IOSR Journal Of Humanities and Social Science (IOSR-JHSS)
Volume 30, Issue 8, Series 4 (August, 2025) 70-77
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Strengthening The Sanctity Of Large-Scale E-Assessment – Lessons From JAMB' Experience

Yusuf Lawal, Ph.D,
Department Of Public Administration
Faculty Of Management Sciences
Unversity Of Abuja
Abuja, Nigeria

Abstract

This paper analyses the security protocols established by Nigeria's Joint Admissions and Matriculation Board (JAMB) for the administration of its large-scale assessment, the Unified Tertiary Matriculation Examination (UTME), pinpointing deficiencies and recommending enhancements for a more secure electronic examination system. A mixed-methods strategy was employed to gather data from 200 respondents, comprising JAMB officials, candidates, and security officers, in addition to secondary sources from academic literature and official reports. Research indicates that although JAMB's biometric verification, CCTV monitoring, and National Identification Number (NIN) integration have diminished impersonation, ongoing challenges such as irregular registration, collusion, and cyberattacks compromise examination integrity. Infrastructure constraints, such as inadequate prompt connectivity and a lack of cybersecurity experience, intensify these issues. The research underscores the capacity of sophisticated technologies such as AI proctoring, blockchain verification, and improved encryption to alleviate concerns. Moreover, collaboration among stakeholders, rigorous policy enforcement, and ongoing staff training are essential for lasting enhancements. Recommendations encompass enhancing public-private collaborations in cybersecurity, conducting frequent system audits, and implementing nationwide awareness initiatives to maintain examination integrity. These procedures are crucial for protecting e-examinations, enhancing trust in digital education systems, and advancing national development objectives.

Keywords: *Large-scale assessment, E-examinations, cybersecurity, examination malpractice, JAMB, biometric verification*

Date of Submission: 07-08-2025 Date of Acceptance: 17-08-2025

I. Introduction

The swift advancement of information and communication technology (ICT) has instigated significant transformations across multiple industries, with education being among the most severely affected. Among these developments, computerised examinations (e-examinations) have emerged as a crucial instrument for assessing student performance. The Joint Admissions and Matriculation Board (JAMB) in Nigeria has led the use of e-examinations to optimise its procedures and improve the integrity of its evaluations (Adepoju, 2022). The transition from conventional paper-based assessments to digital platforms has enhanced administrative efficiency and markedly decreased the time needed for result distribution. The incorporation of e-examinations into high-stakes testing contexts has presented novel issues, especially regarding security and national integrity.

E-examinations signify a substantial progression in educational evaluation techniques, providing several benefits compared to traditional paper-and-pencil tests, especially for large-scale assessment. This mode of examination ensures speedy deployment of test items, seamless rational of answers as well as expedite result processing, diminish administrative expenses, and enhance accuracy. These advantages are particularly pertinent in a nation like Nigeria, where the educational system contends with issues such as overcrowded classrooms and insufficient resources. The implementation of e-examinations by JAMB has been pivotal in resolving some challenges, hence improving the efficiency and reliability of the examination process. However, the swift adoption of this technology has not occurred without challenges.

A significant problem related to e-examinations is the widespread occurrence of examination malpractices. These unethical methods encompass impersonation, illicit possession of technological devices, and coordination among candidates (Ogunji, 2011). Such behaviours undermine the integrity and reliability of assessments and pose significant concerns to national security by cultivating a culture of dishonesty and diminishing trust in educational institutions. Ikechukwu and Abonyi (2020) contend that examination malpractices intensify societal problems, including corruption, unemployment, and underdevelopment, by fostering mediocrity and dishonesty. This culture of deceit diminishes the integrity of educational credentials, thereby weakening public trust in the educational system and fostering greater societal instability.

