E-PROCTORING SYSTEMS: A REVIEW ON DESIGNING TECHNIQUES, FEATURES AND ABILITIES AGAINST THREATS AND ATTACKS

MOHAMMED, H. M.[1*] – ALI, Q. I.[1]

[1] *College of Engineering, University of Mosul, Mosul, Iraq.*

**Corresponding author*
e-mail: hussein.mahmood[at]uomosul.edu.iq

(Received 17th March 2022; accepted 29th June 2022)

Abstract. E-proctoring systems have been proposed and discussed by many researchers and developers previously, but each of these systems has strengths and weaknesses in terms of facing fraud, threats and attacks. Where the e-proctoring systems face many problems that stand in the way of their complete adoption by universities and educational institutions that rely on remote learning, and these problems include cheating, plagiarism, impersonation, theft or leakage of questions, attacks and other security issues which compromise the academic integrity of e-exams. This review was conducted to present the components, types, methods, and security issues related to e-proctoring systems and discuss their technologies, features, and strengths and weaknesses to determine the possibility of designing a safe and effective e-proctoring system against threats and attacks. The study concluded that the use of some restriction programs and monitoring devices led to an increase in the efficiency of these systems, but there are still security vulnerabilities facing e-proctoring systems which must be overcome by modern and effective security solutions.
Keywords: *e-proctoring, cheating, threats, cyber security attacks, authentication, LMS*

Introduction

Remote learning has become a common practice and it has replaced a large percentage of traditional classroom education, especially after the pandemic of COVID-19 (Andersen et al., 2020). Online exams are used to assess the knowledge of students remotely with no need for the physical presence of proctors, which means online proctoring systems have to be used to conduct these exams (Alghamdi et al., 2020). However, the first major challenge that faces online exams is cheating, and the first question to be asked when designing any online exam system is: how to proctor online exams in a convenient, efficient and reliable manner (Li et al., 2021). Researchers and developers make an effort to facilitate the learning process through innovations that can be obtained by employing and integrating objects to the Internet, hence creating new opportunities for applications and services in the learning domain. Besides, the exponential increase in e-learning has motivated scientists and researchers to devise an effective e-proctoring system that can be administered remotely. Many proctoring methods for online exams have been proposed previously by researchers and developers, like online webcam-based proctoring (also known as live proctoring), and biometrics-based proctoring that authenticates students depending on their biometrics and detects cheating by monitoring student`s activities such as head and eye movement, or mouse movement during the exam session. Others proposed to combine several of these methods to obtain an integrated e-proctoring system. The use of Internet of Things (IoT) provides a lot of facilities for both teachers and students, where it enhances teachers' knowledge (through the data of learning) about their students' performance and

their learning progress, and at the same time informs teachers about the difficulties that the students may face, as well as it creates an interactive learning environment for both teachers and students.

On the other hand, online exams and e-proctoring systems are vulnerable to cyber threats and attacks (Slusky, 2020), because they take place via the Internet (Chen and He, 2013), and mitigating these attacks and threats is considered a criterion for any proctoring system to be successful (Rjaibi et al., 2012). There are different types of security threats that the e-proctoring systems can be exposed to, some of them are active (can be detected) and the others are passive (can't be detected), and these threats can be divided into internal threats which are done by authorized individuals (e.g. examinees, proctors) or external threats which are done by unauthorized individuals or entities outside of the system. Ullah et al. (2016), classified security threats into two general types: intrusion and non-intrusion, and further they classified non-intrusion threats into two sub-types: collusion and non-collusion threats. Prior researches (Slusky, 2020; Carrascosa, 2017) classified threats depending on CIAA (Confidentiality, Integrity, Availability, and Authentication) and described the applicability of each element of CIAA to an e-proctoring system (Nickolova and Nickolov, 2007). The current existing e-proctoring systems have features that may differ from each other, and every system may be vulnerable to specific security threats.

In this paper, an academic review on previous research and works related to e-proctoring systems was conducted, as well as a study of the currently used e-proctoring systems to review their features, advantages, and disadvantages, and finally, an e-proctoring system was proposed to exceed, as much as possible, all or most of the problems and challenges that currently exist, to achieve acceptable results with the lowest, as much as possible, percentage of errors. The structure of this paper is as follows, related works were presented in section II. Definition, components, and types of e-proctoring systems were explained in section III. In section IV issues related to e-proctoring systems like cheating, threats, and security attacks were discussed in detail. The current existing e-proctoring systems and their features were discussed in section V. The discussion was presented in section VI. Finally, the conclusion was presented in section VII.

Related work

Many research papers presented the online examination systems and the factors affecting them, and many studies explored the matters that help these systems to be successful to overcome the obstacles that prevent e-exams to be smooth, reliable and safe. Muzaffar et al. (2021), performed a systematic literature review of electronic exams, they selected 53 papers and analyzed them. The authors explored five e-exams features from the selected research papers and they discussed the solutions for implementing and applying e-exams in terms of basic development approaches. Furthermore, they identified 21 e-exams tools that were proposed in the selected studies. In addition to this, the study presented 16 important techniques and algorithms, and 11 datasets, as well as 25 leading existing tools used in the selected studies, were also presented. The authors identified key factors for the global adoption of electronic exams and they made a comparison between them and the major electronic exam features. As the authors thought, the right type of e-exam system can be chosen easily depending on the comparison of the characteristics of the e-exam systems mentioned in their study, the infrastructure of the existing e-learning, and the overall cost.

Another systematic review was made by Karim and Shukur (2015), the study focused on three main topics related to e-exams, user authentication methods, system design, and threats. The authors explored authentication methods that have been used in e-exam systems (e.g., username and password, challenge question, keystroke, timestamp, etc.) and they classified them as knowledge-based, possession-based, and biometric-based. They also presented e-exam systems in terms of authentication technologies used in these systems, and they identified three classes of these techniques, user identification, authentication, and continuous authentication, and summarized the strengths and weaknesses of these techniques. In addition, they presented threats that may occur during e-exams and may threaten the system. Finally, the study presented user authentication methods that are used in the existing e-exam systems like ProctorCam, ProctorU, BioSig-ID, SecureExam, and Webassessor. The authors concluded that the most accurate and popular method for user authentication is the biometric-based method. They also investigated that impersonation is the most type of threats that faces e-exams (Karim and Shukur, 2015).

