IJIE (Indonesian Journal of Informatics Education)

Research Paper ISSN: 2549-0389

Secure Remote (Home) Electronic Examination Systems: Features, Challenges, and the Development of an Offline Model

[1*] Clement Amone Keyamo, [2] Onashoga Saidat Adebukola, [3] Abimbola Adebisi Baale
[1] Department of Cyber Security, Dennis Osadabay University, Asaba, Nigeria
[2] Federal University of Agriculture, Abeokuta, Nigeria
[3] Ladoke Akintola University of Technology, Ogbomoso, Nigeria
Corresponding Email: clement.keyamo@dou.edu.ng

Abstract:

The development of e-examination systems that can meet acceptable standards in the education industry is a present focus of researchers in the distance learning area. The majority of researchers focus on centralized e-proctoring schemes that depend massively on state-of the-art internet connectivity. However, many users of these systems, especially in the developing countries, have limited internet services. This is a major barrier to effective remote e-assessment of learners as majority of these solutions fail with failing internet services. This study aims to identify the features and challenges in the existing remote electronic exams schemes and to propose an alternative model that solves the present challenges. Two research questions were proposed to guide the research: 1. What challenges exists in existing remote electronic exam systems that undermine the sanctity of exams? 2. what features are required in a secure remote electronic exam system that guarantees the sanctity of exams and solves the present challenges? Relevant data was gathered using the review of literature and online questionnaire administered to students of the African Center of Excellence on Technology Enhanced Learning . The Findings show that poor internet services compromise the sanctity of remote e-examinations and that most existing e-examination schemes employ technology that are expensive and intrusive. A secure offline continuous authentication Model (SOCAM) was proposed as a panacea for the identified challenges. it was concluded that the proposed model can offer a cheaper and more efficient alternative to other remote e- examination schemes.

Keywords: *Authentication; Cheating; e-Assessment; e-Examination ; e-Learning Online Examinee; Proctor; Security: Remote Exams; Remote Home Exams*

IJIE (Indonesian Journal of Informatics Education)
Vol 8 Issue 1 2024
DOI: http://dx.doi.org/10.20961/ijie.v8i1.87162
Received: 29/05/24 Revised: 04/08/24 Accepted: 14/08/24 Online: 31/07/24

Introduction

Remote Online examination approach is a key beneficiary of the corona virus pandemic of 2019. The isolation of a vast number of the world's population including teachers and their students due to quarantine, hastened large scale acceptance of this assessment approach . However, the approach is still being frowned at by practitioners in the educational sector due to perceived limitations in tackling challenges of cheating, especially in high stakes exams, when compared to traditional pen-on-paper type exams (Ngqondi et al, 2021; Mohammed and ALI, ,2022 ; Noorbehbahani et al, 2022 ; Chan and Ahn 2023) .

Researchers in a bid to tackle this challenge focus on developing remote online examination systems that can meet similar standards as pen-on-paper exams in terms of security during exams. To achieve this, online examination systems that use video monitoring technology and biometric authentication systems with machine learning and other AI techniques, utilized to check cheating during online exams, have been developed (Sabbat, 2017; Zhu, X Cao, C, 2021; Noorbehbahani et al,2022;).

Online remote exam schemes that utilize continuous monitoring of examinees to detect and manage exam frauds have been categorized into the following (Mohammed,2022): human online proctoring, semiautomatic proctoring , fully automated online exam proctoring and recorded proctoring. As an instance, El Sayad et al (2014) proposed the ' Remote Online Examination Model' (ROES) that can remotely authenticate an examinee and detect cheating without regard to an online human proctor. The model combines PKI Algorithm and Digital signature for Initial identification of examinee and fingerprint and keystroke dynamics, for continuous authentication. Continuous monitoring of examinees to detect and counter cheating is provided by Live video/audio surveillance . The overall aim of the model is to provide a secure e-exam infrastructure without the limitation of location and time for examines that accompanies class room based traditional and electronic-based assessment approaches.

Also, Sabbath (2017,2011), proposed two models: the interactive and Secure e-Exam unit(ISEEU) and the Smart Approach for Bimodal Biometric authentication in Home-exams (SABBAH). the ISEEU model is based on video monitoring of examinees with a live human proctor at the other end. Two structures of the ISEEU model has been proposed. One is based on web cam broadcasting live exam sessions from examinee to proctor via a media server, while the other type uses video calls instead of the web cam. In both cases, the proctor monitors all examinees with multiple screens, one for each. Also, the proctor can interact with the examinees via a tool box, while all sessions are recorded for future revision. The second model, SABBAH, is an upgrade based on the ISEEU model. It combines automatic video matching and continuous authentication using fingerprint and keystroke dynamics to prevent impersonation, effectively eliminating the need for a live human proctor.

Furthermore, Rajendra et al (2022), proposed a proctoring system combining human proctors and AI automation support. The proctoring software consists of two major modules. The first module is responsible for activating and controlling the video recording of the examinee, alerting the human proctor if the AI detects scenarios it can interpret as cheating. The second module is the lock down module, responsible for shutting down all features in the examinee's device, effectively preventing the examinee from accessing illegal materials from the device or the internet.

However, the aforementioned solutions that utilize continuous monitoring techniques, mainly depend on the premise that the examinee can guarantee reliable and adequate connectivity over the internet (Ketab, 2017; Muzaffar et al.,2020). Poor internet services in developing countries is noted to be a major barrier for online real-time assessment of students, especially under remote conditions. These solutions, therefore, quickly become inefficient in such areas were there is such limitations in internet services. Solutions such as ROES and SABBAH logout examinees who cannot stay connected to the central server due to unstable connection over the internet and can even stop them from continuing with the exam once they get reconnected, awarding the victims with zero score. Also, most of these solutions introduce additional cost to students and institutions through the introduction of novel technologies that are expensive and often difficult to implement.

This paper reports on the results of the investigation of existing remote electronic examination systems based on review of literature and data gathered from students of the African center of Excellence for Technology Enhanced Learning (ACETEL) via questionnaire survey, and proposes a *Secure Offline Continuous Authentication and Monitoring model (SOCAM) for remote exams that can serve as panacea to the identified challenges.* The following research questions were used to guide the research: 1. What challenges exists in existing remote electronic exam systems that undermine the sanctity of exams? 2. what features are required in a secure remote electronic exam system that guarantees the sanctity of exams and solves the present challenges?