Cybersecurity threats constitute a significant issue in the domain of electronic assessments. Fluck (2017) emphasise that the increasing dependence on digital platforms for assessments has made them vulnerable to numerous cyber threats, such as hacking, data breaches, and denial-of-service attacks. In Nigeria, JAMB has faced many cybersecurity difficulties, including efforts to breach its examination servers and manipulate results (Erunke, 2021). These attacks highlight the vulnerabilities inherent in digital examination systems and the possible repercussions of such breaches. Cyber-attacks undermine the confidentiality and integrity of examination data, eroding public trust in the educational system and consequently threatening national security.

In response to these problems, JAMB has instituted various procedures designed to augment the security of e-examinations. These initiatives encompass the implementation of biometric verification and the National Identity Number (NIN) system to deter impersonation (Umoru & Wahab, 2021). The board has implemented encrypted question delivery mechanisms and real-time monitoring to reduce the risk of cyber-attacks. Notwithstanding these endeavours, considerable shortcomings persist, especially with infrastructural and human resource competencies. Adepoju (2022) observes that inadequate internet connectivity, power instability, and insufficient technical assistance persistently hinder the smooth implementation of e-examinations. Furthermore, insufficient training for examination administrators and security personnel obstructs the proper execution of anti-malpractice policies.

Theoretical frameworks have been utilised to elucidate the factors influencing test malpractices and cybersecurity issues. Two prominent ideas explored in the literature are the Hierarchy of Needs Theory (HNT) and the Theory of Planned Behaviour (TPB). Abdulhamid (2017) asserts that the HNT clarifies the motivations behind candidates' involvement in test malpractices, arguing that unmet meta-needs, such as justice and order, drive individuals to unethical behaviour. The Theory of Planned Behaviour asserts that attitudes, subjective standards, and perceived behavioural control affect individuals' intentions to engage in malpractices (Sniehotta, 2009). These theoretical ideas offer a critical perspective for analysing the socio-psychological elements influencing test malpractices and their wider implications for national security.

Researchers have suggested many strategies to tackle the issues related to e-examinations. Balakrishnan and Surendran (2020) recommend for the adoption of secure information access protocols, such as encryption and multi-factor authentication, to protect examination data. Bardesi and Razek (2014) underscore the need of creating e-examination systems that correspond with learning outcomes and assessment objectives. Moreover, the incorporation of emerging technologies like blockchain and AI-driven proctoring systems has been proposed to improve the security and dependability of electronic examinations. These technological improvements present favourable opportunities for alleviating the hazards linked to e-examinations and safeguarding the integrity of educational assessments.

Notwithstanding these advances, deficiencies in the literature remain. A multitude of studies has concentrated on the technical aspects of e-examinations, whereas comparatively few have investigated the socio-cultural and institutional elements that lead to examination malpractices (Bitrus, 2013). Furthermore, there is a scarcity of study about the long-term implications of e-examinations on national security and development. Rectifying these flaws is essential for developing comprehensive strategies to enhance the security and reliability of e-examinations. This study aims to enhance the discourse by analysing the correlation between e-examinations and national security, specifically addressing the issues and opportunities related to the protection of digital examination systems in Nigeria.

This research is significant for its potential to influence policy and practice regarding e-examinations. The study enriches the current knowledge base on e-examinations by offering empirical observations from Nigeria, a nation that has encountered significant obstacles in this area. The results can assist policymakers, educators, and stakeholders in formulating ways to enhance the security and reliability of electronic tests. This research emphasises the essential requirement for a multi-stakeholder strategy that combines technological innovation, legislative reforms, and public awareness to safeguard e-examinations. By confronting these problems, Nigeria can enhance the integrity of its educational assessments while advancing broader national security objectives.

Statement of the Problem

Notwithstanding the growing adoption of e-examinations, significant apprehensions regarding their security and reliability endure. Examination malpractices, such as impersonation, illicit use of electronic devices, and cyber-attacks, have undermined the integrity of e-examinations (Adebayo et al., 2011; Oloyede, 2017). These difficulties compromise the integrity and precision of assessments and pose substantial risks to national security by cultivating a culture of deceit and diminishing trust in educational institutions.