Butler-Henderson and Crawford (2020) discussed the e-exam systems from the pedagogical point of view, and they performed a systematic review on the topic to present the challenges and opportunities. The study investigated thirty-six papers and focused on nine key themes: student perceptions, student performance, anxiety, cheating, staff perceptions, authentication and security, interface design, and technology issues. In reference (González-González et al., 2020), a study was made on e-proctoring systems and the motivational factors that motivate the transition from traditional examinations that require the physical presence of examinees toward online exams. The authors studied many factors which are considered the most motivational factors including Quality management, external conditioning, available information, attitude and intention, trust, perceived compatibility, and perceived usefulness, and as the authors thought, the trust factor (which represents security and privacy) is the most decisive factor between other factors in the process of online proctoring. The fuzzy cognitive maps (FCMs) method was used to analyze the gotten information from reviewers.

Foster (2013), stated in his handbook the possible security issues in online exams and technology-based testing, and he mentioned the two main categories of security problems (as he thought) privacy and cheating, and he discussed in detail everything related to test theft and cheating. He also suggested some solutions for test fraud on technology-based tests as protecting test files, downloading only required items, controlling the browser and operating system, using protective item design features, and many other suggestions to mitigate security issues. Reference (Bandara et al., 2014) mentioned some security risks in online exams and suggested some solutions regarding every type of these risks to protect the exam against these risks, like brute force attack, ARP cache poisoning and MITM attack, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).

E-proctoring system

Proctoring, also known as Invigilation, is the process of watching people doing an exam or taking a test to prevent them from cheating. Hussein et al. (2020) defined e-proctoring operation as “the ability of teachers and educational organizations to ensure academic integrity in the absence of a live proctor when an examination is being taken remotely and from a private location”. However, e-Proctoring is a service that can be

managed by a third party online exam proctoring, and it is a method that is used to monitor students as they do their exams in any private location of their choosing. It can be live by a webcam only or technology-based (will be discussed in coming sections) using AI. Researchers and developers proposed different virtual tools to be used in e-proctoring to monitor student activities during the assessment session. By developing these virtual tools to overcome vulnerabilities, researchers and developers can ensure integrity and reliability for e-exams taken by students from anywhere and at any time. This includes some procedures like disabling some properties of the students' exam devices to prevent cheating and authentication (maybe a continuous authentication) of the students to secure and maintain the integrity of an exam (Foster and Layman, 2013). Others defined e-proctor as using a person and/or a system to support invigilation, where the proctor is not physically presented, and to use online connectivity to observe, analyze, and record test-taker behavior.

A: Components of e-proctoring system

Any e-proctoring system, to be acceptable and successful, should be reliable, robust, and dynamic. Most responsibility of these systems relays on the software because the software of the e-proctoring system is at the heart of any e- proctoring system. Nowadays, with the development of communication systems, and the use of the cloud, e-proctoring is usually driven by a cloud-based system (Exam Online Official Portal, 2020). *Figure 1* shows the components of the e-proctoring system, and subsections B and C present the components of the e-proctoring system in detail.

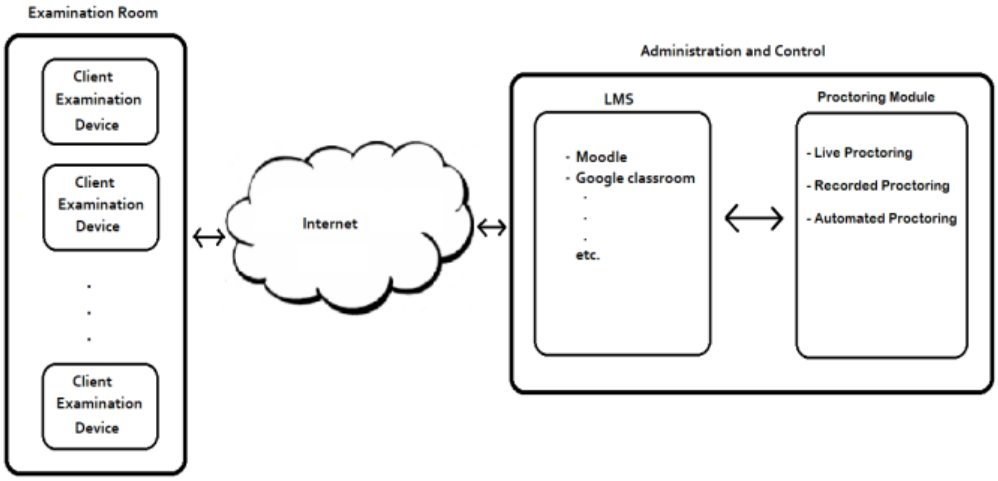

Figure 1. *E-proctoring system components.*

B: Examination

This part of the system involves examinees` devices, and monitoring tools like webcam, microphone, etc. The examinee's device can be a desktop, laptop, tablet, or a special device that is manufactured only for performing the exam through it. It's better if the examination devices are portable, so the students are free to do their exams from anywhere they want. Some of the properties of these devices should be disabled before the student do the exam, so he cannot open any website, any file stored on his device, or cheats from any other resource. To do so, restriction software must be used, for example, Lockdown Browser (a restriction browser), where the examinee is restricted

and has no way to exit/return, use keyboard shortcuts, or manipulate the system. However, some exams might require Internet access to some specific websites, or perhaps the examinee needs to use the e-mail or chat functions, therefore, the settings and configuration of Lockdown Browsers should be updated for every exam (Atoum et al., 2017). Monitoring tools are either integrated with the exam`s device or stand-alone as separate devices. These devices monitor the student during the exam session, so, the proctor can indicate if there are suspicious activities (Prathish and Bijlani, 2016).