The rest of the paper is structured as follows: Section 2 literature review ; Section 3 describes the research method; section 4 describes the proposed model; and finally section 5 covers the conclusion.

Literature Review

Online examination systems are essentially modules of online learning systems. They can be human-proctored, semi-automated (consisting of a blend of software and human proctoring) or fully automated (Mohammed and Alli, 2020). Also, online examination systems can be classroom based or remote\home-based (El Sayad et al, 2014). Several researchers have proposed diverse online examination solutions to meet the challenges itemized in the previous sections.

Sabbah et al (2012) proposed A proctor based remote e-exam model called 'Interactive and Secure E-Examination Unit (ISEEU)'. The aim of the work was to develop a proctor-based and remote e-assessment or e-examination authentication scheme that enables educational institutions to conduct cheating-free e-examinations.

In this scheme, proctoring is implemented using video recording using a camera settled in front of each student. The examinee is connected to a media server (MS) through the Internet . The MS creates a channel for the examinees to broadcast exam sessions to their proctor through an e-learning server (ELS) with all the video streams appearing on the proctor's terminal (PT).

The proposed system was to guarantee that the the same authenticated student took the exam every moment during the exam. That is the system would guarantee continuous authentication of the examinee.The model was designed to cover not only the CIA goals of security, but also to cover three additional security goals identified specifically for e-examination schemes that include: Presence and continuous authenticated presence(P); Identity (I): that is used to differentiate one examinee from another and; Authentication (A): which is used to prove examinee's declared identity.

To implement the ISEEU model, a prototype using PHP, MySQL and HTML was developed and fused with MOODLE. The system was evaluated in terms of the different types of cheating scenarios and impersonation threats earlier identified by the researchers including : Type A: impersonation ; Type B: which can occur when an examinee passes his clearance data (username and password schemes) to an impostor that writes the exam in his stead; Type C: impostor writes for candidate after candidate logs in (biometric authentication schemes). Previous schemes were then compared with ISEEU model and the researchers identified that, while ISEEU was vulnerable to type A threats only , other schemes lagged behind as, in most cases, they satisfied only one of the threats types to e-exam solutions.

Identified strengths of the ISEEU model include :The model is secure and implements continuous authentication;The presence of a monitoring human proctor makes the system as good as the traditional exam situation.The disadvantages of the model include: the human proctors can be compromised or may not pay adequate attention to the exam; the system is costly as the human proctor(s) still have to be paid and trained; the equipment required to implement the scheme further raises up the cost of the system ; the system relies on continuous video transmission over the internet which calls for huge processing resources and an efficient IT infrastructure, which is not always available, especially in the developing countries, and; usability issues were not addressed as the system focused on security and cheating management.

El Sayad et al. (2014) proposed A New Remote Authentication Model for Online Examination Systems (ROES). The aim of the work was to develop a secure online examination system that can be remotely accessed without examinees being constrained to a fixed exam Venue at the remote location.

The ROES model was an enhancement of the Interactive and Secure E-Examination Unit (ISEEU) model developed by Sabbah et al (2011). Though the researchers did not disclose any specific implementation procedure, they evaluated the proposed model through experimentation. The experiment was carried out using 100 students. Security attacks called cheating scenarios were initiated by the students in three stages covering the three threat regimes common with online exam system; registration process attacks (before an exam), ongoing exam attacks (continuous authentication attacks and monitoring attacks), after exam attacks (privacy of examinee attacks). the ROES Model features was then compared with 3 main existing Systems in the Market as at the research time.

The strengths of the ROES model includes: examinees can take the online exam remotely without regard to the fixed place or time; cost, time, health (in the light of Covid 19) and resources advantages to learners and institutions as it can provide secure, effective online examinations for remote locations; and the identity of examinees are preserved from examiners which can enhance the sanctity of the grading process. The identified weaknesses of the ROES model include unaddressed usability issues and also the system became ineffective in areas were internet speed and connectivity was limited.

Adebayo and Abdulhamid (2016) developed an e-exams system for the Nigerian university, emphasizing security and result integrity in their work. Their declared aim was to developing a new acceptable e-Exam system that takes care of the existing system's challenges and security lapses in the Nigerian Clime detected through their investigation of the existing electronic-examination system in the country. The Classical system design and development methodology was used by the researchers. They first Investigated the existing e-exam systems in six universities in Nigeria using questionnaire and interviews covering key stakeholders (examiners and examinees) to identify key weaknesses in them focusing on security and result integrity. They then proposed an e-exams system that uses biometric fingerprint authentication for user identification and cryptography to protect questions in transit in the internet and intranets. The system was designed using the UML language and implemented using Java Applet, PHP and HTML, with the back end done with MySQL they analyzed the system using a small laboratory containing ten computers and a server was with four different browsers and four different OS. The system is able to secure the questions in transit in remote systems and guarantee one time user authentication. However, the system does not deal with cheating challenges during examinations as the authentication is one time and not continuous authentication during the exam.

Ullah et al (2012) proposed a Profile Based Authentication Framework (PBAF): a multi-modal authentication approach implemented on MOODLE Learning Management System (LMS). A two phase methodology is used. In the first phase, the researchers developed the PBAF method for authenticating students. The PBAF authenticates students during the test stage based on profiles generated during the course stage using stored questions asked while the course was on-going.The second phase involved a quantitative design of research questionnaire and the administration of same to students who partoke in the online course and associated test using the PBAF.

A simulated online learning environment with various graphical password strategies for the evaluation of security and usability of the system was implemented using PHP and MYSQL. A total of 13 and 28 text- based and image-based predefined profile generating questions were built into the system. This was then coupled to MOODLE Learning Management System (LMS).

To evaluate the system, 70 students, were recruited. They were then requested to submit feedback after using the system. The authors claimed overall user satisfaction was positive.