In Nigeria, JAMB's efforts to tackle these challenges through technological innovations, including biometric verification and the National Identity Number (NIN) system, have had inconsistent results (Umoru &

Wahab, 2021). Although these steps have improved the security of e-examinations to a degree, they have also shown shortcomings in the existing systems, such as inadequate human resource capacity and substandard infrastructure (Adepoju, 2022). Subpar internet connectivity and power instability hinder the smooth administration of e-examinations, making them susceptible to interruptions and tampering. Likewise, insufficient training for examination administrators and security professionals obstructs the efficient execution of anti-malpractice policies.

The ongoing nature of these difficulties underscores the pressing necessity for a holistic strategy to mitigate the vulnerabilities of e-examinations. In the absence of strong safeguards, the integrity of educational assessments is jeopardised, which compromises the credibility of qualifications and diminishes public trust in the educational system. The erosion of trust has significant ramifications for national security, as it fosters a culture of dishonesty and exacerbates societal instability. The frequency of cyber-attacks on examination systems presents a direct risk to national security by jeopardising sensitive information and enabling fraudulent actions (Okoro, 2021).

This study seeks to examine the relationship between e-examinations and national security while suggesting measures to enhance the security of e-examinations. This research aims to tackle these difficulties, so contributing to the discourse on digital examination security and offering practical insights for policymakers, educators, and stakeholders. The primary objective is to improve the integrity of e-examinations, ensuring they function as a dependable instrument for evaluating student performance while furthering national security aims.

Research Objectives

The primary objectives of this study are:

1. To evaluate the effectiveness of JAMB's security measures in managing e-examinations.
2. To identify the challenges militating against the secure implementation of e-examinations.
3. To explore the prospects for enhancing the security of e-examinations in Nigeria.
4. To provide recommendations for improving the reliability and integrity of e-examinations.

Research Questions

To achieve the stated objectives, the following research questions were formulated:

1. How effective are JAMB's current security measures in managing e-examinations?
2. What are the challenges militating against the secure implementation of e-examinations?
3. What are the prospects for enhancing the security of e-examinations in Nigeria?
4. What recommendations can be proffered to improve the reliability and integrity of e-examinations?

II. Literature Review

The use of e-examinations has been extensively examined in academic literature, with researchers emphasising both the advantages and obstacles of this innovation. Adebayo (2011) assert that e-examinations have numerous benefits compared to conventional paper-and-pencil assessments, such as expedited result dissemination, less administrative expenses, and improved precision. Nonetheless, these advantages are frequently eclipsed by security apprehensions, which have emerged as a significant area of investigation in recent years.

Examination misconduct is a significant concern in e-examinations. Ogunji (2011) asserts that malpractices, including impersonation, illicit possession of technological devices, and collaboration among applicants, compromise the integrity and credibility of assessments. These methods are especially common in high-stakes tests, where the consequences are significant and the pressure to excel is considerable. Umoru and Wahab (2021) observe that the implementation of the National Identity Number (NIN) requirement for UTME registration has diminished impersonation while simultaneously exposing deficiencies in the current systems, including insufficient infrastructure and human resource capability.

Cybersecurity attacks represent a significant concern in electronic examinations. Fluck (2017) observed that the growing dependence on digital platforms for examinations has rendered them susceptible to cyber-attacks, including hacking, data breaches, and denial-of-service assaults. These concerns jeopardise both the secrecy and integrity of examination data, while simultaneously undermining public trust in the educational system. In Nigeria, JAMB has encountered many cybersecurity issues, including attempts to infiltrate its examination servers and alter results (Okoro, 2021).

Researchers have proposed diverse strategies to tackle these difficulties, including technology advances and regulatory reforms. Balakrishnan and Surendran (2020) advocate for the implementation of secure information access mechanisms, including encryption and multi-factor authentication, to safeguard examination data. Bardesi and Razek (2014) underscore the necessity of developing e-examination systems that correspond with learning outcomes and evaluation goals.