C: Administration and control

This part of the system involves Learning Management System (LMS), and Proctoring Module. To facilitate examination management processes like creation, distribution, and management of the delivery of questions to students, e-proctoring systems use software to automate all the functions mentioned above called Learning Management System (LMS) (Turnbull et al., 2019). LMS can be defined as web-based software platforms that provide an interactive online learning environment and automate the administration, organization, delivery, and reporting of educational content and learner outcomes. According to Mahoney and Cameron (2008), LMS automates many of the processes associated with e-learning, it is a management software package enabling the delivery of learning content, resources and activities and also handles the associated administration tasks (Oliveira et al., 2016). The LMS can be hosted as a stand-alone product on the company server, or it can be a cloud-based platform that is hosted by the software firm. LMS has many features that can be utilized in e-proctoring systems to make the proctoring process very effective for both students and instructors, these features may include: (1) offering certifications by providing a place online for instructors to conduct courses and assessment tasks, like assignments and pop quizzes and hence allow students or learners to access these courses and assessment activities; (2) capability for event scheduling and content management through a specific training system; (3) providing course improvements as well as technical support; (4) providing centralization to access content for all learners, instructors, as well as course creators to easily and securely complete tasks; (5) makes the learning process more interactive for both learners and instructors through live classroom and webinar environments, client presentations, etc.; and (6) the ability to automatically correct exam questions and give the score immediately.

Proctoring module includes a control unit and proctoring unit where the instructor monitors the students' activities online or by recording the examination session and displaying it later to detect suspicious activities. There are different types of proctoring methods discussed in the next sub-section.

D: E-proctoring methods

E-proctoring systems are divided in general into three methods (Hussein et al., 2020): (1) live (online) proctoring; (2) recorded proctoring; and (3) fully or semi-automated proctoring. Other researchers (Asep and Bandung, 2019; Atoum et al., 2017), classified e-proctoring methods into four categories, no proctoring (Wahid et al., 2015; Cluskey Jr et al., 2011), human online proctoring (Jung and Yeom, 2009; Guo, 2008), semiautomatic proctoring (Rosen and Carr, 2013), and fully automated online exam proctoring. However the no proctoring method was proposed by with eight strict procedures are imposed on the test taker to increase the difficulty level on cheats

probability, and hence prevent or at least minimize cheating happens online exam environment. A human online exam proctoring (also known as live online proctoring), is a real-time proctoring method, taking place during the exam with a human proctor monitoring/supervising the exam online. This method is based on sending a real-time video or image of the test takers to a streaming media server (Asep and Bandung, 2019). The human proctors have to be professionals to ensure the authenticity of the student and have the ability to detect any abnormal activity such as gazing outside the exam screen, abnormal facial reactions, the existence of unauthorized resources in the exam room, or any other breach. However, there are some drawbacks to this method, where the exam must be scheduled at a date and time that the proctor is available. Moreover, online proctoring requires that the proctors have good knowledge of using technology and also they should develop their efficiencies in online proctoring approaches (Hussein et al., 2020).

Recorded proctoring method, this type of proctoring depends on the recording of the camera that involves student activities throughout the exam session. The proctor then assesses the integrity of the exam by reviewing the recording at a specific time and indicates if there are any malpractices like cheating or fraud. The advantage of this type of proctoring is allowing the student to do his exam at any time. However, the disadvantage of this type is the intervention of human proctors to review the recorded videos, this consumes more time and may be very expensive and hard to apply to high scale exams (Sinha and Yadav, 2020). Semi-automated proctoring method, this method requires additional devices and tools to decrease cheating opportunities on the test taker and to help the proctor to detect any suspicious things that the camera cannot detect, where a proctoring data consists of video streaming, audio streaming and screen snapshot continuously are sent to the server (Rosen and Carr, 2013). A 360o camera and additional sensors (e.g. movement sensor) can be used to send the recorded video to the proctoring and controlling unit when suspicious or violation events are detected. Fully-automated online exam proctoring method is used to detect cheating or fraud attempts of examinees. In this method, there is no intervention of human proctors in the monitoring process, in other words, the monitoring process is the responsibility of the system, the proctoring system indicates the human proctor only when an attempt of cheating or fraud is detected (Tashu et al., 2019). The human proctor is indicated to assess if there is a real attempt for fraud or cheating by reviewing the recorded events. Students and test-takers favor this type of proctoring because there are no constraints from human proctors, they do not need to deal with a human proctor to arrange for an exam, and like the recorded proctoring method there is no scheduling for exams times.

One of the advantages of this type of proctoring is considered to be very scalable, and more cost-effective because of the use of artificial intelligence, techniques, and algorithms instead of human proctors. However, the disadvantages of this method lay in the fact that these techniques and algorithms can be broken and defrauded if the student or examinee can understand the rules on which these techniques and algorithms operate, as well as, this method can involve false positives (e.g. flagging innocent events as potential fraud).

Issues related to e-proctoring systems

Online exams are the most complex process in the e-learning system, as they are considered the most important and focused part for researchers and developers. Therefore, the level of challenges and issues facing online exam systems are at the same

level of that importance. Usually, e-learning platforms are used to conduct online exams, this may require the examinees and the proctors not to be physically present at the same location. This may create security vulnerabilities that can be exploited by examinees or attackers and thus lead to a lack of integrity in exams and reduce the efficiency of the system (Langenfeld, 2020). As it is explained above, e-proctoring systems consist of multiple processes and functions that work simultaneously to complete the online exam operation perfectly. If we take the authentication process as an example of one of these processes, it is considered a very big challenge to the e-proctoring system (Sarrayrih and Ilyas, 2013), where there are many papers and articles (Aisyah et al., 2018; Karim and Shukur, 2015; Smiley, 2013; Clarke and Furnell, 2006) discussed the authentication process and proposed many ideas to mitigate this problem. Moreover, the Internet is an ideal environment for cheating in online exams, as thousands of sources and information that the examinee needs can be easily accessed.

