Current and Prospective Views of Electronic and Remote Invigilation of Examinations

[*1]Iwasokun G. B., [2]Akinyede R. O., [3]Alese B. K., [4]Ayinde F. O., [3]Odeniyi O. A., [5]Afolabi O. O., [1]Ehineni O. J., [1]Gbale M. O., [2]Balogun T. E.

[1]Department of Software Engineering, Federal University of Technology, Akure, Nigeria

[2]Department of Information Systems, Federal University of Technology, Akure, Nigeria

[3]Department of Cybersecurity, Federal University of Technology, Akure, Nigeria

[4]Department of Computer Science, Elizade University, Ilara-Mokin, Nigeria

[5]Department of Information and Communication Engineering, Elizade University, Ilara-Mokin, Nigeria

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2024.8090261

Received: 02 September 2024; Accepted: 10 September 2024; Published: 22 October 2024

ABSTRACT

An examination or a test is intended to measure an examinee's knowledge, skill, aptitude, physical fitness or classification. It varies in style, rigour, and requirements. It may be administered orally, on paper, on a computer, or in a confined area that requires an examinee to perform a set of skills physically. Examinations require thorough invigilation and supervision, which may be based on direct human involvement or the adoption of remote technologies. An adequate invigilation process makes candidates conform to regulations and prevents all forms of infractions. This paper presents a review of the assessment of the existing and relevant literature on electronic-based examination or assessment and its remote invigilation strategies. The review focused on the motivations, objectives, methodologies, results, contributions to knowledge and limitations. The failure of the traditional and human-based invigilation systems was greatly emphasized alongside the urgency in putting in place safer security measures. The review revealed that significant gaps exist in the areas of attaining CBE systems that are fool-proof and infraction-free. The study on the current state of biometrics-based e-invigilation across the world also established its wide deployment and acceptance as well as the challenges of capital intensiveness, lack of political will and expertise, and methodological failure, among others. It was also established that the adoption and deployment of technology for remote/human-less invigilation of examinations is confronted with some issues that need urgent attention.

Keywords: Examination, invigilation, remote monitoring, educational technology, electronic proctoring

INTRODUCTION

Nigeria, which has seen very high enrollments across all educational levels, is currently dealing with the astounding rise of violence and dishonesty in academic examinations. This has been one of the main causes of the low acceptance rate of academic credentials from Nigeria by institutions and organizations in many other nations around the world. At present, the number of applicants to post-secondary institutions in Nigeria stands at one million, nine hundred and forty thousand (1,940,000). This number is expected to increase steadily, although the capacity of all institutions for admission is approximately five hundred thousand (Abubakar & Adebayo, 2014). The extremely fierce competition among candidates is largely attributed to the institutions' low admission rates and capacities. Some desperate applicants have turned to various sorts of examination-related violence and dubious tactics to further their causes. Educational administrators have embraced the adoption of the Computer Based Examination (CBE) model for testing, and evaluation as a remedy to these challenges. In

Nigeria, the CBE platform is being utilized to promote effective, efficient, and reliable assessment on courses with hundreds or thousands of student enrolments across hundreds of higher institutions. This is in addition to post-secondary admission recruitment examinations as well as job placements (Iwasokun *et al.*, 2018). Although CBE introduced flexibility, timeliness, reliability, and impartiality in educational and other types of assessment, there are still cases of excesses and violations on the parts of the test takers and the invigilators.

Cheating problems and other human invigilation-related vices have persisted in tarnishing the credibility, acceptability, and integrity of CBEs around the world (Ricketts et al., 2003). Additionally, the current methods of candidate validation and system integrity checking using passwords, Personal Identification Numbers (PIN), Identification (ID) cards, examination slips, and tokens are vulnerable to theft, imitation, transfer, loss, or forgetfulness, as the case may be. It has been proven that using these possessive approaches to deter applicants from engaging in unethical behaviours including pimping, script exchange, peeping into other candidates' screens, and external sourcing, among others, is ineffective (Wales and Baraniuk, 2008; Goswami and Bau, 1991). Just like in any other nation of the world, governmental, commercial and private organizations continued to leverage on CBE platform for recruitment and career-lifting examinations. To attain academic honesty and integrity through good identity management, the prevention of impersonation, and a decrease in violence, the Joint Admission and Matriculation Board (JAMB) has been saddled with the task of overseeing the nationwide pre-admission examination in Nigeria. The Agency has acknowledged the significance and encouraging impact of the CBE in addressing some of the aforementioned challenges as well as the attendant problems of CBE (Assaf, et al., 2007; Chi-Chien, 2004; Kikelomo et al., 2010; Iwasokun and Akinyokun, 2016).

Existing Works on Remote Invigilation

Iwasokun et al. (2018) proposed a framework for invigilating computer-based examinations using fingerprint and iris biometric technologies to address issues of identity verification and other infractions. The study aimed to develop a robust and effective invigilation system to enhance the credibility and security of CBEs. A framework with three modules; namely CBE, e-invigilation, and control was proposed. The CBE module comprised a network backbone, a server, and several workstations, ensuring a stable and secure examination environment and using fingerprint technology for candidates' authentication. The e-invigilation module requires high-definition and high-resolution iris scanners such as IrisShield-USB MK and CMITech BMT series to capture and process the candidate's iris position and orientation. For either direction, a displacement threshold θ, shown in Figure 1 is defined such that if the iris movement exceeds, the candidate is assumed to be peeking and hence, a warning splash message is displayed on the screen. While the first repeat of such an infraction causes the screen to blink for a set time, a second repeat will cause a logout of the candidate from the examination platform and a notification on these actions is sent to the Administrator. To further enhance the proposed framework, Iwasokun et al. (2019) combined the iris angular displacement with a facial orientation and set thresholds for the two. Infractions are noted and followed with appropriate actions as described by Iwasokun et al. (2018). The proposed frameworks lack the experimental studies to establish their practical functions in a real-world setting. This restricts their evaluations for effectiveness, feasibility and performance evaluation.