The identified Strengths of the system include Improved usability and memorability over text based authentication schemes during authentication due to efficient graphical password scheme, while the major weakness is distraction concerns raised by the students during the profiling stage. Profile questions interfered with courses during the course presentation phase since they ran concurrently. The system could not be used to examine students independently of the course stage. This means that students who did not take part in the learning part of an institution for example, could not be examined. This may not be appropriate in self learning environment were students may decided to study independent of prepared online modules.

Sabbah (2017) proposed a model called smart approach for bimodal biometric Authentication in home-exams (SABBAH) Model. The aim was to present a secure and smart model for remote or home-based e-examination systems with summative e-assessment capabilities using an authentication approach.

The model utilizes a combination of biometric techniques including keystroke dynamics, fingerprint technology and video matching for continuous authentication and verification of users. The proposed SABBAH model is based on modifications to the ISEEU model by Sabbah et al (2011). To implement the model, AI-based algorithms was used. The developed prototype was then integrated t with Moodle (an open source E-learning platform) using PHP.

Identified strengths inherent in the system include: 1. Fusion of various factors eliminates the limitation of noise from one factor compromising the system security; 2. the multi-level authentication improves the security as one compromised factor does not leave the system without security since the other factors are not compromised; 3. In addition, the system has capacity to authenticate users that don’t have all the requirements but have met minimum requirement. Identified weaknesses in the model are: 1. expensive and difficult to implement due to its complexity; 2. system becomes ineffective in situations were poor internet services prevail.

Jegatha et al (2019) proposed the model ‘Secure online system for e-learning’. The Aim was to develop an e-learning management system that can be accessed from any location and with various devices witch guaranteed security using a simple scheme for mutual authentication between the student and the server and secure delivery of question paper from the server. The above aim was attained using the following objective: 1. Automatic verification of students’ identity by the server; 2. develop a simple authentication dialogue for the process of completing the authentication to be done mutually between the student and the server and; 3. Secure distribution and collection of question papers and answers respectively. The model was not implemented, but elaborately described. The system was evaluate using survey type experimentation. Questionnaires where used to obtain response from students and teachers to evaluate the potential of the proposed system as described. Identified strengths of the proposed model include: Strong authentication of the user before examination and secure transmission of questions and answers between users and server across the internet. However, the proposed model does not proscribe methods to prevent exam malpractice while exam is on-going.

Zhu and and Cao (2021) proposed a secure online examination with biometric authentication and blockchain-based framework. The proposed e-exam framework is aimed at resolving problems of security associated with tempering with stored biometric templates (for authentication of users), access control on examination data including question papers, answers from students, scores from examiners and so on, and dispute resolution when contention arises from a breach in the system. The framework utilizes biometric authentication based on facial recognition, combined with cryptographic methods to form a *fuzzy vault*. The fuzzy vault functions to prevent leakage or hacking of the biometric template. In this framework, data (student answers, instructor questions and scores) are secured using collaborative block-chain technology were data is encrypted and stored in a distributed storage network with the evidence of that data stored in a block-chained network built and owned by several credible institutions that constitute a consortium. The stored evidence in the block-chain can be used for dispute resolution when they arise. Fine-grained access control is used in the framework This is founded on attribute-based encryption were only users having the correct access combination keys can access encrypted data in their plain-text form.

The researchers did not implement the proposed framework but the security of the system was analyzed using 8 security propositions and the proves that they hold. Also the performance of the framework was compared with others based on mathematical modelling of the computational and communication cost of the system performance indices.

Identified strengths of the proposed framework are: 1. Provides for protection of bio-metric template by generating a fuzzy vault that prevents template hacking/tempering; 2. confidentiality of data, fine -grained access control and dispute resolution is guaranteed using block-chain storage of forensic evidence of user data and attribute-based encryption. Inherent weakness of the framework include: 1. framework implementation could b**e** Quite expensive and complex; 2. based on single authentication of user as against continuous authentication and verification that can prevent in-exam cheating.

Ngqondi et al (2021) developed a framework that can be used as a standard guide by South African universities that wish to adopt online examination systems, taking into consideration the South African peculiarities. The aim of the proposed framework was to find a balance in the impact of assessment systems on students and the prevention of academic frauds. Review of literature for the purpose of understanding academic threats, and controls, the understanding of the South African higher educational needs and context, the proposal of an online exam framework based on the research data obtained and proposal of an online exam implementation process, were the objective used to achieve the stated aim. The researchers based their work on the premise of the Socio-technical Theory, which states that an information system problem can be resolved by focusing on the social and technical sub-systems.

The proposed framework was composed of two modules: an authentication and continuous monitoring component that constitute the technical sub-system and; the examination systems enablers, that make up the social component. No implementation of the proposed framework was specified but the researchers proposed implementation steps to guide potential adopters of their framework. Also the researchers analyzed the framework by comparing it with existing systems from survey of literature. Identified strengths include: resolves contextual socio-political challenges in the South African higher educational space by Providing a solution to the problem of balancing massification of education, quality and cost and; applied a Socio-technical approach in resolving security issues in e -assessment systems. This is against the common techno-centric approach. to information systems problems solution. The techno-centric approach, the common approach in the surveyed literature, focuses on technical aspect to the detriment of the very important social aspect of the challenge. However, The framework is based on remote continuous monitoring by virtual or human proctors using biometric technology. Either of these approaches introduces challenge of cost both in human and technological resources, and limits implementation in localities with poor IT infrastructure and internet access.

Rajendra et al (2022) proposed the online exam proctoring system. The overall aim of the research was to develop an online exam proctoring system that can maintain the academic integrity of examinations by providing real- time proctoring that can detect diverse cheating actions of the examinee. The researchers introduce a new approach using 360-degree security camera instead of the traditional webcam. They used artificial intelligence technique for the continuous monitoring module with data feeds from client-audio equipment and 60- degree security camera. The AI based proctoring module consist of two elements: element that activates the camera and captures examinee video for processing of cheating scenarios, and the element that implements lockdown of systems tools that can aid cheating during the exam. The researchers Proposed the implementation of the system using python Language, Flask, MySQL, BOOTSTRAP but did not undertake an analysis of their proposed system. The Strength of the proposed system is that the Combination of lockdown software with video monitoring improves continuous authentication and cheating prevention, while its Weaknesses is that it is Expensive and saddled with implementation complexity.