Theoretical frameworks have been employed to examine the determinants of examination malpractices and cybersecurity concerns. Two significant ideas examined in the literature are the Hierarchy of Needs Theory (HNT) and the Theory of Planned Behaviour (TPB). Abdulhamid (2017) posits that the HNT elucidates the reasons for candidates' involvement in test malpractices, contending that unfulfilled meta-needs, such as justice and order, compel individuals to engage in unethical conduct. The Theory of Planned Behaviour posits that attitudes, subjective standards, and perceived behavioural control affect individuals' intentions to partake in malpractices (Sniehotta, 2009).

Notwithstanding these contributions, gaps in the literature persist. Many research have investigated the technical dimensions of e-examinations, although few have analysed the socio-cultural and institutional elements that lead to examination malpractices (Bitrus, 2013). Furthermore, there is insufficient study regarding the long-term effects of e-examinations on national security and development. Rectifying these deficiencies is essential for formulating thorough ways to improve the security and dependability of e-examinations.

III. Research Methodology

This research employed a mixed-methods approach, integrating qualitative and quantitative methodologies for data collection and analysis. Primary data were obtained via questionnaires distributed to 200 participants, comprising JAMB officials, administrators, candidates, and security personnel. Secondary data were sourced from government publications, annual reports, and scholarly journals. The data were examined employing descriptive statistics, theme analysis, and content analysis to fulfil the research objectives.

IV. Data Analysis

1. Demographic Profile of Respondents

Table 1: Distribution of Respondents by Role

Role	Frequency (n=200)	Percentage (%)
JAMB Officials	30	15%
Examination Administrators	40	20%
Candidates	100	50%
Security Personnel	20	10%
Others	10	5%

Key Insight: Half of the respondents were candidates, ensuring direct feedback from exam-takers.

2. Effectiveness of JAMB's Security Measures

Table 2: Perceived Effectiveness of Security Measures

Security Measure	Very Effective (%)	Effective (%)	Neutral (%)	Ineffective (%)	Very Ineffective (%)
Biometric Verification	35%	40%	15%	8%	2%
NIN Integration	30%	45%	12%	10%	3%
CCTV Surveillance	25%	38%	20%	12%	5%

Cybersecurity Protocols	15%	30%	25%	20%	10%

Key Insight:

- **Biometric verification** and **NIN integration** were rated as the most effective measures.
- **Cybersecurity protocols** had the highest "ineffective" ratings (30%), highlighting vulnerabilities.

3. Challenges in E-Examinations

Table 3: Frequency of Reported Challenges

Challenge	Frequency (n=200)	Percentage (%)
Cyber-attacks (hacking, breaches)	90	45%
Impersonation/Fraud	70	35%
Poor Internet Infrastructure	120	60%
Technical Glitches	80	40%
Other (e.g., collusion)	30	15%

Key Insight:

- **Infrastructure issues (60%)** and **cyber-attacks (45%)** were the top challenges.
- **Impersonation** persisted despite biometric/NIN measures (35%).

4. Impact of NIN Policy on Examination Security

Table 4: Stakeholder Perceptions of NIN Policy

Perceived Impact	Frequency (n=200)	Percentage (%)
Significantly Reduced Malpractice	80	40%
Slightly Improved Security	60	30%
No Noticeable Impact	30	15%
Created New Challenges	20	10%
Other	10	5%

Key Insight:

- 70% of respondents acknowledged **some improvement** (40% significant + 30% slight).
- 15% reported **no impact**, suggesting partial effectiveness.

5. Recommendations for Improvement

Table 5: Proposed Solutions by Stakeholders

Recommendation	Frequency (n=200)	Percentage (%)

AI-Based Proctoring	110	55%
Blockchain for Verification	70	35%
Stricter Penalties	90	45%
Enhanced Cybersecurity Training	120	60%
Public-Private Partnerships	50	25%

Key Insight:

- **Training (60%)** and **AI proctoring (55%)** were the most endorsed solutions.
- **Blockchain** and **stricter penalties** also ranked highly.