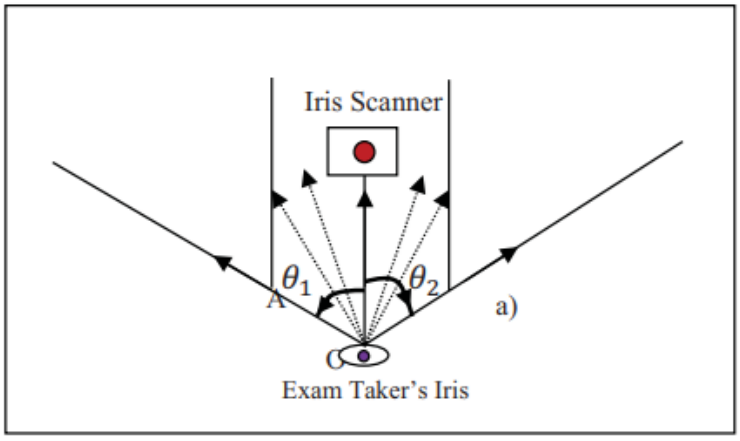

Figure 1: Exam taker's angular facial displacement from the normal

Ketab et al. (2017) presented a continuous authentication and monitoring mechanism based on multi-modal biometrics for computer-based-assessments. The mechanism ensures that only legitimate individuals participate in an examination and its operation is based on an eye tracker that records the examinee's eye movements and speech recognition for the detection and curbing of infractions. The main processes of the mechanism are depicted in Figure 2. Its implementation requires that participants work through a process of registration of facial images, formulation of template data, and calibration of the basic eye movement around the screen. A time-based and continuous 2D facial recognition is also required for the candidate's identification and authentication. The experimental study of the mechanism involved the collection of examinees' biometric data and eye and head movements using customized software. A 3D camera and a built-in microphone were used to capture the facial and voice signals respectively. The multiple-scenario experiment that involved 51 participants justified the ability of the mechanism to suitably identify impostors and misconducts.

Okada *et al.* (2019) attempted to shed light on how the use of e-authentication systems increases trust in e-assessment, and the variations in the level of acceptance would vary across gender, age and programmes based on an authentication system known as adaptive trust-based e-assessment system for learning (TeSLA). The TeSLA project conducted several empirical studies between February and June 2017 across seven universities; namely Anadolu University, the University of Jyvaskyla, the Open University of the Netherlands, The Open University UK (OOUK), Sofia University, the Technical University of Sofia and the Open University of Catalunya. The local ethics committee's approval guided the studies and all data were anonymized and focused on checking the efficacy of the TeSLA instruments while gathering feedback from users about their experiences with the instruments. The TeSLA instruments piloted by the OUUK were keystroke analysis and anti-plagiarism, chosen because of their relatively straightforward implementation in a Moodle virtual learning environment. A mixed-methods model was used to triangulate statistical and qualitative findings on student performance, views and concerns.

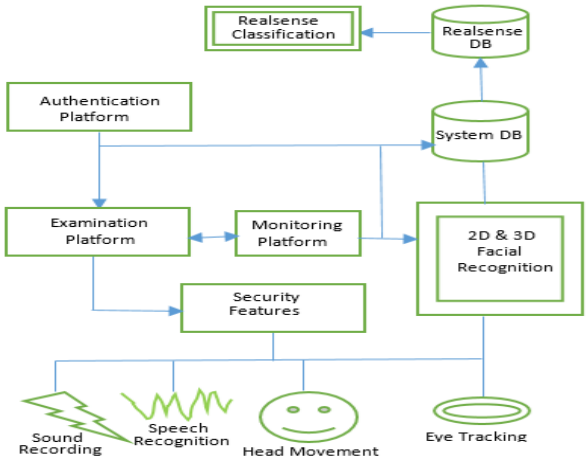

Figure 2: Examination monitoring process (Ketab et al. (2017))

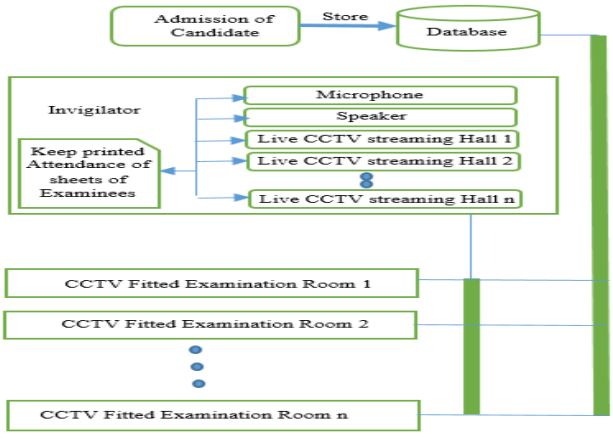

Figure 3: The examination framework proposed by Hoque *et al.* (2020)

Evidence from mixed-method analysis suggests a broadly positive acceptance of e-authentication technologies by distance education students. However, significant differences in the students' responses indicated, for instance, that men were less concerned about providing personal data than women; middle-aged participants were more aware of the nuances of cheating and plagiarism; while younger students were more likely to reject e-authentication, considerably due to data privacy and security and students with disabilities due to concerns about their special needs. The outcomes of the study support the use of innovative technologies in assessment while underscoring the need for the developers of e-authentication systems and pedagogical teams to recognise and respond to the widely differing nature of examinees. According to the authors, a good knowledge of students' attitudes and familiarity with e-assessment is important for achieving a significant reduction in plagiarism and cheating in online assessment. It was also stated that achieving a high-quality assurance assessment process requires a multi-instruments and trust-based system for e-authentication, which aligns with the views presented in (Von-Schomberg, 2011; Baneres et al., 2016; Okada et al., 2015).

