IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN:2278-487X, p-ISSN: 2319-7668. Volume 27, Issue 8. Ser. 5 (August. 2025), PP 09-16
www.iosrjournals.org

E-Examinations And National Security: Challenges And Prospects

Yusuf Lawal Phd[1], Modupeola Adepoju[2], & Ademeso Tosin Success Phd[3]
Department Of Public Administration, Faculty Of Management Sciences, University Of Abuja, Abuja, Nigeria
Department Of Test Development, Joint Admissions And Matriculation Board, Abuja, Nigeria

Abstract
The swift implementation of electronic tests (e-examinations) in Nigeria, especially by the Joint Admissions and Matriculation Board (JAMB), has generated notable efficiency in educational assessments while concurrently elevating important national security issues. This paper investigates the convergence of e-examinations and national security, emphasising the problems and opportunities in safeguarding digital examination systems in Nigeria. The research employs a mixed-methods methodology, utilising primary data from questionnaires distributed to 200 stakeholders, including JAMB officials, administrators, candidates, and security officers, alongside secondary data from academic literature and institutional reports. Critical findings indicate that e-examinations encounter ongoing threats, such as examination malpractices (impersonation, collusion, and unauthorised device utilisation), cybersecurity breaches (hacking, data manipulation, and server assaults), and infrastructural inadequacies (substandard internet connectivity and power instability). These weaknesses undermine the integrity of evaluations and moreover provide significant threats to national security by promoting corruption, institutional distrust, and cybercrime. However, the research suggests implementable options, including blockchain technology for secure data management, AI-driven proctoring systems, enhanced policy enforcement, and capacity-building programs for examination administrators.

Keywords*: E-examinations, national security, JAMB, cybersecurity,*

Date of Submission: 04-08-2025 Date of Acceptance: 14-08-2025

I. Introduction

The emergence of technology has instigated significant transformations across all industries, with education being one of the most deeply affected areas. Among these developments, computerised examinations (e-examinations) have emerged as a crucial tool for assessing student performance. The Joint Admissions and Matriculation Board (JAMB) in Nigeria has been leading the use of e-examinations to streamline its procedures and improve the integrity of its evaluations (Adebayo et al., 2011). The shift from conventional paper-based tests to digital platforms has improved administrative processes and substantially decreased the time needed for result distribution. The integration of technology into high-stakes exams has presented additional concerns, especially with national security. Cyber-attacks, examination misconduct, and inadequate infrastructure threaten the integrity of e-examinations and, by extension, the nation's educational system and security framework.

E-examinations signify a substantial progression in educational assessment techniques, providing several benefits compared to traditional paper-and-pencil evaluations. Adebayo et al. (2011) assert that e-examinations enable rapid result distribution, save administrative costs, and enhance accuracy. These advantages are especially relevant in a nation such as Nigeria, where the educational system contends with numerous obstacles, including overcrowded classrooms and scarce resources. The implementation of e-examinations by JAMB has been pivotal in resolving some challenges, therefore improving the efficiency and reliability of the examination process. Nonetheless, the swift deployment of this technology has encountered certain disadvantages.

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 (Oloyede, 2017). Such behaviours undermine the integrity and trustworthiness of evaluations and pose substantial concerns to national security. Ikechukwu and Abonyi (2020) contend that test malpractices intensify societal problems, including corruption, unemployment, and underdevelopment, by promoting a culture of dishonesty and mediocrity. This culture of deceit diminishes the credibility of educational credentials, consequently weakening public trust in the educational system and contributing to greater societal instability.

Cybersecurity threats constitute a significant issue in the domain of electronic assessments. Fluck et al. (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 attempts to breach its examination servers and manipulate results

(Okoro, 2021). These attacks highlight the vulnerabilities inherent in digital examination systems and the potential ramifications of such breaches. Cyber-attacks undermine the confidentiality and integrity of examination data and erode public trust in the educational system, so constituting a direct threat to national security.