Furthermore, no one can ensure the availability of the Internet to all of the examinees throughout the exam session, as well as in some cases the examinee needs a high-speed connection required for continuous monitoring or for uploading some required files (Muzaffar et al., 2021). These are not the only challenges that face online exams, there are other challenges that the e-proctoring system suffers from, like cybersecurity attacks, threats, privacy, and other issues related to the technical requirements (Ghizlane et al., 2019). All aforementioned problems and issues are discussed in detail in the next sub-sections.

A: Cheating

The first major challenge or issue in online exam systems is cheating. This section presents the types of cheating threats in e-proctoring systems and their countermeasure. Cheating depends on circumventing the rules and violating them directly or indirectly, and this is what many students and examinees around the world do (Fask et al., 2014). The methods of cheating in e-exams are not much different from their counterpart in traditional exams, where some of the traditional cheating methods are writing on small scraps of paper, looking at another colleague's answer sheet, writing on pens and rulers, writing on hands, etc. On the other hand, the means of cheating in e- exams can be, the use of portable communication devices, the use of hidden Bluetooth headphones, programmable calculators, and a lot of modern cheating technologies. Many research papers in the literature (Bawarith et al., 2017; Mitra and Gofman, 2016; Cluskey et al., 2011; Korman, 2010) discussed the activities of students in terms of cheating and proposed how to eliminate or mitigate this issue (Chua et al., 2019).

Despite the many benefits and advantages of the e-exams (e.g., saving printing and paperwork, reducing costs and time) if they are replaced by the traditional exams, the percentage of cheating or trying to cheat can be higher in e-exams (Bawarith et al., 2017). Where a study was made by King, Guyette, and Piotrowski (King et al., 2009), stated that 73.6% of students assume that cheating in online exams is much easier than in traditional exams, and Ndume et al. (2008), said that it is much harder to prevent cheating in the online environment than in the conventional environment. With the emergence of multiple means of communication via the Internet, as well as the rapid development of information technology, several forms of cheating in online exams have emerged, including (not limited to) using social media to exchange information, surfing the Internet (Rogers, 2006), copying from other sources, doing the same exam several times, or obtaining help from unauthorized sources (Underwood and Szabo, 2003).

There are many forms of online exam cheating (Rowe, 2004), like: (1) impersonations; (2) plagiarism; (3) time breaches; (4) stealing exam questions before or even after the exam; and (5) collaboration between students or getting assistance from others.

As mentioned above, researchers and developers suggested and proposed many technologies and tools to prevent or minimize cheating in e-exams (Opgen-Rhein et al., 2018; Bawarith, 2017; Cavalcanti et al., 2012), some of these tools are webcams, microphones, attached sensors, and so on. The technologies that can also be used to countermeasure cheating are Lockdown Browser, recording windows activities, mouse movements, eye tracking, and keyboard shortcuts restrictions (e.g. copy/paste, print screen). Furthermore, there are some instructions and procedures that can be followed to prevent or reduce cheating during the e-exams (Korman, 2010): (1) randomizing sequences of the questions as well as sequences of the choices of the question itself in MCQ questions; (2) disallowing the use of utility tools such as (calculators, and data sheets), instead, it is possible to include these tools within the e-proctoring system; (3) displaying one question at a time, instead of displaying all the questions simultaneously, and randomizing the sequence of the questions, this makes variations between the questions displayed to the participants; (4) informing the participants that there is an automatic checking for plagiarism; (5) using of biometric authentication based system, to prevent impersonation; (6) using technologies that combat cyber-attacks like firewall, antivirus, and other modern technologies; (7) implementing an excellent security system; (8) using a good system that improves confidentiality, accountability, authentication, and authorization; (9) using cryptography techniques to protect data from being stolen; as well as (10) training proctors to professionally manage the exam session to give participants a strong perception of how well the proctors can detect cheating, thus preventing them from trying to cheat.

B: Threats and attacks

E-exam systems use the Internet as the main infrastructure to complete the process of students evaluation (Reeves, 2000), and since the Internet is open to everyone around the world, it can contain many forms of security threats (Furnell and Karweni, 2001), like: (1) masquerading; (2) fraud; (3) malicious software (e.g. viruses, worms, Trojan horses); (4) spoofing; (5) hacking; and (6) denial of service attacks. E-proctoring systems are considered easy prey if they are not strong against these threats. Security threats and attacks are real issues for e-exams because they break the Confidentiality, Integrity, and availability of the system. Therefore, the institutions and universities that use e-exams, apply some procedures, like anti-virus programs, IT tools, scanning and monitoring, and prevention of unauthorized software installation. Moreover, the students in the online environment will be more worried in terms of security concerns than in the conventional environment, which requires more focus on security aspects and providing solutions for these issues.

If we want to classify the attacks according to the location of the attack to the e-proctoring system as a whole, they can be classified as follows (Bandara et al., 2014): (1) software attack: software is the main part of any system and can be argued that the software is a major cause of a system's success or failure. The solution for software attacks is applying good code and secure software in all layers of the implementation; (2) network device attack: this type of attacks can occur when the installation of the network devices is insecure, the device driver software is not up to date, or they do not meet network device configuration standards. To prevent this type of attacks, adopt

standardized devices, make a secure installation and configuration, and be ready and prepare failover scenarios; (3) administrator attack: this type of attacks is done through direct dealing with the proctors, where the test-taker can interact with the proctor and try to bribe him, or threaten and intimidate him. This type of attacks can be eliminated by securing the proctor's identity; as well as (4) user attack: is the attack that is done by a third party that makes the test-taker unable to do his exam at the scheduled time and location. The solution for this type of attacks is by rescheduling the exam.