Given the need to reduce the number of invigilators and malpractices by students during pen and paper-based examinations, Hoque *et al.* (2020) developed a framework for the authentication and monitoring of candidates for the traditional pen-and-paper-based examination. The framework, whose model is shown in Figure 3 requires educational institutions to preserve a database using the Parallax Data Acquisition tool (PLX-DAQ) that incorporates bio-metric information of all students. Before admittance into the examination hall, the examinees are taken through a biometric authentication process. During the examination, examinees are remotely supervised and controlled from a distance via some 360-degree Closed-Circuit Television (CCTV) cameras as well as ultra-high sensitive microphones and speakers. The CCTV cameras and the microphones monitor the examinees' physical activities and vocal communications respectively. The framework allows a single invigilator to remotely monitor proceedings from several examination halls, thereby promoting cost-effectiveness as well as a simple and secure solution to the complex process of traditional examination invigilation. Minott (2021) presented findings on unearthing exam invigilators' perspectives, tacit work-related knowledge, and skills via reflection-on-experience in computer-based examinations. The focus was on showing how reflection-on-experience enacted through interviews can unearth the tacit work-related knowledge and skills exam invigilators developed on the job and address the lack of attention given to invigilators in some existing research works. Data collection was based on interviews and the responses were analyzed for interpretation and answers to the research questions. Results from the interview showed participants saw invigilation of computer-based examinations as either 'easy' or 'demanding'.

Participants also portrayed the facets or procedures of exam invigilation (such as timekeeping, giving instructions, rest, or toilet breaks), the students' attributes (for instance, special educational needs), and computer and operational knowledge (such as knowing about a USB stick and deleting a document, and whom to call when there is a problem with a computer). The procedural skills of the participants (such as discretely directing students to the toilet and computer troubleshooting) and intangible skills (mental flexibility, care, and creativity) also came to bear. The research established that through a critical discussion of the literature, coupled with the findings that invigilators learn on the job, participants developed work-related knowledge and skills which are often implicit or tacit and may be sustained if not given an opportunity, via reflection, to be made explicit. Based on these, the author concluded that the creators of examination invigilation policies at all levels should harvest the thoughts of invigilators through formal and informal means to improve examination policies and procedures.

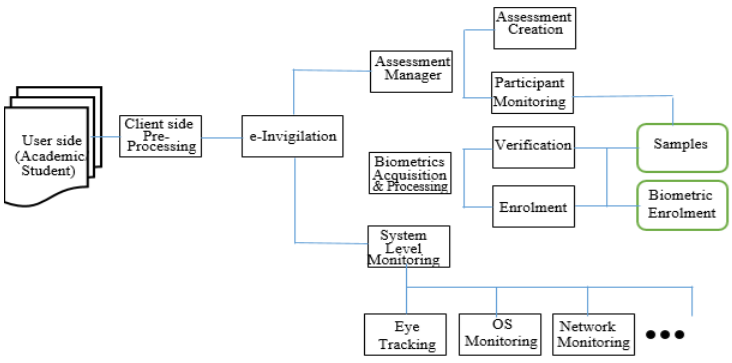

Figure 4: Architecture of the e-assessment framework presented by Ketab *et al.* (2015)

It was also suggested that invigilators should be involved in yearly examination planning meetings, training of new invigilators and informal conversations on their experiences in the role towards greater improvements in the planning, implementation and evaluation of the examination invigilation processes and procedures. Ketab *et al.* (2015) present a general analysis of invigilation and e-assessment solutions. A framework for e-assessment that promotes student convenience and effective verification was also developed based on the architecture presented in Figure 4. Transparent or non-intrusive identity verification was utilized to conveniently capture and process biometric signals, which has the potential to facilitate continuous verification. The framework was designed in a modular fashion to incorporate a range of behavioural and physiological biometrics including face recognition, keystroke analysis, mouse dynamics, linguistic analysis and iris recognition. The opportunity was provided for capturing biometric samples under a range of differing examination scenarios like essay writing and multiple-choice tests. The framework can automatically direct candidates to the required subsystems as well as tabs and sub-tabs to follow predefined system instructions. It also can create, edit and delete previously stored or current tests and results based on the principle of transparent or non-intrusive monitoring which was implemented in a fully controlled manner. The candidates' biometrics were stored to serve as the basis for subsequent matching and monitoring.

Giannopoulou et al. (2023) critically reviewed the European normative framework for countering the risks and situations of harm generated by e-proctoring through the lenses of data protection and anti-discrimination law. The corpus of online proctoring-related decisions that have emerged in the EU over the past three years were systematised and analysed. An overview of the technical aspects of the technology and an outline of the legal issues were debated and followed up with the reconstruction and discussion on the convergences and divergences in how courts and independent authorities have assessed the lawfulness of online invigilation methods and tools. Analysis of the existing e-proctoring instruments based on the concrete features that were implemented showed that with some notable exceptions, the General Data Protection Regulation (GDPR) and the anti-discrimination framework are largely helpful in combating the most intrusive forms of e-proctoring deployment as well as mitigating their risks. It was also established that due attention should be paid to the effectiveness of the collective enforcement of rights, discriminatory effects for people not covered by a protected ground, and the operational guidelines and policies on technology.

