Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 8, No. 4, December 2022, pp. 634-648
ISSN: 2338-3070, DOI: 10.26555/jiteki.v8i4.25094

Cheating Prevention in E-proctoring Systems Using Secure Exam Browsers: A Case Study

Hussein M. Mohammed, Qutaiba I. Ali
Department of Computer Engineering, College of Engineering, University of Mosul, Mosul 41002, Iraq

ARTICLE INFO

Article history:

Received October 24, 2022
Revised December 09, 2022
Published December 28, 2022

Keywords:

E-proctoring;
Cheating;
Moodle;
SEB Browser;
LD Browser;
Threats

ABSTRACT

In this research, a case study has been conducted to analyze the possibility of preventing cheating or reducing it by using one of the lockdown browsers during the exam. An e-exam has been created using Moodle platform, and the exam has been conducted with the Safe Exam Browser (SEB) as a restriction program at one time and without it at another time, and an analysis has been made of the extent of the possibility of cheating during the exam for both cases. Wireshark and Registry Changes View programs have been used to observe the possibility of opening programs and applications or the ability of the examinee to use Windows tools during the exam. The use of Wireshark and Registry Changes View software showed high effectiveness in analyzing the examinee's device data and identifying the examinee's activity during the electronic exam, to give a clear perception of the possibility of preventing access to resources and applications on the examinee's device. The researchers concluded that the use of lockdown browsers is very necessary to prevent the examinee from accessing the resources on his device, which leads to a significant reduction in cheating during the electronic exam. The research contributions are two, the first one is the use of analyzing programs to observe the examinee`s activity during the exam, and the second one is presenting the lockdown browsers` features.

Corresponding Author:

Hussein M. Mohammed, Department of Computer Engineering, College of Engineering, University of Mosul, Mosul 41002, Iraq
Email: hussein.mahmood@uomosul.edu.iq

1. INTRODUCTION

Remote learning has become a common practice, and it recently has increased usage in educational institutions and replaced a large percentage of traditional classrooms [1]. Online examinations are used to assess the knowledge of students remotely with little or no need for the physical presence of proctors, which invariably implies that online proctoring systems have to be used to conduct these examinations [2]. The pace is accelerating in the use of the electronic exams system instead of the traditional exams for several reasons [3], the most important of which is the urgent need to use this type of exam as a result of certain emergency conditions that prevent the use of the traditional system, as well as the advantages that this system has, which facilitate the examinee to perform the exam easily and smoothly [4]. 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 [5]. Besides, the exponential increase in e-learning has motivated scientists and researchers to devise an effective e-proctoring system that can be administered remotely. Researchers and developers conducted several studies and suggested several ways to improve the performance of the e-proctoring system and reduce potential cheating attempts, like the online webcam-based proctoring (live e-proctoring) [6], the biometrics-based proctoring that authenticates students depending on their biometrics and monitoring students' activities such as head and eye movements or mouse movements during the examination session, and some of these studies proposed to combine several methods to obtain an integrated e-proctoring system.

However, there are still obstacles and challenges facing researchers in this field, and the working is still underway to develop the electronic exam system in order to overcome these obstacles and challenges, among these obstacles: potential cheating methods that can be applied in the electronic exams system more than in the traditional exams system. Researchers and developers touched on several methods to control or reduce cheating methods that are potentially used in electronic exams [7], where certain programs or special devices have to be used which cannot be tampered with, these devices are configured and prepared specifically for conducting the electronic exams and the examinees will be forced to take the exam only through these devices. The researchers also suggested using additional devices [8] that help in monitoring electronic exams, such as cameras which are placed in a certain way through which the examinee is monitored and the exam session is recorded for later review. In this research, the performance of the e-proctoring system based on Safe Exam Browser (SEB) integrated with Moodle server as a condition to perform the exam will be studied. The system will be examined against possible cheating methods with a review of the capabilities available in this system, and the results will be presented. E-proctoring systems in general have one working principle, which is to monitor the examinee and provide an exam environment that is close to the traditional exam system, the aim of which is to conduct the exam smoothly and prevent cheating without any problems. But each of the e-proctoring systems proposed in the academic studies or even the existing commercial systems has its features, and each has its advantages and disadvantages and a specific field of work in which it operates [9], [10].

The goal of this work is to describe how lockdown browsers are useful and important to prevent the examinee from accessing the resources on the Internet and that stored on his device and thus preventing the possibility of cheating through the examinee's device during the exam session. The related work from the past research is as follow. Reference [11] discussed the e-examination systems from the pedagogical point of view, performing a systematic review on the topic to present the challenges and opportunities. Their study investigated thirty-six papers and focused on nine key themes: students' perceptions, students' performance, anxiety, cheating, staff perceptions, authentication and security, interface design, and technology issues. Similarly, Ref. [12] carried out a study on e-proctoring systems and the motivational factors responsible for the transitioning from traditional examinations to online examinations. The authors studied many factors which are considered the most motivational factors. These include quality management, external conditioning, available information, attitude and intention, trust, perceived compatibility and perceived usefulness. Their study revealed that the trust factor (which represents security and privacy) is the most decisive factor among other factors in online proctoring. The fuzzy cognitive maps (FCMs) method was used to analyze the obtained information from reviewers.

A qualitative survey design was employed in [13], where several methods were used to assess final examination for students` perceptions with the use of Android-based Exam Browser as a medium for electronic exams. A questionnaire, interview, and observation were used to obtain the results. The students gave positive feedback about using this technique in the electronic exams, where 75.8% of the students believed that this technique is a useful, clear, and understandable platform based on the findings of the study.

Ref. [14], stated in this handbook the possible security issues in online examinations and technology-based testing. He mentioned two main categories of security problems as privacy and cheating; and discussed in detail everything related to test theft and cheating. He also suggested some solutions for test fraud on technology-based tests such as protecting test files, downloading only required items, controlling the browser and operating system, and using protective item design features, among others. Similarly, Ref. [15] highlighted security risks in online examinations and suggested solutions to mitigate the risks.

In this paper [16], the authors conducted a comparative study and analysis of some secure browsers that can be used in electronic exams and the advantages they contain, through which a secure and reliable exam environment can be provided. The authors chose the SEB and LDB browsers and made a comparison between them to choose suitable software and tools to create a reliable and secure electronic exam. The authors also mentioned some of the prerequisites and conditions that must be met before starting the exam, including what is related to the examinee's device and the settings that must be included in it, and what is related to the e-proctoring system in general. At the end of the study, the authors mentioned a number of technical problems that face the examinee during the exam, which affect the performance of the system as a whole, and among these problems: Internet interruption during the exam, the intensity of lighting in the examination hall which may lead to not detecting cheating attempts, as well as some hardware problems related to the examinee's device.

A study has been prepared [17] on the Bring-Your-Own-Device (BYOD) scenario, the current trend of performing electronic exams, which is the most successful scenario in electronic exams with large numbers of examinees doing the test simultaneously. This study dealt with the subject from a different point of view, where the researchers addressed 5 ways to hack and cheat when using this scenario, 4 attacks were tested and

confirmed, and the fifth was theoretically proven without being tested. These attacks are Copying contents of USB to hard disk, Virtual machine, USB keyboard hacks, Modifying software, and Cold boot attack. Finally, the researchers presented the ways that can be used to overcome these attacks.

A secure environment has been created in [3] for the electronic exam at Alpen-Adria-Universität Klagenfurt (AAU), where small exam rooms have been established with a LAN network through which the examinees' devices are connected to a Moodle server. The researchers suggested that the examinees' computers be assigned to an operating system that is owned by the exam administration and booted via the LAN network to prevent the examinees from accessing their internal files, as well as preventing them from using some features that are not allowed during the exam. The exam environment to be more secure, the researchers suggested using a firewall to prevent the examinees from accessing external resources, and because SEB Browser is fully supported by Moodle server and has more stringent restrictions to prevent cheating, it was suggested to be the only browser that the examinees used to access the electronic exam page.