Research Method

A Rapid Literature Review (Smela et al, 2023), was employed to find answers to tw o guiding questions: 1. What challenges exists in existing remote electronic exam systems that undermine the sanctity of exams? 2. what features are required in a secure remote electronic exam system that guarantees the sanctity of exams and solves the present challenges? Also, the opinion of students of the African Center of Excellence on Technology Enhanced Learning (ACETEL), (an Internationally accredited academic center at the National Open University of Nigeria, NOUN), employing remote learning technology in the training of post graduate students, was sampled to further augment and confirm the findings from the literature review using online mixed type questionnaires. A total of 11 post graduate students (PhD and MSc) partook in the survey (see Figure 1, 2 and 3 for relevant student demographics). The findings from the literature review and questionnaire survey are presented in Result section.

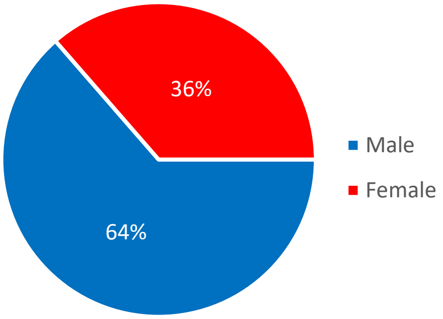

Figure 1. Gender Distribution

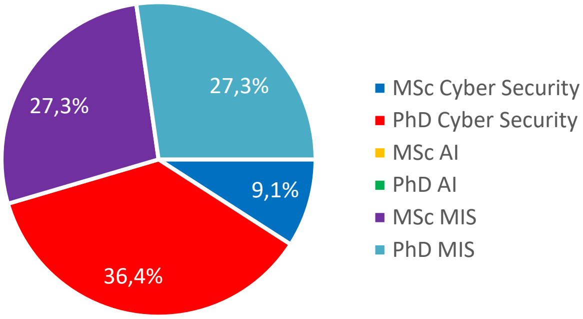

Figure 2. Programme of Study

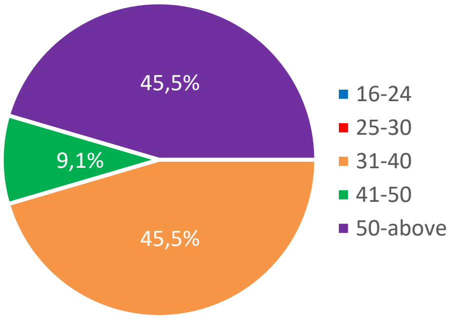

Figure 3. Age Distribution

Findings

This section presents the findings from the literature review and questionnaire survey. The data gathered has enabled the identification of challenges in the state of the art in remote electronic exam schemes and to identify the features required for a secure remote e-exam scheme. The identified features can be adapted to implement an offline remote exam system that resolves the identified challenges. The findings, answering the guiding research questions are in the sub sections below.

What Challenges Exists in Existing Remote Electronic Exam Systems That Undermine the Sanctity of Exams?

It was realized from the review of literature that poor internet services or bandwidth, especially in developing countries, is an important challenge for online or real-time monitoring during the assessment process. Many developed systems for remote assessment of students such as Sabbah (2017) and ROES (2014) fail when internet connectivity is poor. Also, most effective, proposed systems involve additional equipment and cost. Proposed schemes like that by Rajendra et al (2022) require additional equipment (with complex hardware and software requirements) for students that increases the overall cost of acquisition of knowledge. Also, such systems are complex and expensive to implement and manage by institutions.

Another observed challenge that is widespread in the reviewed works is that of intrusion during exams. Most of the designed solutions were intrusive in nature causing students to pause during exams to meet up with exam security demands. For instance, Sabbah (2017) requires examinee to constantly use fingerprint scanners during exams. Most of the schemes emphasized security over intrusion resulting in students being distracted over exams. To ameliorate these challenges, Ketab (2017), recommends that transparent systems that minimize intrusion are required.

Furthermore, from the questionnaire survey, 54% of the students claim that they experienced challenges with their internet services during their exams. The type of challenge experienced by the students include (figure 4): slow speed (80%), intermittent or erratic connection (60%), and complete internet shutdown(10%), while the effect of the internet challenge include (figure 5): difficulty accessing questions (50%), failure to complete exams(40%), distraction (50%), and loose of answers to previously attempted questions (60%). However, only (36.4) claim that the experience affected their overall performance in the exams (figure 6). Another 36.4% of the students stated that they were not sure if their performance was affected, while the remaining 27.3% said their performances were not affected by the internet challenge.

We believe that some students could not claim that their performance was affected by the poor internet service probably due to the excellent challenge redress mechanism put in place by ACETEL authorities. In fact, quite a number of students agreed that their complaints were adequately addressed by the institution, including opportunities to retake exams that experienced such challenges.