Akingbade and Eze (2022) presented a fingerprint-authenticated computer-based examination system that aimed at bridging the security gap of impersonation that is often associated with the use of computers for the conduct of examinations. The system relies on a web application that incorporates fingerprint authentication into the login interface of each examinee as a means of curbing impersonation. The system uses a PHP web-based code/language that uses visual studio code to achieve fingerprint identification that informs the decision to grant or deny access to the examination questions. The system detects a person during identification by comparing his or her fingerprint biometrics with each entry in the database, granting access when there is a match and prohibiting access when there is not. The workflow of the system is presented in Figure 5.

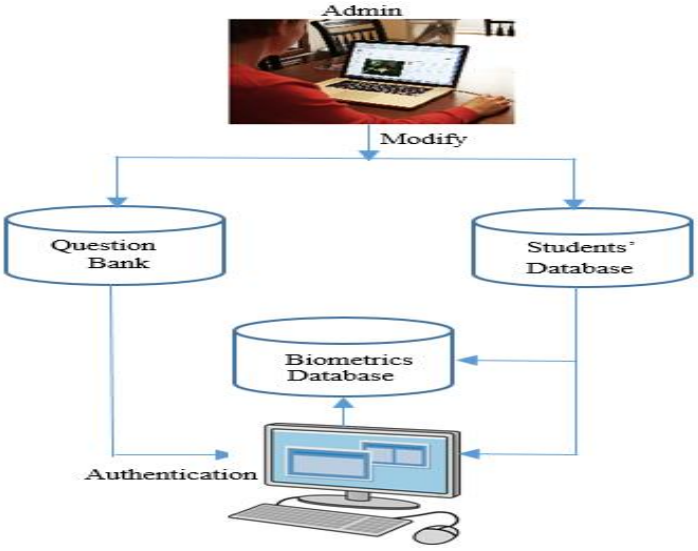

Figure 5: The workflow of the system proposed by Akingbade and Eze (2022)

Elenwo and Nwanguma (2023) investigated electronic invigilation inclusion in curbing examination malpractices among students. The investigation adopted the hypotheses and descriptive survey approach and the Taro Yamane Formula was used for the sample size. The multi-stage sampling techniques were adopted in selecting the sample size of 400 and a structured and validated questionnaire was used as an instrument for data collection. Listed items were rated on a four (4) point scale while the mean and standard deviation were used to answer the research questions with the adoption of a z-test for testing the formulated hypotheses. Analysis of surveyed data revealed a high impact of close-circuit television (CCTV) cameras, biometric systems and signal jamming devices in curbing examination malpractices. According to the researchers, the mere presence of CCTV cameras, biometric systems and signal jamming devices in examination venues is capable of scaring and dissuading candidates from malpractices, since recorded clips could be filed as evidence during investigation and prosecution.

Colonna (2021) focused on live and AI-proctored testing as well as the use of AI-anchored proctoring for online exams and, in particular, to validate students' identities and flag suspicious activities during the exam. Such activities include plagiarism, unauthorized collaboration and sharing of test questions or answers. Emphasis was on AI-based facial recognition technology (FRT) typically shown in Figure 6 that could be used during the authentication process for remote monitoring during the online exam process as well as to identify dubious behaviour throughout the examination. The focus was also on the necessity and lawfulness of remote proctoring systems, fundamental rights implications, current laws and regulations, legality case studies, lawful grounds and the relevant factors for determining whether the use of AI-based tools is necessary and proportionate for remote proctoring exams.

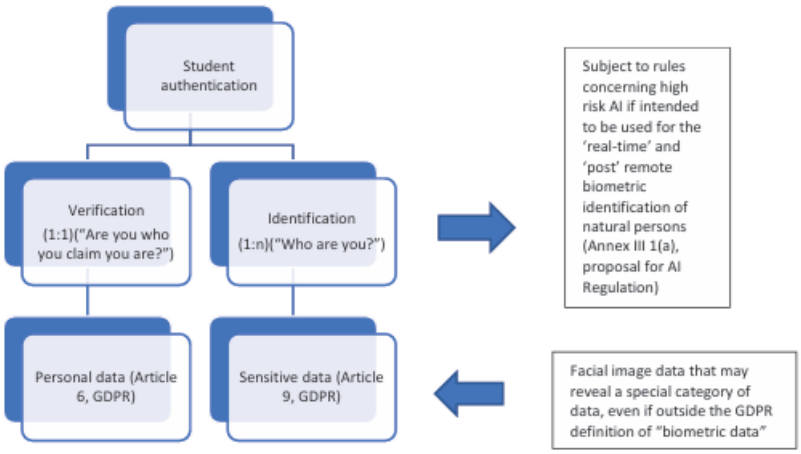

Figure 6: A typical e-proctoring AI-based facial recognition structure suggested Colonna (2021)

To enhance the security and authentication lapses of the existing online examinations, Anandi et al. (2020) proposed an e-monitoring e-examination system using a multi-factor security and authentication mechanism based on biometrics, Encryption and Spyware (BES). The system was designed to address the security and authentication lapses of the existing online assessment platforms such as impersonation and accessing the Internet or remote sharing of desktops for the assessment of the security and authentication features. There are test centre, a security layer and a database layer. Unlike the current practice where the screen is locked for most of the existing e-assessment platforms, the proposed system allows the student to utilize all the permissible system resources but implements measures to log the student out of session if found attempting to access any of the restricted resources such as the Internet. The system was implemented in a Spyware report module which monitors and controls the calls made by applications and services and is programmed to listen to specific IP address and API calls, such as file and application events and Internet activities. During the execution of the spyware program, the API Monitor displays the intercepted API and the activity log is subsequently called for analysis. An experimental study of the system established its good performance.