This paper is divided into two parts, the first part is concerned with describing the e-proctoring system and defining its parts and components, the types of proctoring for e-exams, and the problems related to this system. The second part of this paper represents a case study of using the SEB browser which prevents cheating partially on the e-proctoring system and restricts the examinee from accessing resources on his device. The browser is pre-configured (seb.config file) by the administrator to lock the device and put it in lockdown mode. The case study included the definition of the SEB Browser, a description of its architecture and its features, and a comparison between it and the Respondus LockDown Browser. To analyze the performance of using this browser, a real exam was conducted on Moodle server, the Moodle quiz was linked with SEB once, and without SEB another time and the results were analyzed through Registry-Changes-View and Wireshark programs.

The research contributions are two, the first one is the use of analyzing programs to observe the examinee`s activity during the exam, and the second one is presenting the lockdown browsers` features.

2. METHODS

Proctoring, also known as invigilation, is the process of supervising people writing an examination or taking a test in order to prevent them from cheating. Hussein et al.[9] 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" (pp. 509). Also, e-proctoring refers to the service that can be managed by a third party and is used to monitor students as they take their examinations in any location of their choice. This monitoring can be live through webcam or technology-based using Artificial Intelligence (AI). Researchers and developers proposed different virtual tools to be used in e-proctoring to monitor students' activities during the assessment session. By developing these virtual tools to overcome vulnerabilities, researchers and developers can ensure integrity and reliability for e-examinations taken by students from anywhere and at any time. This includes some procedures like disabling some properties of the examinees` devices by using restriction programs to prevent cheating, and authenticating examinees to secure and maintain the integrity of the examination [18]. Others defined e-proctoring 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 [19].

2.1. Components of e-proctoring system

E-proctoring systems may differ in their features and characteristics, but they are similar in their general structure and working principle. In Fig. 1, shows the components of the e-proctoring system in general. As shown in Fig. 1, the e-proctoring system consists of three main parts: the Examination Room, the Transmission Medium, and the Administration and Control. The examination room 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 the examination. It is better if the examination devices are mobile, so the students can be free to take the examination from anywhere. Some of the properties of these devices should be disabled before the students take the exam to avoid examination malpractice. To do so, a restriction software must be used, for example, LockDown Browser, where the examinee is restricted and has no way to exit/return, use keyboard shortcuts or manipulate the system. However, some examinations might require internet access to specific websites, the e-mail or chat functions; therefore, the setting and configuration of Lockdown Browsers should be updated for every exam [8]. Monitoring tools are either integrated with the examination's device or stand-alone as separate devices. These devices monitor the students during the examination session, so the proctor can indicate if there are suspicious activities [20].

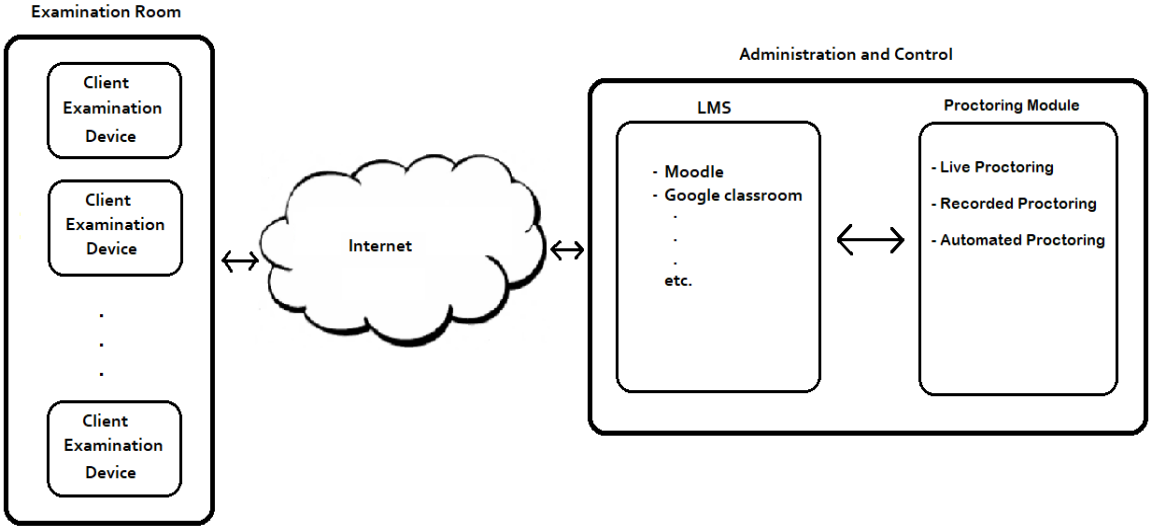

Fig. 1. The components of the e-proctoring system

The administration and control part 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) [21]. 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 [22], 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 [23]. 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:

- Offering certification by providing a place online for instructors to conduct courses and assessment tasks, like assignments and pop quizzes, which allows students or learners to access these courses and assessment activities.
- Capability for event scheduling and content management through a specific training system.
- Providing course improvements as well as technical support.
- Providing centralization to access content for all learners and instructors, as well as course creators to easily and securely complete tasks.
- Making the learning process more interactive for both learners and instructors through live classroom, webinar environments and client presentations.
- The ability to automatically correct exam questions and give the score immediately.

2.2. Issues related to e-proctoring system

Online examinations 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 examination systems are at the same level as that of its importance. Usually, e-learning platforms are used to conduct online examinations. 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 examinations and a reduction in the efficiency of the system [15].

As mentioned earlier, e-proctoring systems consist of multiple processes and functions that work simultaneously to complete the online examination operation perfectly. If we take the authentication process as an example of one of these processes, it is considered a serious challenge to the e-proctoring system [24]. Researchers have further discussed the authentication process and proposed many ideas to mitigate this problem [25], [26]. Likewise, the internet is an ideal environment for cheating in online examinations, as thousands of resources and information can be easily accessed by the examinees.

Furthermore, no one can ensure the availability of the internet to all of the examinees throughout the examination session, as well as in some cases the examinee might need a high-speed connection required for continuous monitoring or for uploading some required files [27]. These are not the only challenges that face online examinations, there are other challenges that the e-proctoring system suffers from, like cybersecurity attacks, threats, privacy, and other issues related to the technical requirements [28]. All the aforementioned problems and issues are discussed in detail in the next subsections.

2.2.1. Cheating

The first major challenge or issue in online examination systems is cheating. This section presents the types of cheating threats in e-proctoring systems and their countermeasures. Cheating depends on circumventing the rules and violating them directly or indirectly, and this is what many students and examinees around the world do [29]. The methods of cheating in e-examinations are not much different from what has been observed in traditional examinations. Some of the traditional cheating methods include writing on pieces of paper, peering into other colleague's answer sheets, writing on pens, rulers, hands, etc. On the other hand, the means of cheating in e-examinations can be through the usage of portable communication devices, hidden Bluetooth headphones, programmable calculators and a lot of modern cheating technologies. Many research papers in the literature discussed the activities of students in terms of cheating and proposed how to eliminate or mitigate these issues [26], [30].

Despite the advantages of e-exams (e.g., saving printing and paperwork, reducing costs and time, etc.), the percentage of cheating is higher in e-exams [26]. In a study conducted by [31], the researchers stated that 52.27% of students thought that there is no difference in the ease of cheating between a traditional exam and an online exam; equally, [32] asserted that it is much harder to prevent cheating in the online environment than in the conventional environment, The results showed that online academic dishonesty was significantly greater among freshmen than graduate students. With the emergence of multiple means of communication 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, copying from other sources, taking the same examination several times or obtaining help from unauthorized sources. There are many forms of online examination cheating [33], which include: impersonations; plagiarism; time breaches; stealing examination questions before or even after the examination; and, a 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-examinations. Some of these tools are webcams, microphones, attached sensors, and so on. The technologies that can also be used to countermeasure cheating include Lockdown Browser, recording windows activities, mouse movements, eye tracking and keyboard shortcuts restrictions (e.g. copy/paste, print screen).