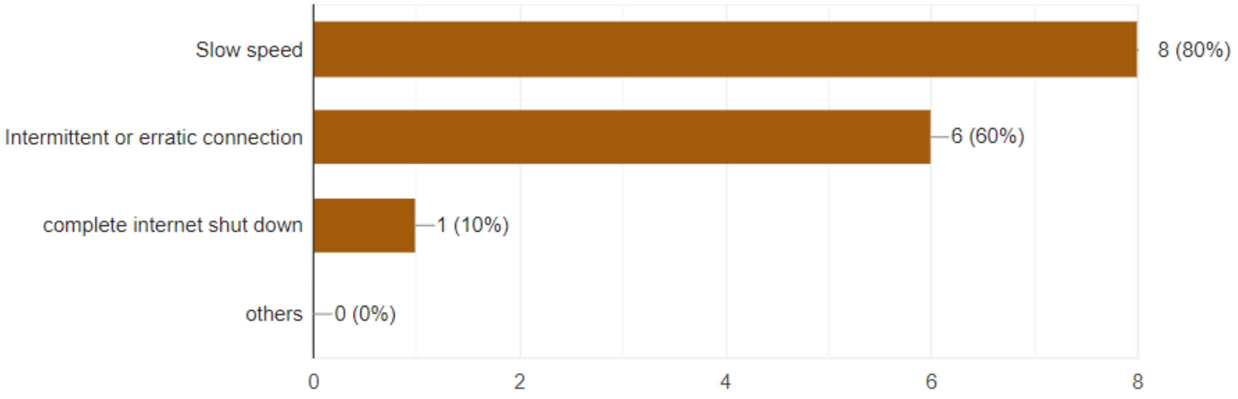

Figure 4. Types of internet challenge experienced by students of ACETEL

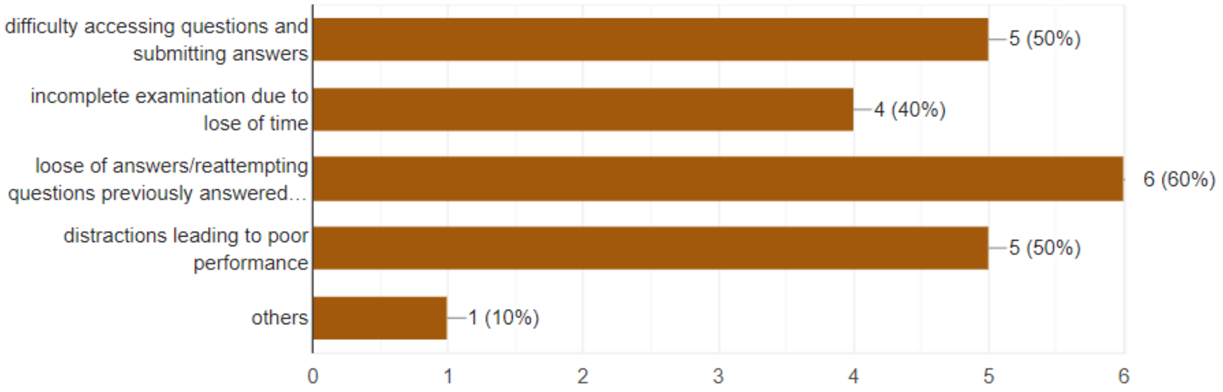

Figure 5. Effects of internet challenges

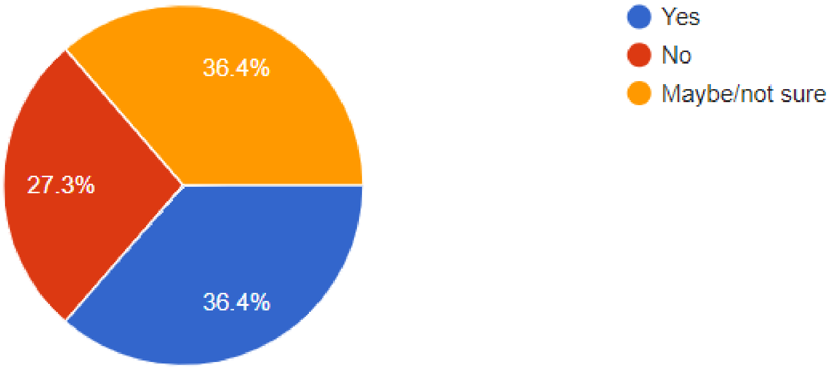

Figure 6. Effect of internet challenges on performance of students

However, in the case of intrusion of monitoring technology during exams, only 18.2%of ACETEL students reported they had challenge of that dimension (figure 7). The remaining 81.8% insisted that they were satisfied with the monitoring system implemented by ACETEL as it did not disturb their exams. We suspect that the reason for this was due to the fact that the ACETEL system uses AI technology that monitored examinees using the inbuilt camera and microphone of the examinees computer only. This is a departure from implementations like Sabbah (2017) and Rajendra et al (2022), that requires additional equipment like keyboards, external fingerprint scanners, and external array of camera sets, in addition to the IA proctor, to monitor the student and thus intrude on their exams as discussed in the literature review.

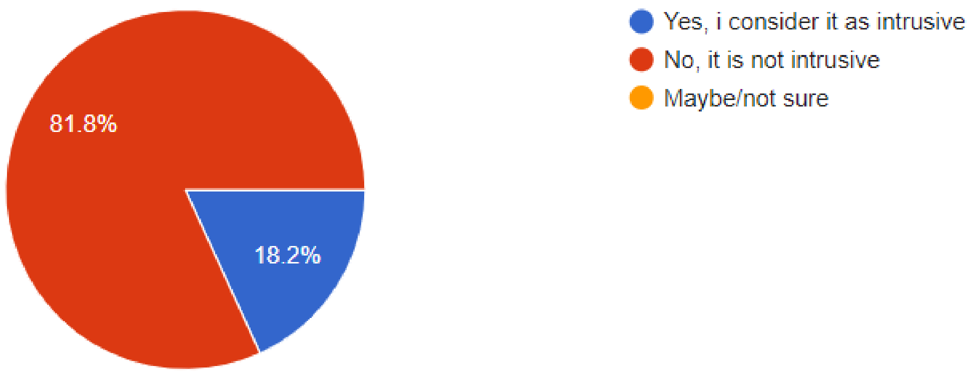

Figure 7. Intrusion of monitoring technology

It is worthy of note that 45.5% of ACETEL students acknowledged that the system used by the institution was effective as an anti cheating systems (see figure 8). The take home from this is that complexity of equipment may not always be the solution in every situation. Some complex systems may improve exam security as in case of Sabbah (2017) and Rajendra et al (2022), but can also introduce other bottlenecks such as intrusion during exams and increased costs . Our take home from this is that the simplicity of the system went a long way to reduce the intrusive effects of monitoring technology. This implies that building related system as ACETEL could ameliorate this kind of challenge while still enforcing security of exam.