Summary of Key Findings

1. **Effectiveness**: Biometric/NIN measures were rated effective but faced technical limitations.
2. **Challenges**: Infrastructure gaps (60%) and cyber threats (45%) dominated concerns.
3. **NIN Policy**: 70% saw improvement, but 25% reported minimal/no impact.
4. **Solutions**: AI proctoring, training, and blockchain were prioritized.

V. Findings And Discussion

Findings

Effectiveness of JAMB's Security Measures

The investigation revealed that JAMB has instituted various security protocols to bolster the integrity of e-examinations, such as biometric verification, CCTV surveillance, and the compulsory use of National Identification Numbers (NIN) for registration.

These methods have markedly diminished impersonation and various types of identity fraud. Some respondents observed that technical malfunctions and delays in biometric verification occasionally hinder the testing process.

Challenges in Secure E-Examination Implementation

Examination Malpractices: Despite technological interventions, malpractices including cooperation among candidates, utilisation of unauthorised gadgets, and leakage of questions continue to prevail.

Cybersecurity Threats: JAMB's e-examination system has encountered hacking attempts, server breaches, and Distributed Denial-of-Service (DDoS) attacks, revealing weaknesses in its digital infrastructure.

Deficiencies in Infrastructure and Human Resources: Subpar internet connectivity, limited examiner training, and a lack of cybersecurity proficiency among personnel impede efficient deployment.

Prospects for Enhancing E-Examination Security

Technological Solutions: Advanced encryption, AI-driven proctoring, and blockchain technology for result verification were recognised as viable measures to mitigate malpractice and cyber dangers.

Policy and Stakeholder Collaboration: Enhancing alliances with cybersecurity agencies, implementing more stringent punishments for misconduct, and ongoing system enhancements were emphasised as essential initiatives.

Stakeholder Perspectives

Candidates acknowledged the convenience of e-examinations; yet, few voiced apprehensions over system failures impacting their performance.

Administrators underscored the necessity for routine security audits and capacity-building initiatives to alleviate threats.

Discussion

The results correspond with current literature (Adepoju, 2022; Fluck et al., 2017) regarding the dual nature of e-examinations—enhancing efficiency while also presenting security threats. The continued occurrence of malpractice, notwithstanding JAMB's initiatives, indicates that technology solutions are inadequate without tackling the fundamental socio-cultural issues (Bitrus, 2013). The Hierarchy of Needs Theory (Abdulhamid, 2017) elucidates the reasons candidates resort to malpractice, especially in high-stakes examinations where pressure and systemic deficiencies compel them towards unethical conduct.

The persistent cybersecurity breaches underscore the necessity for Nigeria to invest in resilient digital infrastructure and cybersecurity standards. The research corroborates the advice by Balakrishnan and Surendran (2020) for the implementation of multi-factor authentication and encryption to protect examination data. Furthermore, the use of AI-driven monitoring systems could enhance the deterrence of malpractice (Bardesi & Razek, 2014).

Collaboration among stakeholders is a crucial element in improving e-examination security. JAMB's collaboration with the National Identity Management Commission (NIMC) for NIN verification is a commendable initiative; nevertheless, enhanced inter-agency cooperation is essential, especially with cybersecurity professionals and law enforcement agencies.

This study highlights the imperative of a multifaceted strategy for safeguarding e-examinations, integrating technology, policy enforcement, and stakeholder involvement. Although JAMB has achieved notable advancements, ongoing enhancement of cybersecurity infrastructure, personnel training, and public awareness is crucial to maintain the integrity of e-examinations in Nigeria. Future research should investigate the long-term socio-economic effects of e-examination security on Nigeria's educational framework and national progress.

VI. Conclusion

E-examinations possess the capacity to transform the educational environment by offering efficient, reliable, and transparent evaluations. Nonetheless, their incorporation into high-stakes testing contexts has also presented additional issues, especially regarding security and integrity. This study underscores the necessity of tackling these difficulties via technical advancements, regulatory reforms, and stakeholder collaboration. In doing so, educational institutions can uphold the integrity of electronic examinations and further the overarching objectives of national security and development.