2.2.2. Threats and Attacks

E-examination systems use the internet as the main infrastructure to complete the process of student evaluation [34]. Since the internet is open to everyone around the world, it can contain many forms of security threats [35]. These include masquerading, fraud, malicious software (e.g., viruses, worms, Trojan Horses), spoofing, hacking and 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-examination because they break the Confidentiality, Integrity, Availability and Authentication of the system. Therefore, institutions and universities that use e-examination should 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.

2.3. Implementing E-Proctoring System using SEB

Safe Exam Browser (SEB) is a web browser environment to carry out e-exams safely. It locks down the examinee`s device and turns it temporarily into a secure machine. It can be used by universities and education institutions to control access to resources like websites, system functions and applications. It prevents examinees from using unauthorized resources during an exam [36]. Generally, what makes SEB a good choice for institutions, is that it can work with any web-based LMS and other kinds of web-based exam systems. On the other hand, some learning management systems offer a quiz mode specifically compatible with SEB. SEB provides a safe environment that allows the examinees to attempt their exams on their own

devices. SEB is currently available for Windows, macOS, and iOS users, and it is highly configurable, allowing educational institutions to create an encrypted configuration file which is used to start the exam.

2.3.1. Architecture of SEB

SEB consists of a kiosk application and a browser part as shown in Fig. 2, which are running on the examination device to provide two functions, locking down the device which is applied by the kiosk application, and communicating with the quiz module of an LMS which is done by the browser part. The kiosk application contains a kiosk mode setting called kill explorer shell, this mode of SEB (for Windows) closes or minimizes Microsoft start menu, taskbar and file explorer windows, and all other applications [37].

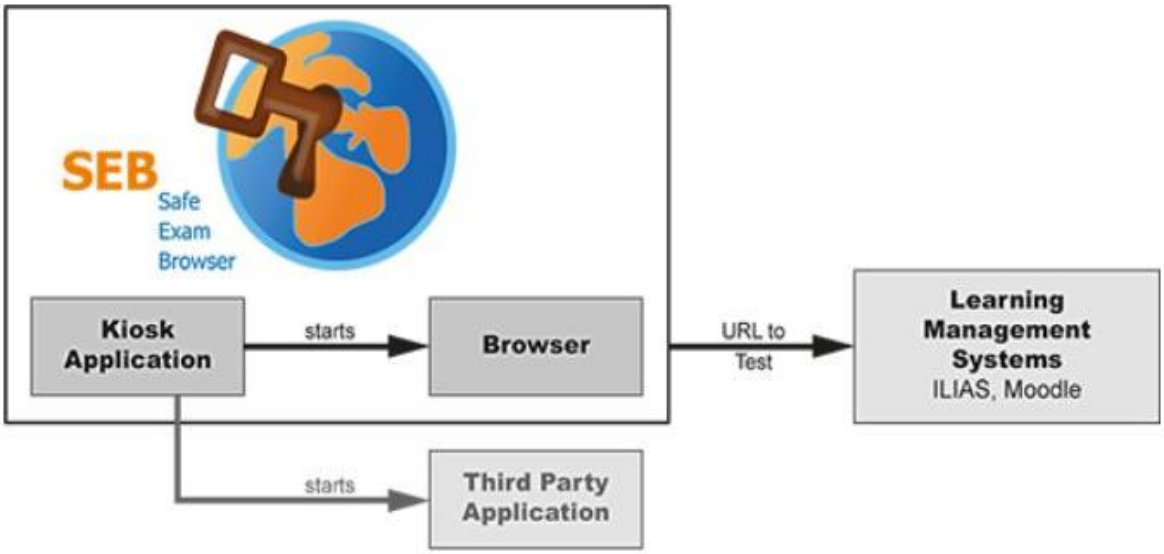

Fig. 2. SEB Browser architecture [36].

2.3.2. Working Principle of SEB

SEB generates an HTTP header called Browser Request Hash and sends it with every request to an LMS to validate that the user is using SEB with the right configuration. Browser Request Hash is generated in two steps, in the first step, SEB generates a Browser Exam Key which is concatenated with the URL of the request, in the second step, the resulted value is hashed using SHA256. The Browser Exam Key is generated by hashing all the files of the current running SEB instance (including its browser components) and then combining that with the SEB configuration file in question. The result is then used to generate a tag using HMAC with SHA256 as the hash function. The Browser Exam Key is shared with any LMS with SEB support before the exam session, and used by the LMS to validate that the user is using SEB. This is done by taking the incoming request URL, concatenated it with the Browser Exam Key (just as SEB does on the client side) and then hashing it with SHA256. Then the generated request hash is checked against the request hash header transmitted from SEB, and if they do not match the request is denied [38].

2.3.3. Integration of SEB with MOODLE

SEB can work with Moodle to provide a safe environment for e-assessments, where the compatibility between them can control the access to the resources during a Moodle quiz attempt. To activate SEB support in Moodle, one of these two options is used, the first one is the built-in support, and when an administration uses it a 'Require Safe Exam Browser' choice appears in the 'Browser security' field on the quiz settings form. The second option needs to Install the 'quiz access rule plugin' in Moodle, this gives more security, and gives you the option to copy/paste the Browser Exam hash Key generated from SEB settings into the quiz settings [39], show in Fig. 3.

Moodle quiz module uses the Browser Exam Key feature to force the examinees to use the right version of SEB to attempt the exam, and to ensure that the examinee is correctly configured for this specific exam. When an e-exam is started in Moodle quiz and the feature of using SEB browser is enabled in the Moodle setting, each HTTP request is checked for the "X-SafeExamBrowser-RequestHash" header through three steps:

i. A SHA256 hash value from the requested absolute URL concatenated with each one of the hash keys 'Browser Exam Key' entered in the quiz settings will be created.
ii. The hash values resulting in step i are compared with the received value with the "X-SafeExamBrowser-RequestHash" header. If one matches, the request will be continued processing.
iii. If none matches, an error message will be displayed and the exam is not started. If the exam was already running, all results entered until now will be saved, the exam will be stopped, and the user will be notified. Otherwise, the exam will be continued till the user finishes his exam, then the result will be saved and the exam will be stopped. In Fig. 4, shows the flowchart of the process of Browser Exam Key checking in Moodle.