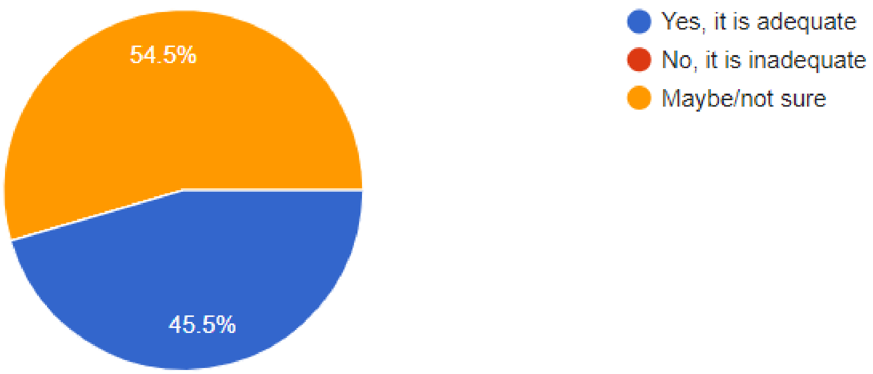

Figure 8. Adequacy of Anti-cheating system

It is concluded here that,the existing systems have not adequately addressed the issue of secure and continuous monitoring of e-assessment systems in remote (home) environment in situations were internet services are poor. Also, intrusion of ongoing exams by complex monitoring processes are poorly addressed by current schemes. Complexity in implementation technology resulting in increased cost is also another challenge that is not properly addressed by existing schemes. Therefore, in locations were internet connectivity is limited, there is a need to develop and implement a scheme that de-emphasizes the transmission of proctoring signal input over the internet for onward analysis but rather, allow for local processing of such input to address the challenge of poor internet services over remote exams. Such system will also address the complexity in central systems that have to manage a large number of remote clients.

.

What Features are Required in a Secure Remote Electronic Exam System that Guarantees the Sanctity of Exams and Solves the Present Challenges?

The basic features of a secure remote e-examination system as identified from the literature review are illustrated using figure 9. Generally, for a remote e-examination systems, a central server manages the processing needs of the continuous verification and monitoring modules of the system. This is based on the premise that there is reliable internet service available to all nodes of the system. In cases were internet services are poor or fail completely, such systems become mostly ineffective, as in the case of Sabbah (2017).

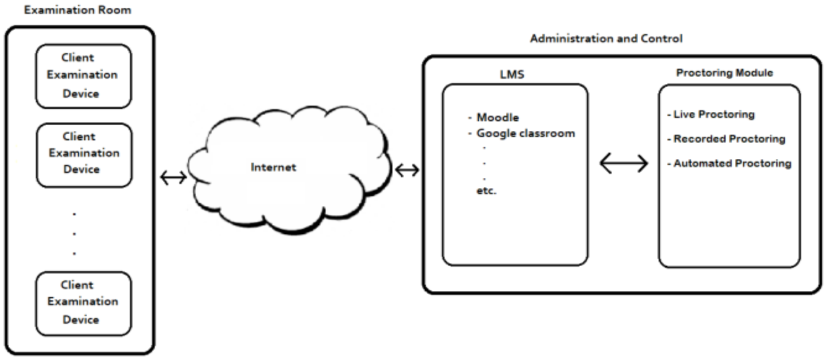

Figure 9. The generic proctored e-examination systems (source:Muhammed and Alli, 2022)

In order for a typical remote exam system to meet acceptable performance standards, it must meet several requirements including the the following (Ketab, 2017; Sabbah, 2017; Rajendra et al ,2022):

1. The system should be capable of monitoring an examinee continuously using biometric or other technology;
2. The system should be secured from attacks both internal and external ;
3. The system should have capacity to effectively counter cheating during exams;
4. The system should be scalable;
5. A system should be based on user-centric design principles;
6. The system should be built to adapt to different platform;
7. The system should use hardware that can be used by less technology savvy individuals;

In addition to the above, and as confirmed from the opinion of sampled students in subsection 3.1.1,:

8. the system should be able to function effectively over slow, intermittent, and even extremely poor or temporarily non existent internet conditions Failed internet connectivity should not be a condition to deprive remote examinees valuable exam time by logging them off. The system should be robust to ensure the security of exams in adverse internet conditions;
9. The system should emphasize simplicity over complexity in the design of the monitoring system with a mind to maximize exam security while minimizing cost and intrusion of system during exam.

Proposed Theoritical Model

In this section, an e-exam model that seeks to address the gaps identified in current remote e-assessment schemes is proposed.

SOCAM model

Here we describe the structure of the proposed model and its operation. Figure 10 shows the structure of the SOCAM model. It consists of two major components: a Central Management Unit (CMU) and the Client-based Unit (CU).

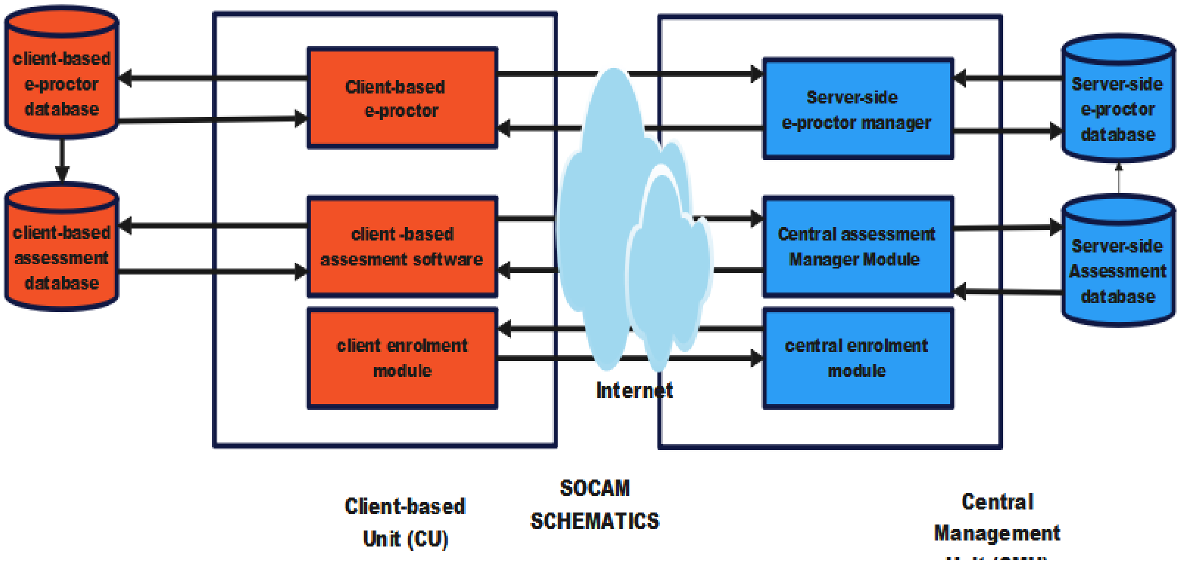
client-based e-proctor database
client-based assessment database
Client-based e-proctor
client -based assesment software
client enrolment module
Internet
Server-side e-proctor manager
Central assessment Manager Module
central enrolment module
Server-side e-proctor database
Server-side Assessment database
Client-based Unit (CU)
SOCAM SCHEMATICS
Central Management