C: Security threats causes

Threats in e-proctoring systems can be tested from two sides: the examinee side and the administration side. The lack of knowledge of the modern communication technologies and emerging techniques, and incorrectly using them, is considered a weak point in the e-proctoring system, which facilitates its exploitation to carry out security attacks on the system. Besides, the security threats that exist on the Internet, the tendency of some institutions to use new not robust technologies, as well as the use of social media helped to allow new security threats to emerge (He, 2012), where recent studies have shown that social media can be utilized to easily carry out attacks and security threats (Lozhkin, 2014; Patel et al., 2012). On the other hand, security issues can be analyzed from the user's point of view, where according to Adams and Blandford (2003), there are two main reasons for security threats in online exams: (1) the mechanisms of security procedures used in e-proctoring systems lack usability; and (2) the security protection process is entrusted to the designers of e-proctoring systems, and therefore the user considers himself not interested in providing security protection and this leads him to neglect many security aspects. They also argued that the security mechanisms' usability is reduced because of the principle of limiting information to only those who need it, in addition to the tendency of some institutions that use e-proctoring systems to unwillingness to know their users. Several e-learning systems do not provide users with sufficient feedback and do not give them the right to control the protection of their data, because of the lack of usability mentioned in the first point above.

D: Detection and protection against threats

The same characteristics and challenges are shared by e-proctoring systems, and like other e-services, they require the sharing and distribution of information. More specifically, the accessibility of service for e-proctoring systems is associated via the Internet (Slusky, 2020). In conjunction with the development of cyber-attack methods, researchers and developers of e-proctoring systems recommend focusing on the security aspect of these systems, taking into account that these security threats are different and varied, so the system design must be commensurate with the level of threats that the system may be exposed to. As mentioned earlier, there are several security threats that e-proctoring systems can be exposed to, like malicious software, snooping, data theft, and intellectual property (piracy, copyright) (Huang et al., 2020). There are many forms of threat, where it can be a person, an object, or any entity that presents a danger like Viruses. The type of threat that the system may be exposed to, depends on the security method used by the system, where the systems that authenticate users by password can be vulnerable to phishing attacks.

Some researchers proposed different protection ideas and used many techniques to manage, quantify, and mitigate security threats. Some papers have discussed security protection from two sides, the examinee side, and the administration side, from the examinee side, a theory called Protection Motivation Theory (used in social psychology) can be used in the information system security field (Rjaibi et al., 2012), by applying this theory the system perceives and evaluates the information and then indicates the user to take the suitable action. The PMT theory is very useful for the users to understand measures of protection for security threats and attacks, and from the administration side, scholars of information security systems adopt a theory called General Deterrence Theory (used in criminal justice). By applying this theory, the scholars show that the perceptions of members in an institution can be increased by security countermeasures regarding the severity and certainty of punishment for any misuse of information. Researchers have proposed many solutions and countermeasures that protect the system from threats and attacks, where Mohd Alwi and Fan (2010) proposed that the providers of e-learning have to apply information security management (ISM) to build a robust security base that prevents security threats and attacks. Other researchers, Furnell and Karweni (2001), discussed security threats issues and proposed a framework to protect the system, the aspects that had been covered in this framework include: (1) authentication and accountability; (2) access control; (3) protection of communications; (4) non-repudiation issues; and (5) learning resource provider server protection.

E: Privacy concerns in e-exams

The designing of any e-proctoring system requires that the ethical aspect should be taken into account in monitoring and analyzing the behavior of the examinee during the exam session (Bandara et al., 2014). Raising the level of security to protect the e-proctoring system from cyber-attacks should not violate the user's privacy. Also, the users' sensitive data must be confidential and maintained in a way that the data cannot be accessed by others and used for commercial and immoral purposes. The term privacy is related to some extent to security, where maintaining the privacy of users requires providing a robust and secure system that prevents intruders and attackers from accessing the personal data of users. Moreover, users must have a good level of understanding of security related issues to protect their data despite the protecting users' data is the responsibility of the providers of e-learning systems, by providing a secure learning environment (Lorenz et al., 2012). On the other side, the students or test-takers have to take some steps to protect their data like using strong passwords to create their accounts, do not share their usernames and passwords with their colleagues, do not sign in to their accounts from devices that they do not own (Huang et al., 2020). The research papers in the literature show that user privacy management is in three modes: In the first mode, e-learning providers manage the user's privacy and do not give him the rights to control his data, in terms of storing or protecting it. In the second mode, the responsibility for privacy management is through the users themselves, so they must have a high level of awareness of knowledge and understanding of privacy management to preserve their data. In the third mode, the bulk of the responsibility lies on the providers of the e-learning environment, and the other part falls on the users themselves through procedures directed to them by the instructors of the e-learning system (May and George, 2011).

F: Authentification

User authentication, a widely discussed subject in online environments, is the process in which the identity of the examinee is ascertained, and he is verified as he claimed to be (Smiley, 2013). Online exam systems perform authentications such as username, password, timestamp, challenge question, and biometric authentication. In general, user authentication is classified into three main categories (Karim and Shukur, 2015); something the user knows known as knowledge-based authentication (e.g., password, PIN, pattern), something the user has known as possession-based or token authentication (e.g., ATM card, smart card, mobile phone), and something the user is known as biometric-based authentication (e.g., fingerprint, face, voice). Due to the importance and sensitivity of e-proctoring systems, and in order to preserve the integrity and credibility of online exams, the authentication mechanism must be robust and effective (Marcialis et al., 2009). The Username and password based authentication method is considered the weakest among other authentication methods, so providing a secure and robust alternative method is very necessary. In addition, the authentication method should be easy to apply by users without unnecessary complications that bother users and make the system undesirable (Clarke and Furnell, 2006). E-proctoring systems often require continuous authentication (Aisyah et al., 2018) to authenticate the student throughout the exam session (Traoré et al., 2017). The systems that investigate exams by human proctors may depend on a 360o camera to authenticate students without using any authentication method during the exam session, just at the beginning of the exam may require authenticating the student and for one time.