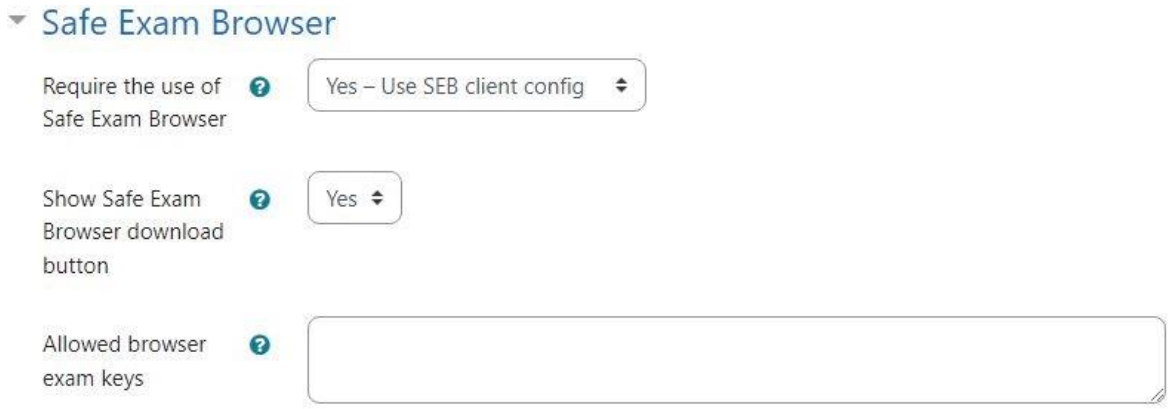

Fig. 3. Integration of Safe Exam Browser in Moodle settings

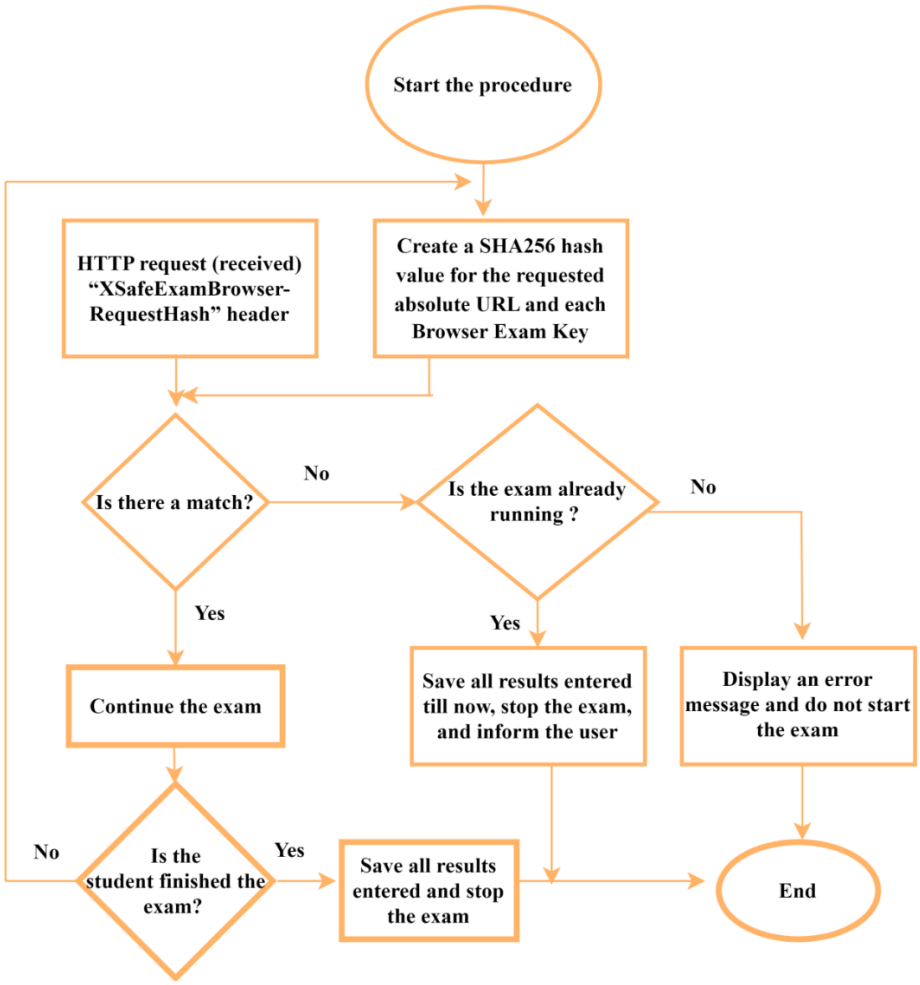

Fig. 4. Flowchart of checking the Browser Exam Key in Moodle

2.3.4. Features of SEB

As mentioned earlier SEB can work with Windows, macOS, and Ios operating systems. Here are the general features of SEB for Windows. SEB for Windows has been chosen because most of the clients' devices work with Windows as an O.S.

- The following actions are disabled if the default settings are used: Windows taskbar and the start menu, switching to other applications, print-screen, and some other keyboard shortcuts like ALT+F4.
- Not allowed processes will be hidden or terminated while SEB is running.
- Third-party applications can be allowed to run together with SEB.
- Spell-checking and dictionaries can be disabled.

Here are some SEB features when integrated with Moodle:

- Students will only be able to attempt the quiz if they are using SEB.
- The browser window won't have a URL or search field and back/forward navigation and reload can be disabled.
- SEB cannot be closed until the test is submitted.
- The clipboard is cleared when starting and quitting SEB Browser.
- The browser context menu is disabled.

2.3.5. SEB vs Respondus LockDown Browser

Lock Down Browser (LD Browser) is a custom browser that locks down the testing environment within a learning management system [40]. As SEB, LD Browser locks down the student`s device and restricts it from using unauthorized resources and functions.

Here are some basic exploits possible with not strongly secured browsers :

- Remote desktop and screen-share.
- Undesirable applications running in the background (e.g screen recording, instant messages).
- Exploits related to VM and Safe Mode.
- Programmable and extended mouse buttons.
- Browser cache and JavaScript injection exploits.
- Task switching swipes.

In Table 1, presents a comparison between SEB and Respondus LD Browser to show their strengths and weaknesses against cheating, these two browsers were chosen as they are the most used in the proctoring systems of e-exams.

Table 1. A comparison between SEB and Respondus LD Browser.

Feature	SEB	Respondus LD Browser
Full-screen mode	Yes	Yes
Disallowing opening a new tab or another website	Yes	Yes
Keyboard shortcuts and keystroke combinations	Can be disabled	Can be disabled
Mouse menus (e.g. printing, copy/paste, task switching).	Can be disabled	Can be disabled
Open source	Yes	No
Native application.	Yes	Yes
Automated proctoring.	No	Yes, using Respondus Monitor app.
Data encryption	Yes	Yes
Integration with Moodle LMS	Yes	No, needs Moodle Extension
Screen recording by student	Can be disabled	Can be disabled
Support for live-remote proctoring	No	Yes, via Zoom and Jitsi Meet
Remote desktop app.	Denied with version 3.1.1 and higher	Denied
VM detection	Yes	Yes
Purchase fee	Free	Depending on the volume

3. EXPERIMENTAL RESULTS

An accurate Moodle quiz with various types of questions (MCQ, short answer questions, essay questions) was conducted using the SEB 3.3.2 browser integrated with Moodle 4.1 LMS, where all the violations that the examinee could make during the exam were tested [26], [37], [41], including attempting the exam outside of the SEB browser, changing settings of SEB, using keyboard shortcuts, screenshot

captures, trying to record screen to store questions, right-clicking the mouse, using processes invoked by Ctrl+Alt+Del, trying to reattempt the exam, trying to reattempt the exam from another device.

The above cheating types are related to the examinee`s device only, however, there are other types of cheating related to cheating outside the examinee`s device like using a cell phone, another laptop, existing of another person in the examination room, or even using a hardcopy of notes to cheat from them, these types of cheating will be discussed in future work.

To check the performance work of SEB in the e-exams, an actual exam was conducted using SEB with Moodle Learning Management System and some tests were conducted on the system to simulate possible cheating attempts during the exam. Moodle 4.1 was installed on the Windows 10 operating system and some auxiliary files were installed to make the system work as a server (Apache/2.4.41, OpenSSL/ 1.1.1c, PHP/7.3.11), SEB browser also has been installed and configured on the Windows 10 operating system in the client machine so that the exam can be conducted remotely through it. A Moodle quiz was created consisting of a variety of questions, which included (4 MCQs, 2 short answer questions, and 1 Essay question) in the field of computer networks, show in Fig. 5. A small W.LAN network was made and the IP addresses were: 192.168.0.110 for the server and 192.168.0.113 for the client. A demo course has been created to add a Moodle quiz, and users have been added to this course to enable them to take the test. The Registry-Changes-View program was installed on the examination device to check and follow the examinee's activities during the exam session.

The following steps have been followed:

1. Attempting the exam without using the SEB browser: where the examinees were not restricted to taking the exam through the SEB browser, and they were given the freedom to take the exam from any browser, as a result, the following cases were recorded:
   a. The examinee has been able to access the device's internal resources as shown in the registry changes view program in Fig. 6. The date and time of the exam as shown in Fig. 8.
   b. He has been able to use keyboard shortcuts (such as Alt+Ctrl+Del, PrtSec, etc.) in addition to using copy/paste, as shown Fig. 7.
   c. He has been able to use a screen recording program to record the full exam session as shown in Fig. 8.
   d. He has been able to use the Wireshark program to analyze network traffic.