In response to these problems, JAMB has instituted various steps to bolster the security of e-examinations. These activities encompass the implementation of biometric verification and the National Identity Number (NIN) system to avert 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, substantial shortcomings persist, especially with infrastructural and human resource competencies. Adepoju (2022) observes that inadequate internet connectivity, power inconsistencies, and insufficient technical assistance persistently hinder the smooth administration 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. Bardes and Razek (2014) underscore the imperative of creating e-examination systems that correspond with educational objectives and assessment aims. 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 technical innovations 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. Numerous research have 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 devising 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 due to 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 over 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 mitigate these challenges through technological innovations, including biometric verification and the National Identity Number (NIN) system, have shown varied 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 proper execution of anti-malpractice policies.

The ongoing nature of these difficulties underscores the critical necessity for a holistic approach to mitigate the vulnerabilities of e-examinations. In the absence of strong protections, the integrity of educational assessments is jeopardised, compromising the authenticity of qualifications and diminishing 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. Moreover, the frequency of cyber-attacks on examination systems constitutes a direct threat to national security by jeopardising important information and enabling fraudulent operations (Okoro, 2021).

This study seeks to examine the relationship between e-examinations and national security, while offering recommendations to enhance the security of e-examinations. This research aims to tackle these difficulties, 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 examine the relationship between e-examinations and national security.
2. To evaluate the role of JAMB in managing examination security in Nigeria.
3. To identify the challenges militating against the effective implementation of e-examinations.
4. To explore the prospects for improving the security of e-examinations in Nigeria.

Research Questions

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

1. What is the relationship between e-examinations and national security?
2. What are the issues of e-examinations that affect national security?
3. What are the challenges militating against e-examinations and national security?
4. What are the prospects for JAMB's provision of adequate security for its e-examination operations?

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 et al. (2011) assert that e-examinations have numerous benefits compared to conventional paper-and-pencil assessments, such as expedited result dissemination, diminished administrative expenses, and improved precision. Nonetheless, these advantages are frequently eclipsed by security apprehensions, which have emerged as a significant area of inquiry in recent years.

Examination malpractice is a significant concern in e-examinations, involving several unethical practices, including impersonation, unauthorised possession of electronic devices, and coordination among applicants (Oloyede, 2017). These behaviours compromise the integrity and reliability of evaluations and present considerable threats to national security. Ikechukwu and Abonyi (2020) contend that test malpractices exacerbate societal issues including corruption, unemployment, and underdevelopment by fostering a culture of dishonesty and mediocrity.

Cybersecurity attacks represent a significant concern in electronic examinations. Fluck et al. (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 dangers undermine both the secrecy and integrity of examination data, while simultaneously diminishing public trust in the educational system. In Nigeria, JAMB has encountered many cybersecurity difficulties, including attempts to infiltrate its examination servers and alter results (Okoro, 2021).

Researchers have offered diverse answers to these difficulties, encompassing technology breakthroughs and policy reforms. Balakrishnan and Surendran (2020) advocate for the implementation of secure information access mechanisms, including encryption and multi-factor authentication, to safeguard examination data. Bardes 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 applicants partake in examination 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; however, few have analysed the socio-cultural and institutional elements that lead to examination malpractices (Bitrus, 2013). Moreover, there is insufficient study regarding the long-term effects of e-examinations on national security and development. Rectifying these deficiencies is essential for formulating comprehensive measures to improve the security and reliability 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 gathered via questionnaires distributed to 200 participants, comprising JAMB officials, administrators, candidates, and security personnel. Secondary data were acquired from government publications, yearly reports, and scholarly journals. The data were examined utilising descriptive statistics, theme analysis, and content analysis to fulfil the research objectives.