Figure 10. Schematics of SOCAM

1. **Central Management Unit (CMU)**

   This unit provides an interactive online environment that automates the administration of the e-examination. It is a server- based system responsible for the following:

   a. Registration of examinees, examiners and other users of the system;
   b. Administration, Storage, Organization and delivery of relevant assessment media and reports;
   c. Secure storage of e-proctor reports;
   d. Reporting of examination outcomes to users;
   e. Secure communication with the client -based assessment application and e-proctor
   f. Central security management.

2. **Client-Based Unit (CU)**

   This unit is a client- based software application responsible for the following:

   a. E-proctoring service customized to examinee
   b. Local security management
   c. Assessment interface
   d. Secure temporary Local storage of examinee assessment media and exam report
   e. Secure temporary storage of e-proctor reports.
   f. Secure communication of assessment and e-proctor reports to central server

3. **Operation of the proposed SOCAM model**

   The operation of the proposed model shall be divided into three stages:

   Stage one: Enrollment

   The following is requested and stored by the CMU in the profiles of each registering student:

   a. User name and password
   b. High resolution photo shot(s)
   c. Series of high resolution photo shots of student while he reads and answers typical sample questions
   d. Short video clip of student while he reads and answers typical sample questions

   Stage two: examination stage

   In this stage:

   a. the examinee downloads and installs (or updates) a web application having e-assessment interface and e-proctoring capability.
   b. He logs into his CMU profile page using his username, password and photo matching technology. If the log in fails, an error message is generated and another login trial issued

c. He selects a scheduled exam. The CMU sends command that initializes the client based proctor.
d. The Client-based proctor activates examination screen. The exam window covers the desktop and initiates a lockdown. At this point, the examinee cannot leave the exam area consisting of his desk carrying the local machine. The proctor warns the examinee via an instruction on the screen and shuts down the exam if this is violated at anytime.
e. E-proctor request examinee to read and answer a stored typical exam question. Collects verification and monitoring samples (photo+video clips). and sends to CMU for matching if network is adequate to do this. If not, system waits until network becomes available with warning screen stating examinee cannot leave area while network fluctuates else session is discontinued.
f. CMU matches and reports to local proctor. If matching fails, error message is issued and session is terminated, else CMU delivers encrypted copy of the exam questions to the local question database, and encrypted copies of the biometric samples of the examinee to the local biometric database. Cryptographic keys for the duration of the exam session are also delivered to the local database at the time of commencement of the examination. Each question requires separate keys for decryption .
g. If the examinee clicks the start button presented by the e-proctor at this phase, The local question 'generator' selects a question or batch of questions (essay type for which the examinee selects the question to answer first) and a decryption algorithm decrypt the selected question or batch and presents to the examinee.
h. The examinee completes the question(s) and submits. The proctor checks for internet connection, if ok updates the CMU with encrypted report of current answers of the examinee and current verification and monitoring report for storage. Else stores encrypted report locally awaiting connectivity. The assessment continuous this manner until the examination is terminated.
i. The e-proctor initiates periodic verification and monitoring procedures for continuous verification and to detect cheating all through this stage. Violation occurs when some well defined rules are broken. Violation can be Impersonation and cheating violation or system violation. Impersonation violation occurs when the examinee tries to cheat or cheats. System violation occurs when defined system features such as camera, keyboards or power is disconnected. In cheating violation, a penalty is issued with weight depending on the gravity of the offence. The penalties are reported on the screen and added up. If the sum of the weighted violations exceeds a predefined threshold, the exam can be terminated and a report of the current state generated for onward post examination action by human authorities.

Finally, the exam can end when:

a. The examinee completes the exam and ends the session. Here the system generates the updated reports (answers+proctor reports), encrypts, and sends to the CMU if network permits, else it awaits network and stores copy in local database. The examinee cannot leave the exam area until the final report is dispatched to the CMU.
b. The proctor terminates the session due to violation exceeding threshold. The final report is generated at this point and delivered to CMU before examinee leaves the area. Examinee is informed of reason for termination which can be printed from his profile in the CMU

Stage three: Report Generation stage

Report generation occurs all through the examination with a final report at the end of the examination. The system is based on periodic updating of the CMU depending on the internet connectivity during the exam session. If the session is terminated due to system or cheating violation, the report is based on the current state of the examination answer and e-proctor assessments. Otherwise, an end of examination report is generated by the CMU based on the report of the client-based application periodic updates and final termination update. A typical report (periodic or terminal) consists of the examinee answers to questions, periodic exam session photo shots and video clips and e-proctor analysis of authentication and monitoring data.

4. Evaluation of the proposed model

The features of the proposed model is based on modification of existing e-exam schemes, such as schemes by Sabbah (2017), that are proven to be effective for the conduct of high stakes exams under favourable internet conditions. The modifications are targeted at correcting the weaknesses inherent in such schemes while leveraging their strength . This implies that the proposed model is an enhancement of existing schemes, allowing for cheaper implementation and efficient operation during poor or unavailable internet service.

However, the proposed model is still at the conceptual stage. A prototype will be developed and experimented upon to evaluate the proposed model in the areas of its exam security (impersonation and cheating threats) ,system security (external and internal threats), accessibility, efficiency and usability. The proposed model will be compared to other automated proctored system to see how it performs in comparison to existing systems.