Features of e-proctoring systems

When we talk about e-proctoring features, we can discuss them from four main aspects, and we can make a comparison between them according to these aspects (OReilly and Creagh, 2016; Foster and Layman, 2013). Firstly, the general characteristics and control, where there are differences between online proctoring systems of what the system requires from the test-taker to be available during the test, what technologies that the system requires (e.g., Internet speed, Encryption for Data Transfer, Schedule Availability, etc.), and the ability of the proctor to control and manage the exam (start, pause, cancel, and end the exam). Secondly, authentication, which type of authentication is covered by the e-proctoring system, is it continuous, intermittent, or just needed at the beginning of the test? Thirdly, lockdown feature, many e-proctoring systems provide a “lockdown” program due to its efficiency, but the functions performed by this program differ from one proctoring system to another depending on what the lockdown means for the system. In several systems, the lockdown program locks the Internet browser of the user's device and does not allow him to browse the Internet, and hence does not allow him to obtain information from other Internet resources. Some systems use a lockdown program that completely controls the student's device and prevents him from using many operating system features like keyboard shortcuts (such as Ctrl+c, Ctrl+v, PrtSc, on Windows O.S), as well as, preventing him from adding peripheral devices by taking the control over all ports of the device. Fourthly, notifications (created during the exam session), which present the examinee`s activities to the human proctors (Hussein et al., 2020). *Table 1* summarizes the features of some of the existing e-proctoring systems (blank cell means that the information about a particular feature has been not gathered).

***Table 1**.Features of some proctoring systems.*

Proctoring features	Proctor U	Respondus	Proctori	AIProctor	Kryterion	Software secure	B Virtual
Live proctors	✓	×	×	×	✓	×	✓
Scheduling	✓	✓	×	✓	✓	✓	
Training	✓	×	✓	✓	✓	✓	✓
Encryption	✓	✓	✓	✓	✓	✓	✓
Continuous Internet required	✓	✓	✓	✓	✓	×	✓
Certification	✓	×	✓	✓	✓		✓
Automated proctoring	×	✓	✓	×	✓	×	×
Recorded proctoring	×	✓	✓	×	✓	✓	
Audio recording	×	×	✓	×	✓	×	×
Proctor can view student screen	✓	×	✓	✓	×	×	✓
Prevent proctor to view examinee screen	×	✓		×	✓		×
Pause, stop, or cancel test	×	×	✓	×	✓	×	×
Interaction with examinees	✓	×	✓	✓	✓	×	✓
Instructions are given live	✓	×	✓	×	✓	×	✓
Messaging for emergency	✓	×	✓	×	✓	×	
Webcam Features							
Webcam needed	✓	✓	✓	✓	✓	✓	✓
Panning of room	✓	✓	✓	✓	✓	✓	✓
Authentification options							
User authentication	✓	✓	✓	✓	✓	✓	✓
Login by username/password	✓	✓	×	✓	✓	✓	✓
Is ID of student needed?	✓	✓	✓	✓	✓	×	
keystroke tracking	×	×	✓	×	✓	×	×
Facial biometrics	×	×	✓	×	✓	×	×
Voice biometrics	×	×	✓	×	×	×	×
Fingerprint biometrics	×	×	×	×	×	✓	×
Iris biometrics	×	×	×	×	×	×	×
Lockdown features							
Browser	×	✓	✓	×	✓	✓	×
Disabling copy/paste	×	✓	✓	×	✓	✓	×
Disabling browser control options	×	✓	✓	×	✓		×
Disabling printing	×	✓	✓	×	✓	✓	×
Disabling min/max of windows	×	✓	✓	×	✓		×
Disabling right- click	×	✓	✓	×	✓		×
Desktop/taskbar hiding	×	✓	✓	×	✓		×
Windows and Mac O.S	✓	✓	✓	✓	✓	✓	×
Disallowing applications to be launched	×	✓	✓	×	✓	✓	×
Disallowing applications from running	×	✓	✓	×	✓	✓	×
Navigation is disallowed	×	✓	✓	×	✓	✓	×
Stops simultaneous tests	×	✓	✓	×	✓		×

Source: Hussein et al. (2020); Foster and Layman (2013).

Discussion

The proposed and current existing e-proctoring systems are good and efficient systems for proctoring e-exams, and despite their use of many modern technologies that helped increase their efficiency, they may be vulnerable to security attacks, such as DoS, Phishing, etc. The examinee's side is more vulnerable to security threats and

attacks than the administration and control side of the e-proctoring system, where the user may have a low degree of awareness of security attacks and therefore be exploited by the attackers. Security threats are generally divided into two parts: internal and external. The current systems have been focused on the internal threats (e.g. cheating, impersonation, masquerading, etc.) through the use of restriction programs, camera monitoring, authentication, and encryption methods, but external attacks (e.g. DoS, sniffing, spoofing) are just as important as internal attacks and must be focused and addressed to ensure a robust, reliable, and secure system. Based on the foregoing, a secure and effective e-proctoring system should be proposed against all the aforementioned security threats and attacks.

Conclusion

Professional e-proctoring systems are no less efficient than physical proctoring in traditional exams, and perhaps even superior to them. E-proctoring system must be an integrated system because if any part of its three main parts, is exposed to a specific breach, will lead to the failure of the system as a whole. Despite the use of e-proctoring systems for many techniques that helped improve and increase the efficiency of proctoring, they are not able to overcome all the issues they face, where they can be vulnerable to some security attacks such as DoS, Phishing (password-based systems), Impersonation (systems that do not use biometric authentication), or any other attacks. Automating proctoring by utilizing IoT devices integrated with open-source platform (e.g., Moodle) and AI technologies lead to a robust, safe, and reliable system. The full automated proctoring method is the best one among the proctoring methods, where it consumes less effort and a less human element, and it is also easy to follow the technical and administrative matters of the system, but it may has a high false rejection rate. Finally, from Table I, we can notice that e-proctoring systems have variation in terms of the features and capabilities they provide, and therefore the process of choosing a specific system depends on the nature of the institution's work, where universities need a proctoring system that may differ from the system needed by a marketing training institution.

Acknowledgement

The authors would like to acknowledge the University of Mosul, Computer Engineering Department for their help to accomplish this work.