Data Analysis

Section A: Demographic Information

Variable	Category	Frequency (n=200)	Percentage (%)
Gender	Male	120	60%
	Female	80	40%
Age	18–25	90	45%
	26–35	70	35%
	36–45	30	15%
	46 and above	10	5%
Role	JAMB Official	30	15%
	Examination Admin	40	20%
	Candidate	100	50%
	Security Personnel	20	10%
	Other	10	5%

Section B: E-Examinations and National Security

Question	Response Option	Frequency	Percentage
4. To what extent do you agree that e-examinations impact national security?	Strongly Agree	80	40%
	Agree	70	35%
	Neutral	30	15%

	Disagree	15	7.5%
	Strongly Disagree	5	2.5%
5. Major security challenges in e-examinations (Multiple responses allowed)	Cyber-attacks	150	75%
	Impersonation	140	70%
	Unauthorized access	100	50%
	Biometric failures	60	30%
	Others (e.g., power outages)	20	10%
6. Effectiveness of JAMB's security measures	Very Effective	30	15%
	Effective	60	30%
	Neutral	50	25%
	Ineffective	40	20%
	Very Ineffective	20	10%

Section C: Challenges and Prospects

Question	Response Option	Frequency	Percentage
7. Biggest obstacles to secure e-examinations (Multiple responses allowed)	Poor internet infrastructure	160	80%
	Lack of technical expertise	120	60%
	Corruption among officials	90	45%
	Inadequate funding	70	35%
	Others (e.g., low awareness)	20	10%
8. Strategies to improve e-examination security (Multiple responses allowed)	Enhanced biometrics	140	70%
	Cybersecurity training	120	60%

	Stiffer penalties	100	50%
	Blockchain-based systems	80	40%
	Others (e.g., AI proctoring)	30	15%

Key Findings from Frequency Analysis

1. **Demographics**:
   - Majority of respondents were **candidates (50%)**, followed by administrators (20%).
   - 60% were male, and 45% were aged 18–25.
2. **Perceived Impact on National Security**:
   - **75% agreed or strongly agreed** that e-examinations affect national security.
   - Top security threats: **Cyber-attacks (75%) and impersonation (70%)**.
3. **JAMB's Security Measures**:
   - Only **45% rated them as effective or very effective**, while **30% deemed them ineffective**.
4. **Challenges**:
   - **Poor internet infrastructure (80%)** was the biggest obstacle.
   - **Corruption among officials (45%)** was also significant.
5. **Proposed Solutions**:
   - **Enhanced biometrics (70%) and cybersecurity training (60%)** were top recommendations.
   - **Blockchain technology (40%)** was seen as a promising solution.

The research indicates that although e-examinations are acknowledged as influential on national security, considerable obstacles persist, especially in infrastructure, cybersecurity, and institutional corruption. Participants predominantly endorsed technical enhancements (biometrics, blockchain) and regulatory improvements (increased penalties) to bolster security.

IV. Findings And Discussion

Findings

Relationship Between E-Examinations and National Security

The research identified a significant association between the security of electronic examinations and national security. Examination malpractices, including impersonation, hacking, and result manipulation, compromise the integrity of educational assessments, thereby cultivating a culture of dishonesty and eroding institutional trust. Cyber-attacks on examination systems, exemplified by those encountered by JAMB, present a direct threat to national security by compromising sensitive data and facilitating fraudulent activities (Adepoju, 2022).

Challenges Militating Against E-Examinations

- **Examination Malpractices:** According to Oloyede (2017), impersonation, the use of unapproved gadgets, and candidate collaboration are still common problems.
- **Cybersecurity Threats:** According to the study, regular cyberattacks, such as Distributed Denial-of-Service (DDoS) attacks and server breaches, are a serious issue (Okoro, 2021).
- **Infrastructural Inadequacies:** Subpar internet connectivity, power fluctuations, and insufficient technical assistance impede the seamless execution of e-examinations (Umoru & Wahab, 2021).

Human Resource Limitations: Inadequate training for examination administrators and security personnel impairs the implementation of anti-malpractice protocols (Adepoju, 2022).

Role of JAMB in Managing Examination Security

JAMB has instituted biometric verification and the National Identity Number (NIN) system to prevent impersonation. Nonetheless, these steps have encountered obstacles, including delays and technical malfunctions.

The board has implemented encrypted question delivery methods and real-time monitoring; yet, cybercriminals persist in exploiting loopholes (Bitrus, 2013).

Prospects for Improving E-Examination Security

Augmented Cybersecurity Protocols: The implementation of blockchain technology, AI-driven proctoring, and multi-factor authentication may bolster security (Balakrishnan & Surendran, 2020).