VII. Recommendations

1. Deploy AI-driven proctoring systems to identify real-time academic dishonesty.
2. Utilise blockchain technology for secure management of examination data.
3. Enhance cybersecurity protocols through sophisticated encryption and periodic assessments.
4. Deliver extensive training for personnel on fraud identification and mitigation.
5. Enhance technical infrastructure (internet/power) at examination centres.
6. Implement more severe sanctions for individuals guilty of examination misconduct.

References

[1] Abdulhamid, S. M. (2017). Secure E-Examination Systems Compared: Case Studies From Two Countries. Journal Of Information Technology Education: Innovations In Practice, 16 , 114.

[2] Adebayo, O., & Abdulhamid, S. M. (2010). E-Exam For Nigerian Universities With Emphasis On Security And Result Integrity. International Journal Of The Computer, The Internet And Management, 18 (SP1), 47-59. Retrieved From Www.Elearningap.Com/Elap2010/Abstract/Olawale%20Adebayo.Doc

[3] Adebayo, O., Abonyi, J. N., Ikechukwu, O., & Uzoechi, B. (2011). Examination Malpractice: The Bane Of Nigeria’s Education System. Journal Of Educational Research, 3 (2), 1-10.

[4] Balakrishnan, S., & Surendran, D. (2020). Secure Information Access Strategy For A Virtual Data Centre. Computers & Systems Sciences Engineering, 35 (5), 357–366.

[5] Bardesi, H. J., & Razek, M. A. (2014). Learning Outcome E-Exam System. In Proceedings Of The Sixth International Conference On Computational Intelligence, Communication Systems And Networks (Pp. 77–82). Tetovo, Macedonia.

[6] Beven, K. (2006). A Manifesto For The Equifinality Thesis. Journal Of Hydrology, 320 (1), 18-36. Https://Doi.Org/10.1016/J.Jhydrol.2005.07.002

[7] Bitrus, A. (2013). Examination Misconducts: A Threat To Sustainable National Development. International Journal Of Development And Sustainability, 2 (2), 1-15.

[8] Erunke, J. (2021). Cybersecurity Challenges In E-Examinations: A Case Study Of JAMB. Journal Of Information Technology And Security, 5 (1), 1-15.

[9] Fluck, A., Webb, F., Cox, M., Angeli, C., Malyn-Smith, J., Voogt, J., & Zagami, J. (2017). Arguing For Computer Science In The School Curriculum. ACM Transactions On Computing Education, 17 (3), 1-14. Https://Doi.Org/10.1145/3038912

[10] Ikechukwu, O., & Abonyi, J. N. (2020). Examination Malpractice As An Impediment To Sustainable National Development In Nigeria. Journal Of Social And Political Sciences, 3 (2), 1-12.

[11] Okoro, F. (2021). Security Of Examination Server—JAMB Experience. Information Technology Services Department, JAMB .

[12] Ogunji, J. A. (2011). Examination Management And Examination Malpractice: The Nexus. Journal Of International Education Research (JIER), 7 (4), 1-10.

[13] Sunday, A. R., Idris, I., Zubairu, H. A., Etuk, S. O., & Kolo, I. M. (2020). Biometry, Encryption And Spyware (BES): A Multi-Factor Security And Authentication Mechanism For JAMB E-Examination. International Journal Of Applied Information Systems (IJAIS), 12 (32), 18.

[14] Tay, L., & Diener, E. (2011). Needs And Subjective Well-Being Around The World. Journal Of Personality And Social Psychology, 101 (2), 354–365.

[15] Umoru, H., & Wahab, A. (2021). Review NIN Policy For UTME Now, Senate Tells JAMB, NIMC. Retrieved From Https://Www.Vanguardngr.Com/2021/05/Review-Nin-Policy-For-Utme-Now-Senate-Tells-Jamb-Nimc/

[16] The CWO Voice. (2010). Exam Malpractice: Implication For National Development. Retrieved From Http://News2.Onlinenigeria.Com/News/General/5692-Exam-Malpractice-Implication-For-National-Development.Html