Conflict of interest

The authors declare that the research was conducted in absence of any conflict of interest.

REFERENCES

[1] Adams, A., Blanford, A. (2003): Security and online learning: To protect and prohibit. – In Usability evaluation of online learning programs, IGI Global 28p.

[2] Aisyah, S., Bandung, Y., Subekti, L.B. (2018): Development of continuous authentication system on android-based online exam application. – In 2018 international conference on information technology systems and innovation (ICITSI) 6p.
[3] Alghamdi, A.A., Alanezi, M.A., Khan, F. (2020): Design and Implementation of a Computer Aided Intelligent Examination System. – International Journal of Emerging Technologies in Learning (IJET) 15(1): 30-44.
[4] Andersen, K., Thorsteinsson, S.E., Thorbergsson, H., Gudmundsson, K.S. (2020): Adapting Engineering Examinations from Paper to Online. – In 2020 IEEE Global Engineering Education Conference (EDUCON), 5p.
[5] Asep, H.S., Bandung, Y. (2019): A design of continuous user verification for online exam proctoring on M-learning. – In 2019 International Conference on Electrical Engineering and Informatics (ICEEI) 6p.
[6] Atoum, Y., Chen, L., Liu, A.X., Hsu, S.D.H., Liu, X. (2017): Automated Online Exam Proctoring. – IEEE Transactions on Multimedia 19(7): 1609-1624.
[7] Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. – In Proceeding of ICERI2014 Conference 7p.
[8] Bawarith, R., Basuhail, A., Fattouh, A., Gamalel-Din, S. (2017): E-exam cheating detection system. – International Journal of Advanced Computer Science and Applications 8(4): 176-181.
[9] Bawarith, R.H. (2017): Student Cheating Detection System in E-exams. – King abdulaziz University-Jeddah 98p.
[10] Butler-Henderson, K., Crawford, J. (2020): A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity. – Computers & Education 159: 12p.
[11] Carrascosa, I.P., Kalutarage, H.K., Huang, Y. (2017): Data analytics and decision support for cybersecurity: trends, methodologies and applications. – Springer 270p.
[12] Cavalcanti, E.R., Pires, C.E., Cavalcanti, E.P., Pires, V.F. (2012): Detection and Evaluation of Cheating on College Exams using Supervised Classification. – Informatics in Education 11(2): 169-190.
[13] Chen, Y., He, W. (2013): Security risks and protection in online learning: A survey. – The International Review of Research in Open and Distributed Learning 14(5): 109-127.
[14] Chua, S.S., Bondad, J.B., Lumapas, Z.R., Garcia, J.D.L. (2019): Online examination system with cheating prevention using question bank randomization and tab locking. – In 2019 4th International Conference on Information Technology (InCIT) 6p.
[15] Clarke, N.L., Furnell, S.M. (2006): Authenticating mobile phone users using keystroke analysis. – International Journal of Information Security 6(1): 1-14.
[16] Exam Online Official Portal (2020): How do online proctored exams work? – Exam Online Official Portal. Retrieved from: https://examonline.in/how-do-online-proctored-exams-work
[17] Fask, A., Englander, F., Wang, Z. (2014): Do online exams facilitate cheating? An experiment designed to separate possible cheating from the effect of the online test taking environment. – Journal of Academic Ethics 12(2): 101-112.
[18] Foster, D. (2013): Security issues in technology-based testing. – In Handbook of test security. – Routledge 45p.
[19] Foster, D., Layman, H. (2013): Online proctoring systems compared. – Caveon Test Security Official Portal 11p.
[20] Furnell, S.M., Karweni, T. (2001): Security issues in online distance learning. – Vine 31(2): 28-35.
[21] Ghizlane, M., Hicham, B., Reda, F.H. (2019): A new model of automatic and continuous online exam monitoring. – In 2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS) 5p.

[22] González-González, C.S., Infante-Moro, A., Infante-Moro, J.C. (2020): Implementation of e-proctoring in online teaching: A study about motivational factors. – Sustainability 12(8): 13p.
[23] He, W. (2012): A review of social media security risks and mitigation techniques. – Journal of Systems and Information Technology 14(2): 171-180.
[24] Huang, R.H., Liu, D.J., Zhu, L.X., Chen, H.Y., Yang, J.F., Tlili, A., Fang, H.G., Wang, S.F. (2020): Personal data and privacy protection in online learning: Guidance for students, teachers and parents. – Beijing: Smart Learning Institute of Beijing Normal University 109p.
[25] Hussein, M.J., Yusuf, J., Deb, A.S., Fong, L., Naidu, S. (2020): An evaluation of online proctoring tools. – Open Praxis 12(4): 509-525.
[26] Cluskey Jr, G.R., Ehlen, C.R., Raiborn, M.H. (2011): Thwarting online exam cheating without proctor supervision. – Journal of Academic and Business Ethics 4(1): 1-7.
[27] Jung, I.Y., Yeom, H.Y. (2009): Enhanced Security for Online Exams Using Group Cryptography. – IEEE Transactions on Education 52(3): 340-349.
[28] Karim, N.A., Shukur, Z. (2015): Review of user authentication methods in online examination. – Asian Journal of Information Technology 14(5): 166-175.
[29] King, C.G., Guyette Jr, R.W., Piotrowski, C. (2009): Online exams and cheating: An empirical analysis of business students' views. – Journal of Educators Online 6(1): 11p.
[30] Korman, M. (2010): Behavioral detection of cheating in online examination. – Lulea University of Technology 110p.
[31] Langenfeld, T. (2020): Internet-Based Proctored Assessment: Security and Fairness Issues. – Educational Measurement: Issues and Practice 39(3): 24-27.
[32] Li, H., Xu, M., Wang, Y., Wei, H., Qu, H. (2021): A visual analytics approach to facilitate the proctoring of online exams. – In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems 17p.
[33] Lorenz, B., Sousa, S., Tomberg, V. (2012): Privacy awareness of students and its impact on online learning participation–a case study. – In IFIP WG 3.4 International Conference on Open and Social Technologies for Networked Learning, Springer, Berlin, Heidelberg 4p.
[34] Lozhkin, S. (2014): Analysis of malware from the MtGox Leak Archive. – Kapersky Official Portal. Retrieved from: https://securelist.com/analysis-of-malware-from-the-mtgox-leak-archive/58553/
[35] Mahoney, K., Cameron, L. (2008): An introduction to learning management systems. – University of Fraser Valley 10p.
[36] Marcialis, G.L., Roli, F., Muntoni, D. (2009): Group-specific face verification using soft biometrics. – Journal of Visual Languages & Computing 20(2): 101-109.
[37] May, M., George, S. (2011): Privacy Concerns in E-learning: Is UsingTracking System a Threat? – International Journal of Information and Education Technology 1(1): 1-8.
[38] Mitra, S., Gofman, M. (2016): Towards greater integrity in online exams. – AMCIS 2016 Proceedings p28.
[39] Mohd Alwi, N.H., Fan, I.S. (2010): E-Learning and Information Security Management. – International Journal for Digital Society 1(2): 148-156.
[40] Muzaffar, A.W., Tahir, M., Anwar, M.W., Chaudry, Q., Mir, S.R., Rasheed, Y. (2021): A systematic review of online exams solutions in e-learning: Techniques, tools, and global adoption. – IEEE Access, 9: 32689-32712.
[41] Ndume, V., Tilya, F.N., Twaakyondo, H. (2008): Challenges of adaptive elearning at higher learning institutions: A case study in Tanzania. – International Journal of Computing and ICT Research 2(1): 47-59.
[42] Nickolova, M., Nickolov, E. (2007): Threat model for user security in e-learning systems. – International Journal Information Technologies and Knowledge 1(1): 341-347.