Policy Reforms: Enhanced sanctions for examination fraud and engagement with cybersecurity agencies may dissuade misconduct (Ikechukwu & Abonyi, 2020).
Capacity Building: Training initiatives for examiners, invigilators, and IT professionals would enhance system resilience (Adebayo et al., 2011).

Discussion

The results correspond with current literature, affirming that e-examinations, notwithstanding their advantages, pose considerable security threats that impact national stability. The Hierarchy of Needs Theory (HNT) (Abdulhamid, 2017) elucidates the rationale behind candidates' engagement in malpractice, positing that unfulfilled needs, such as fear of failure and pressure to achieve, catalyse unethical behaviour. The Theory of Planned Behaviour (TPB) (Sniehotta, 2009) posits that cultural views regarding exam fraud, such as the normalisation of cheating, affect applicants' behaviours.

The research also underscores institutional deficiencies in Nigeria's electronic examination system. Despite JAMB's laudable efforts, deficiencies in infrastructure and human resources hinder efficacy. In comparison, nations with strong digital examination systems (e.g., UK, US) allocate substantial resources to cybersecurity and stakeholder training—an approach that Nigeria should consider implementing.

Moreover, the socio-cultural aspect of examination misconduct is crucial. The drive to obtain university admissions in a fiercely competitive landscape intensifies fraudulent activities. Therefore, in addition to technology solutions, public awareness initiatives and ethical reorientation programs are essential.

The research highlights that inadequately secured e-examinations pose a risk to national security by facilitating fraud, cybercrime, and eroding institutional confidence. Despite JAMB's advancements, ongoing issues necessitate collaborative efforts across several stakeholders, stringent policy implementation, and the integration of new technology. Future investigations should examine AI-driven anti-fraud mechanisms and the enduring socio-economic consequences of examination misconduct.

V. Conclusion

E-examinations possess the capacity to revolutionise the educational framework by offering efficient and dependable evaluations. Nonetheless, their incorporation into high-stakes assessments has also presented new concerns, especially with national security. This study emphasises the necessity of tackling these difficulties via technical advancements, legislative modifications, and stakeholder cooperation. By implementing this approach, educational institutions may uphold the integrity of electronic examinations and advance the overarching objectives of national security and development.

Recommendations

1. **Adopt Blockchain Technology –** Utilise blockchain for secure, immutable storage and transmission of examination data.
2. **Strengthen Cybersecurity Protocols —** Implement AI-driven proctoring, multi-factor authentication (MFA), and encryption to thwart hacking and impersonation attempts.
3. **Enhance Penalties for Malpractice —** Implement more stringent legal repercussions for examination fraud, encompassing candidates, authorities, and cybercriminals.
4. **Enhance Infrastructure —** Upgrade internet connectivity, power supply, and technical support for efficient e-examination administration.
5. **Train Examination Personnel —** Implement regular cybersecurity and anti-fraud training for JAMB officials, invigilators, and IT teams.
6. **Enhance Public Awareness -** Initiate ethical campaigns to deter malpractice and inform candidates about digital examination processes.

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] 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
[9] 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.
[10] Ogunji, J. A. (2011). Examination Management And Examination Malpractice: The Nexus. Journal Of International Education Research (JIER), 7 (4), 1-10.
[11] Okoro, F. (2021). Security Of Examination Server—JAMB Experience. Information Technology Services Department, JAMB .
[12] Oloyede, W. (2017). Examination Malpractice In Nigeria: Causes, Effects, And Solutions. Journal Of Education And Practice, 8 (12), 1-10.
[13] Sniehotta, F. F. (2009). Towards A Theory Of Intentional Behaviour Change: Plans, Planning, And Self-Regulation. British Journal Of Health Psychology, 14 (2), 261-273. Https://Doi.Org/10.1348/135910708X347281
[14] Umoru, T. A., & Wahab, A. (2021). Cybersecurity Challenges In E-Examinations: A Case Study Of JAMB. Journal Of Information Technology And Security, 5 (1), 1-15.