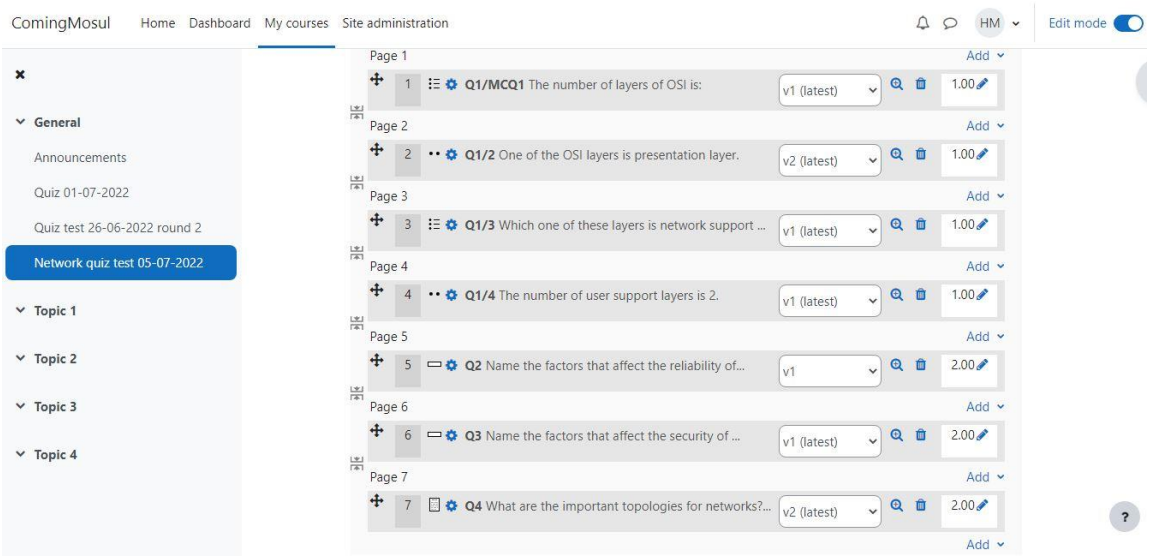

Fig. 5. Moodle quiz questions

2. Attempting the exam through the SEB browser: where the examinees were restricted to taking the exam only through the SEB browser, this is configured in the Moodle quiz setting, with a specific Browser Exam Key, and the following cases were recorded:
   a. SEB browser has been opened with a full-screen mode and Minimizing/Maximizing feature is prohibited.
   b. The examinees tried to access the exam from a browser other than the SEB, but they were prevented from doing so. The examinees tried to change the SEB settings and access the exam, but they were also prevented from doing so as shown Fig. 9.

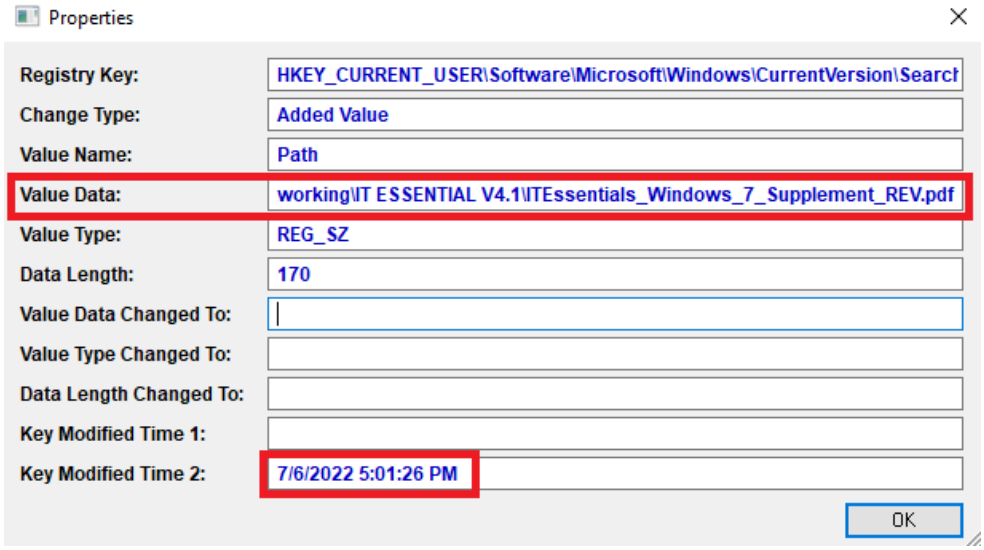

Fig. 6. Opening a pdf file activity during exam session

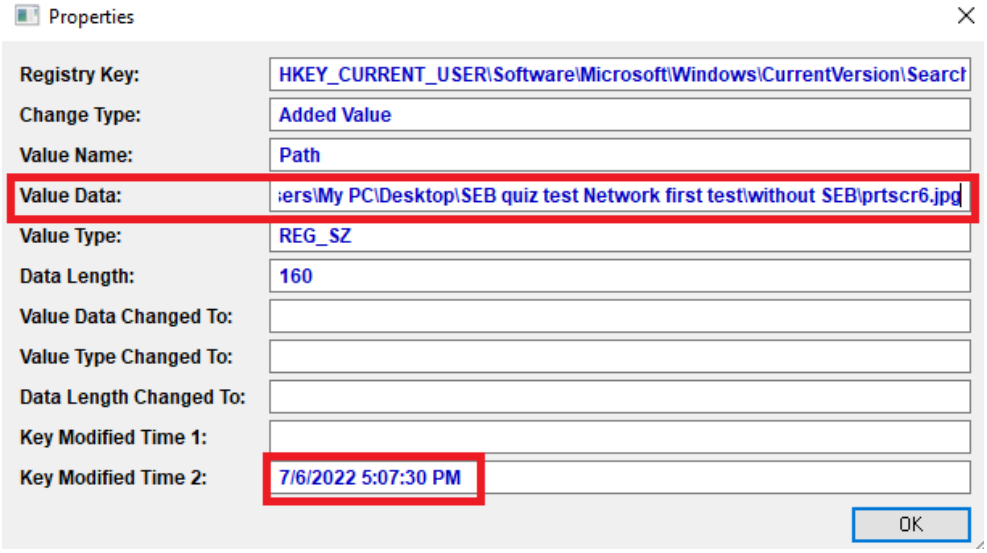

Fig. 7. Print screen activity during the exam session

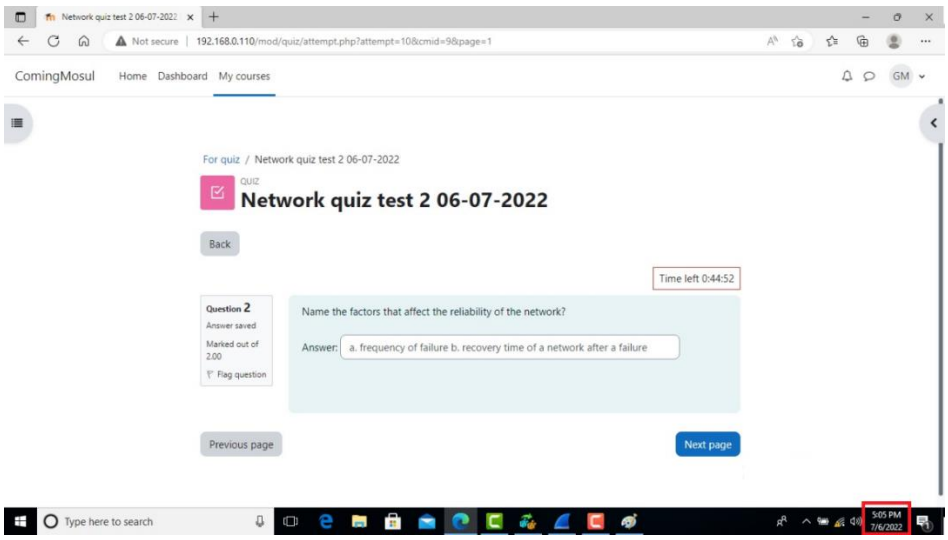

Fig. 8. Users can open any program and access resources during test attempting without SEB

Note: The figures (pictures) may be unclear, where they are taken by a Huawei phone camera because the print screen feature is not allowed while using the SEB browser.