[43] Oliveira, P.C.D., Cunha, C.J.C.D.A., Nakayama, M.K. (2016): Learning Management Systems (LMS) and e-learning management: an integrative review and research agenda. – JISTEM-Journal of Information Systems and Technology Management 13: 157-180.
[44] Opgen-Rhein, J., Küppers, B., Schroeder, U. (2018): An Application to Discover Cheating in Digital Exams. – In Proceedings of the 18th Koli Calling International Conference on Computing Education Research 5p.
[45] OReilly, G., Creagh, J. (2016): A categorization of online proctoring. In Global Learn. – Association for the Advancement of Computing in Education (AACE) 11p.
[46] Patel, A., Taghavi, M., Júnior, J.C., Latih, R., Zin, A.M. (2012): Safety Measures for Social Computing in Wiki Learning Environment. – International Journal of Information Security and Privacy 6(2): 1-15.
[47] Guo, P. (2008): The research and application of online examination and monitoring system. – In 2008 IEEE International Symposium on IT in Medicine and Education 6p.
[48] Prathish, S., Bijlani, K. (2016): An intelligent system for online exam monitoring. – In 2016 International Conference on Information Science (ICIS) 6p.
[49] Reeves, T.C. (2000): Alternative assessment approaches for online learning environments in higher education. – Journal of Educational Computing Research 23(1): 101-111.
[50] Rjaibi, N., Rabai, L.B.A., Aissa, A.B., Louadi, M. (2012): Cyber security measurement in depth for e-learning systems. – International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) 2(11): 107-120.
[51] Rjaibi, N., Rabai, L.B.A., Ben Aissa, A., Mili, A. (2013): Mean Failure Cost as a Measurable Value and Evidence of Cybersecurity: E-Learning Case Study. – International Journal of Secure Software Engineering 4(3): 64-81.
[52] Rogers, C.F. (2006): Faculty perceptions about e-cheating during online testing. – Journal of Computing Sciences in Colleges 22(2): 206-212.
[53] Rosen, W.A., Carr, M.E. (2013): An autonomous articulating desktop robot for proctoring remote online examinations. – In 2013 IEEE Frontiers in Education Conference (FIE) 5p.
[54] Rowe, N.C. (2004): Cheating in online student assessment: Beyond plagiarism. – Online Journal of Distance Learning Administration 7(2): 1-10.
[55] Sarrayrih, M.A., Ilyas, M. (2013): Challenges of online exam, performances and problems for online university exam. – International Journal of Computer Science Issues (IJCSI) 10(1): 439-443.
[56] Sinha, P., Yadav, A. (2020): Remote proctored theory and objective online examination. – International Journal of Advanced Networking and Applications 11(6): 4494-4500.
[57] Slusky, L. (2020): Cybersecurity of online proctoring systems. – Journal of International Technology and Information Management 29(1): 56-83.
[58] Smiley, G. (2013): Investigating the role of multibiometric authentication on professional certification E-Examination. – Nova Southeastern University 325p.
[59] Tashu, T.M., Esclamado, J.P., Horvath, T. (2019): Intelligent on-line exam management and evaluation system. – In International Conference on Intelligent Tutoring Systems, Springer, Cham 7p.
[60] Traoré, I., Nakkabi, Y., Saad, S., Sayed, B., Ardigo, J.D., de Faria Quinan, P.M. (2017): Ensuring Online Exam Integrity Through Continuous Biometric Authentication. – In I. Traoré, A. Awad, & I. Woungang (Eds.), Information Security Practices, Springer International Publishing 9p.
[61] Turnbull, D., Chugh, R., Luck, J. (2019): Learning management systems: An overview. – Encyclopedia of Education and Information Technologies, Springer 10: 978-983.
[62] Ullah, A., Xiao, H., Barker, T. (2016): A classification of threats to remote online examinations. – In 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) 7p.

[63] Underwood, J., Szabo, A. (2003): Academic offences and e-learning: Individual propensities in cheating: Academic offences and e-learning. – British Journal of Educational Technology 34(4): 467-477.
[64] Wahid, A., Sengoku, Y., Mambo, M. (2015): Toward constructing a secure online examination system. – In Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication 8p.