Balogun (2023) highlighted the ongoing challenges to academic tests and assessments and their impacts on the validity and acceptance of certificates and degrees. Focused was also on addressing the integrity issues in CBEs by proposing a conceptual framework that utilizes multimodal biometrics to achieve human-less invigilation.

The framework is based on the integration of fingerprint verification with facial and iris recognition technologies for real-time monitoring. An HTML, JavaScript, and PHP-inspired CBE module were blended with the iris, face and voice signals using Python programming language to remotely monitor and control examinees' activities based on advanced machine learning. The operational flow of the monitoring and control unit is presented in Figure 7. The platform emphasizes continuous candidate monitoring as a means of achieving a comprehensive and infraction-free testing environment. An experimental study of the practical function of the framework demonstrated its ability to monitor and document instances of unethical behaviour in a manner devoid of extensive video data storage and transmission. The platform is however susceptible to the privacy and data security concerns that are associated with biometric data collection and processing. There are issues with accuracy and reliability under varying environmental conditions, such as lighting and background changes as well as the intensive cost of implementation and maintenance which could restrict their adoption in less affluent set-ups. Furthermore, the system was only studied in a controlled environment, and its performance in real-world settings with diverse populations and varying conditions remains uncertified.

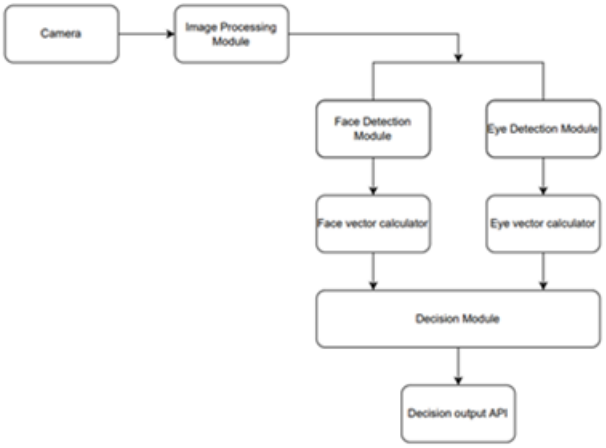

Figure 7: The operational flow of the monitoring and control unit of the framework proposed by Balogun (2023)

Current State - Existing Measures

Recently, there have been concerted efforts at remote invigilation which are premised on the use of fool-proof and specific tools. Institutional bodies are being compelled to take drastic actions during peculiar situations where examinees are unavoidably absent due to some complex logistical needs. Such actions include the adoption of online technologies like Skype-based invigilation framework on an *ad-hoc* basis where a human examiner is expected to oversee or monitor the process, which may be cumbersome and complex (Cramp *et al.*, 2019). The need for more remote testing procedures has also greeted the rising increase of international students for institutions at all levels. This has culminated in the emergence of a wide range of third-party test centres with a huge potential for increased flexibility, greater convenience as well as very reliable remote invigilation services. The ever-increasing number of students and teachers dealing with millions of courses has further heightened the concern over protection against misuse in the form of cheating or unauthorized help during online or remote examinations. Although several scientists presently concentrate efforts on proposing solutions to this concern through methods that demand an examinee intrusively provide an authentication sample such as a password, Identity Card, and Radio Frequency Identification (RFID), there is still the issue of achieving the mandatory level of safety or reliability (Ketab, 2016).

Efforts are now been geared at using one or more biometric features of the examinee to achieve safety, integrity and reliability during computer-based assessments. The biometric features presently enjoying dominance include face, voice, fingerprint, palm print, iris, keystroke analysis and mouse dynamic (Iwasokun et al., 2022). User acceptance satisfaction has also been pursued as an essential factor, hence, transparency and continuous authentication are being utilized to attain a proven scale. According to Colonna (2021), in a bid to prevent postponing or stalling examinations in the wake of the COVID-19 pandemic, establishments such as universities opted for virtual proctoring technologies, using multifaceted problems on ascertaining the reliability and transparency of online assessments without disregarding ethical and legal constraints, specifically concerning

students' major privileges vis-a-vis confidentiality, data safety and non-apathy. While educational centres assert that the technologies are important for achieving the objective of remote learning (distance education) and ensuring the integrity of tests and examinations, there has been agitation from examinees on whether institutions possess the right to process their private records without their consent or approval. There were also questions on the reconnaissance effect of virtual or online monitoring that can raise testing concerns in addition to diminishing confidence and student-institution collaborations. There is also fear about the methodological and communal prejudices which may be entrenched into the procedures which propel the technology, resulting in learners inexplicably ostracised and unfairly made to pay bills, through hypothetically discriminatory, chauvinist, ableist, and hetero-centrist norms.

