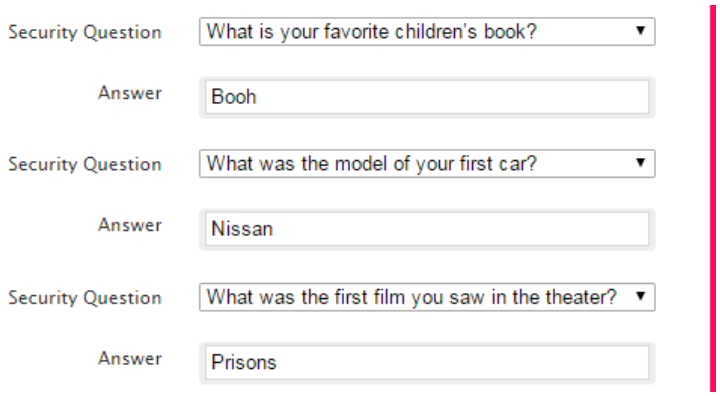

Fig.8 security question (scheme q 2)

5- Conclusion :

It turned out that the matter is vital for e-learning systems because they work and contain sensitive information and processes, and one of these processes is the electronic exam, which has received significant attention recently because schools, universities, and courses have shifted from traditional learning to electronic learning and

exams due to the pathological conditions prevailing in countries of the whole world.

The electronic exam faces a number of problems, the most important of which is that the electronic exam is not entirely reliable, and from here many efforts have been made to provide a reliable electronic test by proposing a new scheme in addition to the standard electronic authentication methods used in the electronic exam to raise the level of safety and reduce fraud, despite From these schemes, we can not find a competition between the traditional student-teacher-based exam, the exam in the school or university halls, to prevent cheating and real evaluation.

This work contributes to solving the problem of fraud and raising the level of safety in the electronic exam while taking into account most of the potential weaknesses in each method.

In our proposed model, we can contribute to the field of continuous validation that the actual student is the one who takes the exam, and it may be a competitive, simple, and easy-to-implement method, as it is possible to demonstrate reasonable security with its predecessors from the certification systems.

References

[1] E.Ktizinger, "Information Security in an e-Learning Environment",2006 Last access Dec. 2016 http://sedici.unlp.edu.ar/bitstream/handle/10915/24349/documento_com%20pleto.pdf%3Fsequence%3d1

[2] R. Raitman, L.Ngo, and N. Augar, "Security in the online e-Learning Environment" Proceedings of the 5th IEEE International Conference on Advanced Learning Technologies,Kaoshsiung, Taiwan,pp702-706, July 2005.

[3] W. Stallings, "Data and Computer Communications", Eighth Edition, Prentice Hall 2007.

[4] K.El-Khatib, L.Korba, Y.Xu, and G. Yee, "Privacy and security in e-Learning", International Journal of Distance Education, vol.1, no.4, PP.1-19,2003.

[5] J. F Gonzalez, M. C. Rodringuez, M. L. Nistal, and L. A. Rifon, "Reverse OAuth: A Solution to Achieve Delegated Authorizations in single Sign-On e-Learning Systems" Computers and Security, Vol.28, no.8, PP843-856, November 2009.

[6] M. Hentea, M. J. Shea and L. Pennington, "A Perspective on Fulfilling the Expectations of Distance Education", Proceedings of the 4th Conference on Information Technology Curriculum (CITC4) Lafayette, Indiana, USA, PP.160-167, October 2003.

[7] N. H. Mohd Alwi, and I.-S.Fan, "Information Security Threats Analysis for e-Learning" Proceedings of the First International Conference TECH-EDUCATION, Athens, Greece, PP.285-291, May 2010.

[8] E.Flior and K.Kowalski, "Continuous Biometric User Authentication in online Examinations", Proceedings of the 7 the International Conference on Information Technology: New Generation, Las Vegas, PP.488-492, April 2010.

[9] S Alotaibi, "Using Biometrics Authentication via Fingerprint Recognition in e-Exams in e-Learning Environment", In the 4th Sudi International Conference, The University of Manchester, UK, July 2010.

[10] N.C. Rowe, "Cheating in Online Student Assessment: Beyond Plagiarism", Online Journal of Distance Learning Administration, vol.7, no.2, summer 2004

[11] M. Dick, J. Sheard, C. Bareiss, J. Carter, D. Joyce, T. Harding, and C. Laxer, "Addressing

[12] Student Cheating: Definitions and Solutions", ACM Special Interest Group on Computer Science Education Bulletin, vol.[32], no.2, pp.172-184, June 2003.

[13] Y. Levy and M. Ramim, "A Theoretical Approach for Biometrics Authentication of e-Exams", Chais Conference on Instructional Technologies Research, Israel, pp.93-101, 2007. Last access December 2016. http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf

[14] K. M. Apampa, G. Wills and D. Argles, "User Security Issues in Summative e-Security", International Journal of Digital Society, vol.1, no.2, June 2010.

[15] A. Kapil and A. Garg, "Secure Web Access Model for Sensitive Data", vol.1, no.1, pp.13-16, January-June 2010.

[16] C. W. Ng, I. King, and M. R. Lyu, "Video Comparison Using Tree Matching Algorithms", Proceedings of the International Conference on Imaging Science, Systems and Technology, Las Vegas, USA, pp.184-190, June 2001.

[17] M. S. Ryoo and J. K. Aggarwal, "Spatio-Temporal Relationship Match: Video Structure Comparison for Recognition of Complex Human Activities", Proceedings of the IEEE 12th International Conference on Computer Vision pp.1593-1600, Kyoto, Japan, September-October 2009.

[18] G. Harrison, "Computer-Based Assessment Strategies in the Teaching of Databases at Honours Degree Level 1", In H. Williams and L. MacKinnon (Eds.), BNCOD, vol.3112, pp.257-264, Springer 2004.

[19] S. Kikuchi, T. Furuta, and T. Akakura, "Periodical Examinees Identification in e-Test Systems using the Localized Arc Pattern Method", Proceedings of the Distance Learning and Internet Conference, Tokyo, Japan, pp.213-220, November 2008.

[20] Y. Levy and M. Ramim, "Initial Development of a Learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM)", Interdisciplinary Journal of e-Learning and Learning Objects, vol.5, pp.379-397, 2009.

[21] J. A. Hernández, A. O. Ortiz, J. Andaverde and G. Burlak, "Biometrics in Online Assessments: A Study Case in High School Students", Proceedings of the 18th International Conference on Electronics, Communications and Computers, Puebla, Mexico, pp.111-116, March 2008.

[22] C. C. Ko and C. D. Cheng, "Secure Internet Examination System Based on Video Monitoring" Internet Research: Electronic Networking Applications and Policy, vol.14, no.1, pp.48-61,2004

[23] National Institute of Standards and Technology. An Introduction to Computer Security: The

[24] NIST Handbook. Special Publication 800-12, October 1995.