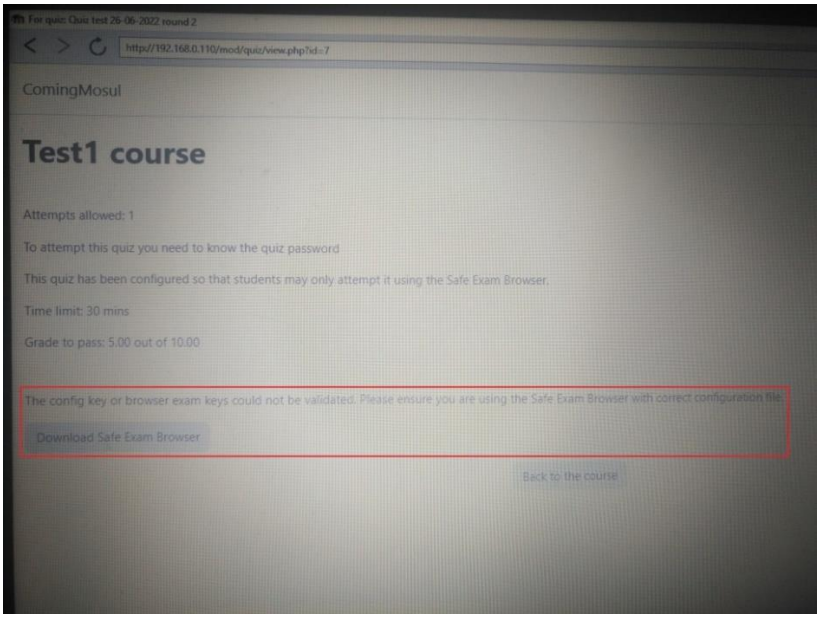

Fig. 9. Test attempt is allowed only using SEB with correct configuration

c. The examinees tried to record the exam session by using the Camtasia program, but they were prevented from using this program, a popup window appeared to inform the examinee that this program is disallowed from working during the exam, and the program will be closed, can be seen in Fig. 10.
d. The Wireshark program was also prevented from working during the exam, where the administrator added this program to the prohibited programs list.
e. All the keyboard shortcuts were prohibited, so the examinee was prevented from using them.

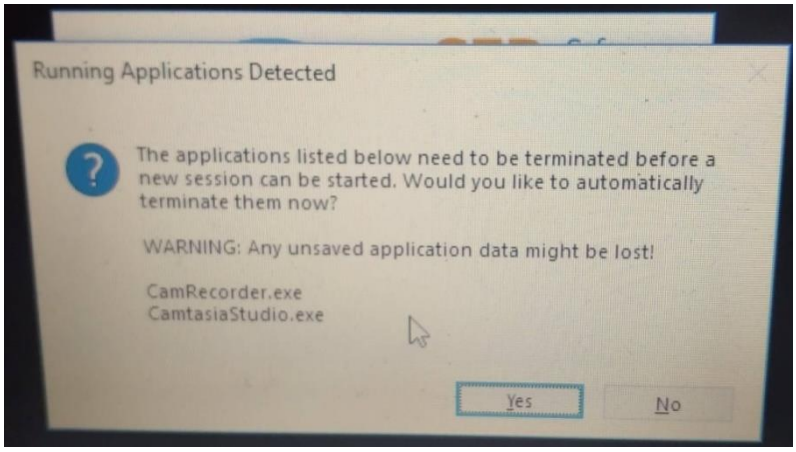

Fig. 10. Prohibited programs are terminated

3. Wireshark was allowed to run during the exam in order to more accurately understand the functioning of the SEB browser. The following notes were recorded:
   a. In every "HTTP" packet that is sent from the client to the server, the "Request-Hash-Value" is included in the packet, to be compared with the Hash-Value of the received one to indicate if the packet was sent from a legal SEB or not, can be seen in Fig. 11.
   b. Moodle-session value is sent in each HTTP packet, this value is the same for all packets in one exam session, to indicate that this packet is for the same exam session to overcome Replay Attack, can be seen in Fig. 12.

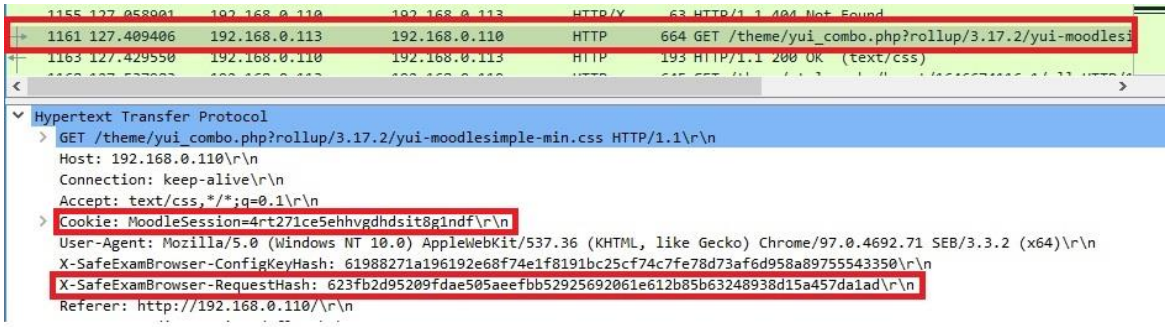

Fig. 11. HTTP packet with request hash value

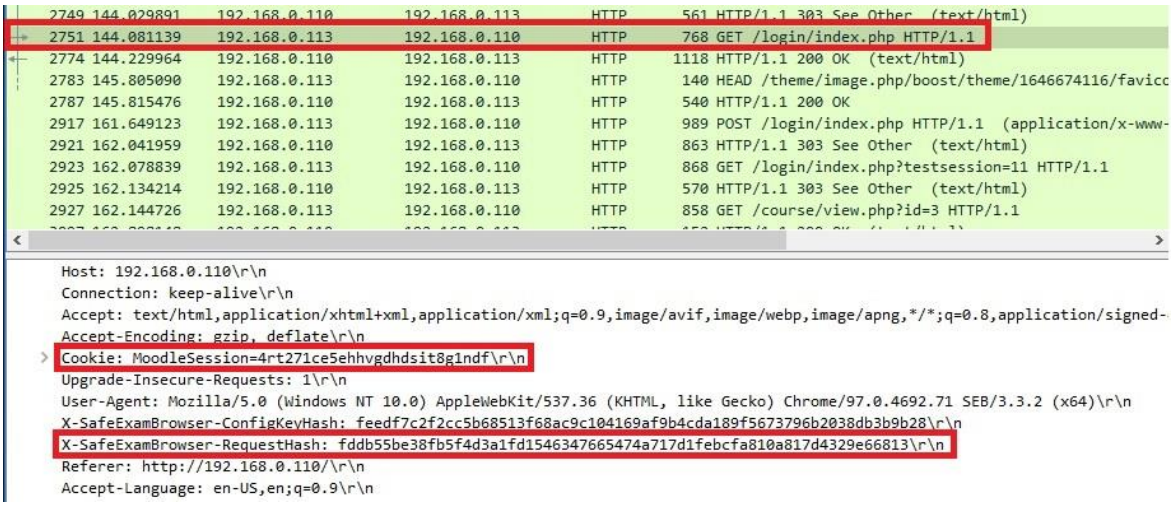

Fig. 12. HTTP packet with Moodle session value

In Table 2 summarizes the cheating attempts that the examinees tried to do during the exam session, the response with and without SEB browser, and if the attempt failed or succeeded.