Schools have also been adopting biometric systems for registration and confirmation of the identity of students to achieve cashless catering systems, automated registration of students' arrival in school and school library automation (Bryce et al, 2010). Attentions are also being shifted to using fingerprints, iris prints, voice prints and facial recognition systems for enhanced control, monitoring and administration in non-educational and educational settings. It is also noted that smart and intelligent operational environments now constitute the major application areas of pervasive computing, hence personal authentication approach based on uni-modal or multi-modal biometrics now features in the establishment of a secured verification method for real-time monitoring of patients and those working in telemedicine environments (Mohsin, 2018). Biometrics is also being adopted for the psychometric remote monitoring of patients associated with major adverse cardiac events (MACE) risk biomarkers. It is also being used for remote monitoring of access control, clinical trials, research and attendance tracking in healthcare facilities to achieve accurate identification, and streamlined administrations, among others (Shufeit *et al.,* 2020).

Biometrics is equally being used in law enforcement through a series of Automated Biometric Identification Systems (ABIS) which create and store biometric information that matches biometric templates for the face, finger, and/or iris. There are face-based surveillance or recognition systems for real-time or post-event monitoring with much interest and acceptance in cities, airports, borders, or other sensitive places such as stadiums and worship centres. There are also series of faces, irises, fingerprints, and DNA data that form the existing biometric identification systems for the use of various defence Agencies across the world in the tracking of criminals and enforcement of law and order. In the border control, travel, and migration sectors, there are biometric passports (based on the adoption of fingerprints and facial images) that help in achieving speedy border crossing processing, check-ins and bag-drop solutions as well as high levels of security. Digital fingerprints, photos, and iris scans are also being combined for higher recognition reliability in civil identity, population and voters' registration, public subsidy, unemployment benefit schemes, and payment schemes with attendant solutions to **c**orruption and high cost of delivery of public services. Biometrics adopted for monitoring and control in commercial applications is also noted. There exists a mandatory biometrics-based process for Banks, financial technology organizations, and telecommunication operators, among others to periodically identify and verify customer's identity in the fight against financial crime, money laundering, impersonations and slash account takeover fraud (ATO). Conclusively, the points raised in this section underscore the prevailing yearning and craving for remote invigilation with robustness and efficiency among its principal requirements.

Existing Challenges

Observed problems of the existing modes of e-proctoring for control and monitoring at various levels of examinations and assessments include effort demand and cost intensiveness as several proctors are required to monitor the examinees. In cases of examination monitoring, proctors often experienced a limited vision, hence being unable to observe all cheating strategies, like notes laying, peeking and unlawful information exchange. In cases where a remote proctor may pass some instructions via the webcam, there is the resultant effect of undue pressure and stress on the test taker in addition to the likelihood of revealing intimate information in privacy. The existing surveillance camera-based remote proctored examination systems also require well-established infrastructure such as software, hardware and a stable internet connection on both the examinee and organizer's sides. There is a substantial body of research that tries to establish how the adoption of some face-based technologies poses some threats to some groups as well as better detection of light-skinned people than dark-skinned people and men than women. This assertion has raised concerns that the female gender women or students of colour will inexplicably and unfairly accept the imports of these technologies. Students with poor

accessibility, learning disabilities, neuro-divergence, anxiety; low-income, transgender and rural conditions are also at the risk of discrimination (Colonna, 2021; Kharbat and Daabes, 2021; Barker; 2020). Bohmer et al. (2018) outlined common issues with remotely monitored examinations including complexity in the monitoring of examinees, lack of secured authentication process, lack of academic integrity on the part of the personnel, and privacy and data security breaches. It has also been established that in some cases, the process is complex, tasking and time-demanding. Furthermore, there are cases of lack of expert knowledge for the setting up, conduct and administration of the online examinations on the part of staff and students which often results in anxiety. There are also issues such as poor internet connection, ageing hardware, software compatibility and power failure. These problems became less common as students used the remote invigilation service more. Some students found navigating the online exam environment challenging which put them off in online exams (Frankl and Bitter; 2012; Davis, Rand and Seay et al., 2016; Cramp et al., 2019; Wibowo et al. 2016). This shortcoming motivated the need to complement the live monitoring technology with virtual or AI proctoring that is fitted with measures for scientifically recognizing signs and clues of likely infractions (Aiman et al., 2020; Langenfeld, 2020; Colonna, 2021).

Future Expectations

Bicz (2023) envisaged the future development of more remote invigilation technologies that can recognize people by observing their behaviours. The emergence of such technologies will create a variety of different approaches, even in relatively simple devices and with full integration of multimodal biometrics. Contactless voice, face, and body shape recognition among others are very much expected and special roles will be played by software with capacities to evaluate hominoid behavior and knowledge in a manner that resembles human beings. According to recent research by ROGO (2023), the majority of assessment stakeholders have a positive disposition toward remote online assessment and hope for better-than-experienced frameworks, relatively straightforward, and greater convenience and infraction-free test methodologies. There are also expectations on how the online assessment platforms could be improved from technical details to more flexibility through the adoption of voice, live chat support, study advice, live invigilation, environmental control, Internet restrictions and test times flexibility. Colonna (2021) also posited that Artificial Intelligence (AI), virtual reality and data analytics, could take online assessment platforms to the next level. AI could be useful in areas such as the mark of examinations, providing quicker test results based on word recognition and unbiased testing. Patterns of testing behaviour are also expected to help combat plagiarism and endorsement of examinees' identities. The rising trend of virtual reality and its associated platforms will ultimately propel examinations to ‘existent virtual’ environments from students’ homes, leading to the emergence of more practical examinations. Expectedly, e-assessment platforms will experience increased diversity assessment methods, with better prospects for personalized assessment formation. Though Internet access is currently unrelated to the online assessment, it is expected that necessities will be placed on it in the future to stand the impacts of high-tech failures during the assessment. Hopefully, platform providers will prioritize user know-how while constructing fresh software that will encompass structures for integration, and exportation, among others. Notably, the demand for online assessments will continue to increase, leading to growth opportunities inform of market expansions and diversifications (Rogo, 2023; Dawson, 2023).