Conclusion

In this paper, a Rapid Review of Literature (RLR) and Mixed type online survey questionnaire was used to find answers to two research questions: 1. What challenges exists in existing remote electronic exam systems that undermine the sanctity of exams? 2. what features are required in a secure remote electronic exam system that guarantees the sanctity of exams and solves the present challenges?

Findings from the investigation show that the existing remote e-exams schemes are challenged when there is limited internet services as is often the case in developing countries. This leads to disruptions during exams resulting in poor scores or in some cases, zero scores for students. Also, the schemes often involved the use of expensive technology beyond the rich of poor students. Furthermore, several existing schemes implement technology that cause intrusion during exams. The implication of the above is that such systems may be very difficult to use in regions that have internet challenges and in poor regions where students and institutions cannot afford these technologies. To resolve the challenges, the identified features required for effective remote e-exam conduction were modified and used to propose an emerging Secure offline continuous authentication and monitoring (SOCAM) model for remote online examination . The model allows an examinee to register for a remote examination by capturing his biometric data including image and video clips. The examinee can take an exam at the comfort of his home or any other location with minimum internet connectivity. Breakage in internet connection for chunks of times is tolerated by the model without compromise of exam security.

It is concluded that the proposed model, which is based on the strength of the existing schemes and modification of features to eliminate inherent weaknesses in them, can offer a cheaper and more efficient alternative to other remote e- exam schemes that depend massively on outstanding internet connectivity during exam lifetime.

Future works include prototype development and experimentation on the emerging model. Exam security, internal and external threats capacities, efficiency and usability are some of the criteria to be evaluated. Also, The model will be compared with related existing systems. Generic theories on remote electronic examination will be examined closely using the model.

References

Adebayo, O., & Abdulhamid, S. M. (2014). E-exams system for Nigerian universities with emphasis on security and result integrity. arXiv preprint arXiv:1402.0921.

ARSLAN, A. P. K., & SEMENDEROĞLU, A.() Development and application of S-GALL: an online examination system for higher education in turkey.

Ayo, C. K., Akinyemi, I. O., Adebiyi, A. A., & Ekong, U. O. (2007). The prospects of e-examination implementation in Nigeria. Turkish online journal of distance education, 8(4), 125-134.

Bailie, J. L., & Jortberg, M. A. (2009). Online learner authentication: Verifying the identity of online users. Journal of Online Learning and Teaching, 5(2), 197-207.

Bertiz, Y., & Hebebci, M. T. (2021). Security for Online Exams: Digital Proctoring. International Society for Technology, Education, and Science.

Butler-Henderson, K., & Crawford, J. (2020). A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity. Computers & Education, 159, 104024.

Chong, S. W. (2019). College students' perception of e-feedback: a grounded theory perspective. Assessment & Evaluation in Higher Education, 44(7), 1090–1105. https://doi.org/10.1080/02602938.2019.1572067

Desmond, A. Farouk, L. aAkos, S. (2020). Multimodal Biometric Authentication For a Computer-Based Test (CBT) Application. IRJCS:: International Research Journal of Computer Science, Volume VII, Issue VII, 179-196.

El Sayad, G. A., El Aziem, M. A., & El Fakharany, E. E. D. (2014). A new remote authentication model for online examination systems. European Journal of Scientific Research, 125(1), 115-127.

Frankl, G., Schartner, P., & Jost, D. (2017). The "Secure Exam Environment": e-testing with students' own devices. In Tomorrow's Learning: Involving Everyone. Learning with and about Technologies and Computing: 11th IFIP TC 3 World Conference on Computers in Education, WCCE 2017, Dublin, Ireland, July 3-6, 2017, Revised Selected Papers 11 (pp. 179-188). Springer International Publishing.

Karthika, R., Vijayakumar, P., Rawal, B. S., & Wang, Y. (2019, May). Secure online examination system for e-learning. In 2019 IEEE Canadian conference of electrical and computer engineering (CCECE) (pp. 1-4). IEEE.

Kumar, K., & Farik, M. (2016). A review of multimodal biometric authentication systems. Int. J. Sci. Technol. Res, 5(12), 5-9.

McCoy, C., Yu, A., & Ramazanova, S. (2015). An author co-citation analysis: Examining the intellectual structure of e-learning from 1981 to 2014. Proceedings of the Association for Information Science and Technology, 52(1), 1-3.

MOHAMMED, H. M., & ALI, Q. I. (2022). E-Proctoring Systems: A Review on Designing Techniques, Features and Abilities Against Threats and Attacks. Quantum Journal of Engineering, Science and Technology, 3(2), 14-30.

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.

Ngqondi, T., Maoneke, P. B., & Mauwa, H. (2021). A secure online exams conceptual framework for South African universities. Social Sciences & Humanities Open, 3(1), 100132.

Noorbehbahani, F., Mohammadi, A., & Aminazadeh, M. (2022). A systematic review of research on cheating in online exams from 2010 to 2021. Education and Information Technologies, 27(6), 8413-8460.

Sabbah, Y. W. (2017). Security of online examinations. Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications, 157-200.

Sabbah, Y., Saroit, I., & Kotb, A. (2011, June). An interactive and secure e-examination unit (ISEEU). In 2011 RoEduNet International Conference 10th Edition: Networking in Education and Research (pp. 1-5). IEEE.

Smela, B., Toumi, M., Świerk, K., Francois, C., Biernikiewicz, M., Clay, E., & Boyer, L. (2023). Rapid literature review: definition and methodology. Journal of market access & health policy, 11(1), 2241234.

Ullah, A., Xiao, H., Lilley, M., & Barker, T. (2012). Using challenge questions for student authentication in online examination. International Journal for Infonomics (IJI), 5(3/4), 9.

Ullah, A., Xiao, H., Lilley, M., & Barker, T. (2014, September). Privacy and usability of image and text based challenge questions authentication in online examination. In 2014 International Conference on Education Technologies and Computers (ICETC) (pp. 24-29). IEEE.

Zhu, X., & Cao, C. (2021). Secure online examination with biometric authentication and blockchain-based framework. Mathematical Problems in Engineering, 2021.