3.1. Comparison with a similar work

Compared to previous works, we find that restriction browsers are very important programs for creating any safe and reliable electronic exam system, where in reference [16], the researchers at Trakia University made a study to analyze the use of restriction browsers in e-exams by creating an e-exam system using these browsers as a case study. In Table 3 shows a comparison between the research of Karabaliev et al. and our research.

Table 2. The response of cheating attempts in e-exams with and without SEB browser

Cheating attempt	Definition	Steps	Response without SEB	Response with SEB	Countermeasure	Fail/ Success
Unauthorized resources	Internal files and documents saved on the examinee`s device	The examinee tries to open files and documents to cheat	The examinee could to access internal files and pdf`s	Unauthorized resources have been prevented	SEB uses the kiosk application which locks down the device	Failed when SEB browser is used
Unauthorized programs	Like chatting programs, Some mathematics, and statistical programs	The examinee tries to open some programs to help solve the questions	Yes, he can open any program and software	Terminated by SEB browser	SEB uses the kiosk application which locks down the device	Failed with SEB
Screen recording and Wireshark programs	Programs that record exam sessions to leak the questions, and network traffic analytical programs	The examinee tries to run screen recording software like Camtasia to get a copy of the exam questions	Yes he can use these programs	Terminated by SEB browser	The administrator can add any program or software to the prohibited program`s list	Failed with SEB

Cheating attempt	Definition	Steps	Response without SEB	Response with SEB	Countermeasure	Fail/ Success
Attempting the exam from unauthorized devices	The examinee can attempt the exam from any device he wants, which may be an uncontrolled device	The examinee pretending to attempt the exam from a controlled device but he uses another device	Allowed	Not allowed	The administrator restricts the examine to use the controlled device with the legal configurations	Failed
Ending the exam without confirming	The examinee can end the exam Incorrectly or unintentionally	The examinee ends the exam session and then he claims that he did not do that.	Allowed	Password is needed to confirm ending the exam	The administrator restricts the examinee to enter the password	Failed
Keyboard shortcuts & mouse right click	The examinee can use keyboard shortcuts and mouse right click to perform copy/ paste or other cheating tools	The use of these features can help the examinee to open some windows features like task manager	Allowed	Not allowed	SEB uses the kiosk application which locks down the device	Failed
Print screen	The examinee tries to print the exam screen to leak the questions to another person	This cheating attempt can help the examinee to get a copy of the questions	Allowed	Not allowed	SEB uses the kiosk application which locks down the device	Failed
Minimizing exam`s window	The examinee tries to minimize the window to open another app. or another web browser	This cheating attempt can help the examinee to open another app. or web browser	Allowed	Not allowed	Setting the SEB browser on full- screen mode	Failed
Virtual machine	Using a virtual machine to attempt the exam, so the examinee can open other web browsers and access unauthorized resources and programs	The examinee installs a V.Box and attempts the exam inside it, so he can cheat.	Allowed	SEB Browser detects virtual machines	The administrator enables detecting virtual machine in the SEB configuration file	Failed
Remote desktop	The examinee can attempt the exam from another device, so he can open other web browsers and access unauthorized resources	The examinee can follow some steps to enable this feature.	Allowed	SEB Browser prevents remote desktop properties	The administrator enables detecting remote desktop in the SEB configuration file	Failed

Table 3. A comparison with a similar work

	Karabaliev et al. [16]	Our work
Contents	An analysis study of some software tools, and a comparison between restriction browsers such as SEB and LDB, creating a secure and reliable e-exam at TRU University, a case study.	Using restriction browsers to prevent cheating, studying and analyzing the examinee's device performance during the exam to find out the possibility of accessing the resources, and analyzing the examinee's activity on the device using Wireshark and RCV programs. Use of SEB browser and the Moodle platform, a case study.
Outcomes	The study showed that SEB and LDB browsers effectively prevent the examinee from accessing the resources. Recommendations were made for creating a secure and robust electronic test.	The study showed that SEB browser effectively prevents the examinee from accessing the resources. The system has been exposed to real cheating attempts and proved effective in preventing them.
Advantages	It helps to understand the loopholes that can be exploited to prevent accessing resources during the exam.	It helps to understand how restriction browsers (SEB, LDB) work, in addition to understanding how to create a secure and reliable online exam and integrate it with the Moodle platform
Drawbacks	The research is not supported by working steps that show the ability of restriction browsers to prevent cheating and their response to real cheating attempts.	The research discussed cases of fraud related to accessing resources through the examinee's device and did not discuss other cases of fraud such as impersonation

4. CONCLUSION

Professional e-proctoring systems are no less effective than physical proctoring in traditional exams, and perhaps even inferior to traditional physical proctoring. An e-proctoring system must be an integrated system because if any part of its three main parts is exposed to a specific breach; it will lead to the failure of

the system as a whole. The e-proctoring system based on SEB browser and Moodle server only can be considered a good system and can be used in some cases, but since the e-proctoring system is an integrated system and does not accept weakness at any point, it needs additional measures to overcome its weaknesses and thus can be relied upon at a high rate, and among these procedures: adding surveillance cameras to the system through which manual authentication is done, instructions to the examinees are streamed, preventing the examinees from communicating with any person or using other devices. There is compatibility between the SEB browser and the Moodle server through which a secure exam environment can be provided, and there is also compatibility between the SEB browser and Google Meet which can be used to communicate with the examinees during the exam session. SEB Browser works with several operating systems, like Windows, macO.S, and iOS, and the features in these systems can be used to provide a more suitable exam environment for examinees. The future research is cheating detection in online exams using AI technologies with wearable IoT devices.

REFERENCES

[1] H. M. Alessio, N. J. Malay, K. Maurer, A. J. Bailer and B. Rubin, "Examining the Effect of Proctoring on Online Test Scores," *Online Learning*, vol. 21, no. 1, 2017, https://doi.org/10.24059/olj.v21i1.885.

[2] A. A. Alghamdi, M. A. Alanezi and F. Khan, "Design and Implementation of a Computer Aided Intelligent Examination System," *International Journal of Emerging Technologies (IJET)*, vol. 15, no. 01, pp. 30-44, 2020, https://doi.org/10.3991/ijet.v15i01.11102.

[3] G. Frankl, P. Schartner, and D. Jost, "The 'Secure Exam Environment': E-Testing with Students' Own Devices," In *IFIP World Conference on Computers in Education*, pp. 179–188, 2017, https://doi.org/10.1007/978-3-319-74310-3_20.

[4] S. Khan and R. A. Khan, "Online assessments: Exploring perspectives of university students," *Education and Information Technologies*, vol. 24, no. 1, pp. 661–677, 2019, https://doi.org/10.1007/s10639-018-9797-0.

[5] H. Li, M. Xu, Y. Wang, H. Wei and H. Qu, "A Visual Analytics Approach to Facilitate the Proctoring of Online Exams," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–17, 2021, https://doi.org/10.1145/3411764.3445294.

[6] A. Jadi, "New Detection Cheating Method of Online-Exams during COVID-19 Pandemic," *International Journal of Computer Science & Network Security*, vol. 21, no. 4, pp. 123–130, 2021, https://doi.org/10.22937/IJCSNS.2021.21.4.17.

[7] O. Kurniawan, N. T. S. Lee and C. M. Poskitt, "Securing Bring-Your-Own-Device (BYOD) Programming Exams," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, pp. 880–886, 2020, https://doi.org/10.1145/3328778.3366907.

[8] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu and X. Liu, "Automated Online Exam Proctoring," in *IEEE Transactions on Multimedia*, vol. 19, no. 7, pp. 1609–1624, 2017, https://doi.org/10.1109/TMM.2017.2656064.

[9] M. J. Hussein, J. Yusuf, A. S. Deb, L. Fong and S. Naidu, "An Evaluation of Online Proctoring Tools," *Open Praxis*, vol. 12, no. 4, pp. 509-525, 2020, http://doi.org/10.5944/openpraxis.12.4.1113.