CONCLUSION

A critical assessment of the existing and predicted states of e-invigilation of examinations has been presented. The focus was on the review of some current related works which emphasized the motivations, objectives, methodologies, results, contributions to knowledge and limitations. The failure of the traditional and human-based invigilation systems was greatly emphasized alongside the urgency in putting in place safer security measures. It was also revealed that significant gaps still exist in the areas of attaining CBE systems that are fool-proof and infraction-free. The study on the current state of biometrics-based e-invigilation across the world established its wide deployment and acceptance, though not without some challenges. The challenges include capital intensiveness, lack of political will and expertise, methodological failure, undue manipulation, and subjectivity. It was also established that the adoption and deployment of technology for remote/human-less invigilation of examinations is confronted with the issues of privacy intrusion, and discrimination against some sections of the populations, notably the disabled, lack of integrity, poor network connectivity and hardware and

software incompatibility. The study also revealed increased adoption of remote invigilation based on a variety of techniques and emerging technologies that will create several e-invigilation approaches, even with relatively simple devices and with full integration of multimodal biometrics. Contactless voice, face, and body shape recognition among others are being envisaged to play special roles alongside software with capacities to evaluate hominoid behavior and knowledge in a manner that resembles human beings. Based on these findings, further research will focus on the baseline studies of assessment, examinations and remote invigilation. Focus will also be on the formulation of techniques and models that will improve on the accuracy and performance of the existing e-proctoring methods.

Availability Of Data

Not Applicable

Competing Interests

The authors declare that there are no conflicts of interests

FUNDING

The support of the Nigerian government through the National Tertiary Research Trust Fund (TETFund) towards the success of this study is greatly acknowledged.

Authors Contributions

All the authors contributed to the review, documentation and proofreading

ACKNOWLEDGEMENT

The noble roles played by the Centre for Research and Development (CERAD), The Federal University of Technology, Akure, Nigeria are greatly acknowledged.

REFERENCES

1. Abubakar, A. S., and Adebayo, F. O. (2014). Using Computer-Based Test Method for the Conduct of Examination in Nigeria: Prospects, Challenges and Strategies. Mediterranean Journal of Social Sciences, MCSER, 5(2)
2. Aiman A. T., Jawad H. A. & Abdulrahman A. A. (2020). Students Online Exam Proctoring: A Case Study Using 360 Degree Security Cameras, Emerging Technology in Computing, Communication and Electronics, 1–5
3. Akingbade, O. L. & Eze, B. E. (2022). Enhanced Computer Based Examination System with Fingerprint Authentication, International Journal of Advances in Engineering and Management, 4(11), 64-70
4. Assaf W., Elia G., Fayyoumi A., & Taurino C. (2007). The prospect of e-Learning: The Case of Jordan". e-Society IADIS Multi Conference on Computer Science and Information Systems, Lisbon, 5(4): 414-424,3-8 July 2007
5. Balogun, T. E. (2023). Framework for Enhancing Security in Computer-Based Examinations Using a Multimodal Biometrics-Supervision System. Benin Journal of Advances in Computer Science. 8(2), 29-39.
6. Baneres, D., Baro, X., Guerrero-Roldan, A., & Rodrıguez, M. (2016). Adaptive e-assessment system: a gen eral approach. International Journal of Emerging Technologies in Learning, 11, 16–23.
7. Barker A. (2020). Big Brother is Proctoring You, The Daily Texan, http://thedailytexan.com/2020/09/23/big-brother-is-proctoring-you/ (accessed April 27, 2021).
8. Bicz W. Homeland Security, Biometric Identification and Personal Detection Ethics https://cordis.europa.eu/project/id/217762