[10] H. Mohammed and Q. Ali, "E-Proctoring Systems: A Review on Designing Techniques, Features and Abilities Against Threats and Attacks," *Quantum Journal of Engineering, Science and Technology*, vol. 3, no. 2, pp. 14–30, 2022, https://qjoest.com/index.php/qjoest/article/view/66.

[11] K. Butler-Henderson and J. Crawford, "A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity," *Computers & Education*, vol. 159, p. 104024, 2020, https://doi.org/10.1016/j.compedu.2020.104024.

[12] C. S. González-González, A. Infante-Moro and J. C. Infante-Moro, "Implementation of E-Proctoring in Online Teaching: A Study about Motivational Factors," *Sustainability*, vol. 12, no. 8, p. 3488, 2020, https://doi.org/10.3390/su12083488.

[13] P. A. Fegasanti and A. S. Priyatmojo, "Students' perception on the use of android-based exam browser to assess final examination," *ELT Forum: Journal of English Language Teaching*, vol. 9, no. 2, pp. 162-170, 2020, https://doi.org/10.15294/elt.v9i2.40073.

[14] D. Foster, "Security Issues in Technology-Based Testing," in *Handbook of Test Security*, pp. 53-98, 2011, https://doi.org/10.4324/9780203664803.

[15] T. Langenfeld, "Internet-Based Proctored Assessment: Security and Fairness Issues," *Educational Measurement: Issues and Practice*, vol. 39, no. 3, pp. 24–27, 2020, https://doi.org/10.1111/emip.12359.

[16] M. Karabaliev, V. Nedeva, T. Pehlivanova and A. Minchev, "Reliable and secure online exams during the COVID-19 pandemic," in *Proceedings of the 15th International Conference On Virtual Learning*, pp. 326-331, 2020, https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/covidwho-1361039.

[17] P. Dawson, "Five ways to hack and cheat with bring-your-own-device electronic examinations: Five ways to hack and cheat with BYOD e-exams," *British Journal of Educational Technology*, vol. 47, no. 4, pp. 592–600, 2016, https://doi.org/10.1111/bjet.12246.

[18] K. A. D'Souza and D. V. Siegfeldt, "A Conceptual Framework for Detecting Cheating in Online and Take-Home Exams: Conceptual Framework for Detecting Cheating in Exams," *Decision Sciences Journal of Innovative Education*, vol. 15, no. 4, pp. 370–391, 2017, https://doi.org/10.1111/dsji.12140.

[19] "Online Learning Practices & Guides | UTM VOLT." https://olc.utm.my/online-learning-practices-guides/ (accessed Aug. 09, 2022).
[20] S. Prathish, A. N. S., and K. Bijlani, "An intelligent system for online exam monitoring," in *2016 International Conference on Information Science (ICIS)*, pp. 138–143, 2016, https://doi.org/10.1109/INFOSCI.2016.7845315.
[21] D. Turnbull, R. Chugh and J. Luck, "Learning Management Systems: An Overview," in *Encyclopedia of Education and Information Technologies*, pp. 1–7, 2019, https://doi.org/10.1007/978-3-319-60013-0_248-1.
[22] A. Aldiab, H. Chowdhury, A. Kootsookos, F. Alam and H. Allhibi, "Utilization of Learning Management Systems (LMSs) in higher education system: A case review for Saudi Arabia," *Energy Procedia*, vol. 160, pp. 731–737, 2019, https://doi.org/10.1016/j.egypro.2019.02.186.
[23] P. C. de Oliveira, C. J. C. de A. Cunha and M. K. Nakayama, "Learning Management Systems (LMS) and e-learning management: an integrative review and research agenda," *Journal of Information Systems and Technology Management*, vol. 13, no. 2, pp. 157-180, 2015, https://doi.org/10.4301/S1807-17752016000200001
[24] A. Nigam, R. Pasricha, T. Singh and P. Churi, "A Systematic Review on AI-based Proctoring Systems: Past, Present and Future," *Education and Information Technologies*, vol. 26, no. 5, pp. 6421–6445, 2021, https://doi.org/10.1007/s10639-021-10597-x.
[25] S. Aisyah, Y. Bandung and L. B. Subekti, "Development of Continuous Authentication System on Android-Based Online Exam Application," in *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*, pp. 171–176, 2018, https://doi.org/10.1109/ICITSI.2018.8695954.
[26] R. Bawarith, Dr. Abdullah, Dr. Anas, and Prof. Dr., "E-exam Cheating Detection System," *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 8, no. 4, 2017, https://dx.doi.org/10.14569/IJACSA.2017.080425.
[27] A. W. Muzaffar *et al*.,"A Systematic Review of Online Exams Solutions in E-learning: Techniques, Tools and Global Adoption," in *IEEE Access*, vol. 9, pp. 32689-32712, 2021, https://doi.org/10.1109/ACCESS.2021.3060192.
[28] M. Ghizlane, B. Hicham and F. H. Reda, "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)*, pp. 1–5, 2019, https://doi.org/10.1109/SysCoBIoTS48768.2019.9028027.
[29] A. Fask, F. Englander and Z. Wang, "Do Online Exams Facilitate Cheating? An Experiment Designed to Separate Possible Cheating from the Effect of the Online Test Taking Environment," *J. Acad. Ethics*, vol. 12, no. 2, pp. 101–112, 2014, https://doi.org/10.1007/s10805-014-9207-1.
[30] S. S. Chua, J. B. Bondad, Z. R. Lumapas and J. D. L. Garcia, "Online Examination System with Cheating Prevention Using Question Bank Randomization and Tab Locking," in *2019 4th International Conference on Information Technology (InCIT)*, pp. 126–131, 2019, https://doi.org/10.1109/INCIT.2019.8912065.
[31] A. Reedy, D. Pfitzner, L. Rook and L. Ellis, "Responding to the COVID-19 emergency: student and academic staff perceptions of academic integrity in the transition to online exams at three Australian universities," *International Journal for Educational Integrity*, vol. 17, no. 9, 2021, https://doi.org/10.1007/s40979-021-00075-9.
[32] C. Y. Chuang, S. D. Craig and J. Femiani, "Detecting probable cheating during online assessments based on time delay and head pose," *Higher Education Research & Development*, vol. 36, no. 6, pp. 1123–1137, 2017, https://doi.org/10.1080/07294360.2017.1303456.
[33] J. Golden and M. Kohlbeck, "Addressing cheating when using test bank questions in online Classes," *Journal of Accounting Education*, vol. 52, p. 100671, 2020, https://doi.org/10.1016/j.jaccedu.2020.100671.
[34] A. Lambert and P. Etim, "E-examination and academic performance of biology students in Akwa Ibom State College of Education, Afaha Nsit- Nigeria," *Journal of Educational and Learning Studies*, vol. 4, no. 1, 2021, https://doi.org/10.32698/0822.
[35] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors and Microsystems*, vol. 77, p. 103201, 2020, https://doi.org/10.1016/j.micpro.2020.103201.
[36] "Safe Exam Browser – Developer File Format." https://safeexambrowser.org/developer/seb-file-format.html (accessed May 02, 2022).
[37] T. M. Søgaard, "Mitigation of Cheating Threats in Digital BYOD exams," M.Sc. Thesis, Norwegian University of Science and Technology, Norway, 2016. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2410735.
[38] A. Heintz, "Cheating at Digital Exams," M.Sc. Thesis, Norwegian University of Science and Technology, Norway, 2017. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2460113.
[39] "How to Create a Moodle Quiz: Step-by-Step Guide (2022)." https://www.ispringsolutions.com/blog/how-to-create-a-moodle-quiz (accessed May 02, 2022).
[40] "LockDown Browser - Respondus." https://web.respondus.com/he/lockdownbrowser/ (accessed Aug. 12, 2022).
[41] F. Noorbehbahani, A. Mohammadi and M. Aminazadeh, "A systematic review of research on cheating in online exams from 2010 to 2021," *Education and Information Technologies*, vol. 27, pp. 8413–8460, 2022, https://doi.org/10.1007/s10639-022-10927-7.