9. Bohmer C., Feldmann N., & Ibsen M. (2018). E-exams in engineering education-Online testing of engineering competencies: experiences and lessons learned', IEEE Global Engineering Education Conference. 571-576
10. Bryce T. G.K., Nellis M., Corrigan A., Gallagher H., Lee P., & Sercombe H. (2010). Biometric Surveillance in Schools: Cause for concern or case for curriculum?, Scottish Educational Review, 42 (1), 3-22.
11. Butler-Henderson, K., & Crawford, J. (2020). A systematic review of online examinations: A pedagogical innovation for scalable authentication and integrity. Computers & Education, 159, 104024. doi: https://doi.org/10.1016/j.compedu.2020.104024
12. Chi-Chien P. (2004). Secure Online Examination Architecture Based on Distributed Firewall, e-technology, e-Commerce and e-Service, 2004 IEEE International Conference on, 28-31 March 2004, 533-536
13. Clarke, N.L., Dowland, P., & Furnell, S.M. (2013). E-Invigilator: A biometric-based supervision system for e Assessments. Proceedings of International Conference on Information Society. (pp. 238-242). Toronto, Canada.
14. Colonna L. (2021). Legal Implications of Using AI as an Exam Invigilator, https://www.diva-portal.org/smash/get/diva2:1657842/FULLTEXT01.pdf, (accessed 23/02/2023)
15. Cramp J., John F. Medlin, P. L., Sharp, C. (2021). Lessons learned from implementing remotely invigilated online exams, Journal of University Teaching & Learning Practice, 6(1)
16. Dawson P. (2020). Strategies for Using Online Invigilated Exams, onlinelearning@teqsa.gov.au
17. Elenwo P. M., & Nwanguma T. K. (2023). Electronic Invigilation Inclusion In Curbing Examination Malpractices Among Postgraduate Students In Selected Public Tertiary Institutions In Rivers State, British Journal of Education, Learning and Development Psychology, 6(2), 100-113
18. Kharbat F. K., & Daabes, A. S. A. (2021). E-proctored Exams during the COVID-19 Pandemic: A Close Understanding, Education and Information Technologies, (2021).
19. Giannopoulou A., Ducato R., Chiara A., & Giulia S. (2023). From data subjects to data suspects: challenging e-proctoring systems as a university practice, Jipitec, https://abdn.elsevierpure.com/en/publications/from-data-subjects-to-data-suspects-challenging-e-proctoring-syst, (accessed 23/11/2023)
20. Goswami S. K., & Bau S. K. (1991). Direct Solution of Distribution Systems, IEEE Proceedings-C 138(1), 78–88.
21. Hoque J. R. A. (2020). Automation of Traditional Exam Invigilation using CCTV and Bio-Metric, International Journal of Advanced Computer Science and Applications, 11(6)
22. Iwasokun G. B, & Akinyokun O. C. (2016), Singular-Minutiae Points Relationship-Based Approach to Fingerprint Matching, Artificial Intelligence Research, 5(1), 78-86
23. **Iwasokun G. B.**, Akinwonmi A. E. & Bello O. A. (2022): Baseline Study of COVID-19 and Biometric Technologies, International Journal of Sociotechnology and Knowledge Development, 14(1)
24. **Iwasokun G. B.**, Akinyokun O. C., Omomule T. G. (2019), Design of E-Invigilation Framework Using Multi-Modal Biometrics, 15th International Conference on Electronics Computer and Computation (ICECCO 2019), December 10-12, 2019, Nile University, Abuja, Nigeria (Nigeria)
25. Iwasokun, G. B., Omomule, T. G., & Akinyede, O. R. (2018). Design of a Framework for Computer-Based Examination Invigilation Using Fingerprint and Iris Technologies. 2nd International Conference on Information and Communication Technology and Its Applications. Federal University of Technology, Minna, Nigeria, 2, 177-183.
26. Ketab S. S., Nathan L. C., & Paul S. A. (2017). Robust e-Invigilation System Employing Multimodal Biometric Authentication, International Journal of Information and Education Technology, 17
27. Ketab S. S., Clarke N. L., Dowland, P. S. (2016). The Value of the Biometrics in Invigilated E-Assessments, https://researchportal.plymouth.ac.uk/en/publications/the-value-of-the-biometrics-in-invigilated-e-assessments, (accessed 23/02/2023)
28. Kikelomo M. A, Wills G., & Argles D. (2010). User Security Issues in Summative E-Assessment Security, International Journal of Digital Society (IJDS), 1(2)
29. Langenfeld T. (2020). Internet-Based Proctored Assessment: Security and Fairness Issues, Educational Measurement: Issues & Practice, 24

30. Learning Light, Online Proctoring / Remote Invigilation – Soon a Multibillion Dollar Market within eLearning & Assessment, https://www.learninglight.com/remote-proctoring-invigilation-market/
31. Minott M. A. (2020). Computer-based examinations: unearthing exam invigilators' perspectives, tacit work-related knowledge, and skills via reflection-on-experience, Journal of Perspectives in Applied Academic Practice
32. Mohsin A. H., Zaidan A. A., Zaidan, B. B., Albahri, A. S., Albahri O. S., Alsalem, M. A., & Mohammed K. I. (2018), Real-Time Remote Health Monitoring Systems Using Body Sensor Information and Finger Vein Biometric Verification: A Multi-Layer Systematic Review, Journal of Medical Systems, 42:238 https://doi.org/10.1007/s10916-018-1104-5
33. Okada, A.; Whitelock, D.; Holmes, W., & Edwards, C. (2019). e Authentication for online assessment: A mixed-method study. British Journal of Educational Technology, 50(2), 861–875.
34. Ricketts C., Filmore P., Lowry R., & Wilks S. (2009). How should we measure the costs of computer aided assessment? Proceedings 7th Computer Assisted Assessment Conference, Loughborough University, UK,. [viewed 11 Aug 2009] http://hdl.handle.net/2134/1924
35. Ketab S. S., Clarke N.L., Dowland P. S. (2015). E-Invigilation of E-Assessments, Proceedings of INTED2015 Conference 2nd-4th March 2015, Madrid, Spain
36. Shufelt C. L.; Cheng S.; Kim A., Joung S., Barsky L., Arnold C., Dhawan S., Fuller G., Speier W., Lopez M., Mastali M., Mouapi K., van den Broek I., Wei J., Spiegel B., Van Eyk J. E., & Bairey-Merz C. N. (2020). Biometric and Psychometric Remote Monitoring and Cardiovascular Risk Biomarkers in Ischemic Heart Disease, Journal of the American Heart Association, https://www.ahajournals.org/doi/10.1161/JAHA.120.016023 (accessed 23/02/2023)
37. The ROGO (2023). The Future of e-Assessment: Where will we be in 2027? https://eintech.com/wp-content/uploads/2022/09/Rogo-Market-Analysis-Report-v1.5.pdf
38. Von-Schomberg, R. (2011). Prospects for technology assessment in a framework of responsible research and Innovation (pp. 39–61). Wiesbaden, Germany: Springer.
39. Wales J., & Baraniuk R. (2017). Technology opens the doors to global classrooms, The Australian, 2-3 February, 2017, p. 27.