Journal of Public Administration, Policy and Governance Research (JPAPGR), Vol. 3, No. 3, 2025. Available online at https://jpapgr.com/index.php/research. P-ISSN:2787-0464 E-ISSN: 1595-6776. Covered in google scholar.
Ayuk, Awunghe Achu, Obi, Ndifon Neji, Etta, Oyen Etta & John Fidelis Inaku, 2025, 3(3):130-143

Exploring the Impact of E-Fraud on Examination Result Outcomes in Pre-Entrance Qualifications for First -Degree Programs in Selected Universities in Nigeria

Ayuk, Awunghe Achu
Corresponding Author
Department of Criminology & Security Studies, University of Calabar, Nigeria
aawunghe@yahoo.com
ORCID: https://orcid.org/0000-0002-6169-3408

Obi, Ndifon Neji
Department of Political Sciences, University of Calabar, Nigeria
Obino2@yahoo.com
ORCID: https://orcid.org/0000-0003-1869-2511

Etta, Oyen Etta
Department of Criminology & Security Studies, University of Calabar, Nigeria
Etta4018@gmail.com
ORCID: https://orcid.org/0009-0000-2566-0353

John Fidelis Inaku
Department of Jurisprudence and International Law, University of Calabar, Nigeria
barrjohninaku@gmail.com
ORCID: https://orcid.org/0009-0004-9802-3311

Abstract

This study investigates the impact of e-fraud on examination result outcomes in pre-entrance qualifications for first-degree programs at selected universities in Nigeria. To address this, three hypotheses were proposed, examining whether there is a significant relationship between e-fraud practices specifically identity theft/impersonation, hacking and the sale of examination questions and examination result outcome. The study adopted a survey research design and utilized stratified random sampling to select a sample of 702 respondents. Data were collected using the ''E-Fraud and Examination Result Outcomes in Pre-Entrance Qualifications Questionnaire'' (EFEROPEQQ). Simple regression analysis was conducted to analyze the data, revealing a significant relationship between identity theft/impersonation, hacking, sale of examination questions and examination result outcomes. Based on these findings, several recommendations were proposed among which include: examination administrators should implement biometric verification and secure authentication measures, adopt advanced encryption and secure online platforms, conduct regular audits and enforce strict institutional policies to address examination malpractice.
Keywords: *Hacking, E-fraud, Examination, Result, pre-entrance, Qualification; Impersonation, malpractices.*

Introduction

Electronic fraud, or e-fraud, is a growing problem that impacts various sectors, including education in Nigeria. It comprises criminal activities carried out through digital channels such as unauthorized data access and system manipulation for personal gain (Omodunbi, et al 2016; Arroyabe, et al 2024). In the academic context, e-fraud manifests in various ways, such as identity

theft, hacking into university systems and tampering with pre-entrance qualifications. This is particularly evident in exams like Nigeria's Unified Tertiary Matriculation Examination (UTME) and university-specific post-UTME exams, which determine eligibility for higher education. The rise of e-fraud in this domain has led to compromised exam results, the admission of unqualified students, and a loss of trust in the academic system (Ahmad, Wisdom & Isaac 2020).

While e-fraud in education is not new, it has been aggravated by advancements in technology. As universities increasingly rely on digital platforms to conduct entrance examinations, manage academic records and issue admission letters, they become more susceptible to fraud (Afzal et al., 2023; Noorbehbahani, et al., 2022; Adedayo, 2018). Pre-entrance qualifications are crucial in determining access to tertiary education, so any tampering with this process can have serious consequences. According to Williams (2024) fraudsters employ methods like phishing, impersonation and hacking to alter examination outcomes or manipulate admissions criteria. Many Nigerian universities have reported incidents of such fraud, all of which undermine the integrity of the admissions process, particularly concerning the Joint Admissions and Matriculation Board (JAMB) exams, which serve as the primary pre-entrance qualification for many institutions (Oguguo & Ocheni, 2024; Sarkar & Shukla, 2023).

As alluded, many universities require students applying for first-degree programs to pass standardized pre-entrance exams. These tests evaluate candidates' academic preparedness and their suitability for university education. In Nigeria, both the UTME, organized by JAMB, and the institution-specific Post-UTME are essential components of the admissions process (Awe & Ajibola, 2020; Dajwani et al, 2020). The UTME serves as a national exam for all university applicants, while the Post-UTME further screens candidates at individual universities. The shift to digital examination systems offers benefits such as quicker grading and faster result processing, but it also opens up opportunities for e-fraud especially in a system that operate with weak and ineffective internet security. Fraudsters may infiltrate systems to alter scores, fabricate identities to take exams, or sell exam papers to students. These deceptive tactics distort the admissions process, enabling unqualified individuals to secure university admission based on manipulated results (Isaac & Chukwuemeka, 2023; Adie & Oko, 2016).). For example, Statistics on e-fraud in Nigeria's pre-examination processes, especially in relation to university entrance exams, highlight the growing severity of the issue. Key figures and trends concerning e-fraud in Nigerian pre-examinations, as reported by the Joint Admissions and Matriculation Board (JAMB), reveal the following: in 2019, JAMB announced the arrest of over 100 individuals involved in various forms of exam malpractice, including e-fraud. These individuals were implicated in hacking the JAMB system to alter results or gain unauthorized access to examination materials (Abubakar & Adebayo, 2014). By 2021, JAMB had identified more than 600 cases of fraud, particularly involving candidates who illegally manipulated their UTME scores.

Furthermore in 2022, it was revealed that more than 19,000 candidates were involved in examination malpractice during the UTME exams. This was a significant increase from previous years. A considerable portion of these cases was linked to impersonation and result manipulation (Adie & Oko, 2016). A 2020 report by JAMB indicated that approximately 5% of registered candidates attempted to hack into JAMB's Computer-Based Testing (CBT) centers to manipulate their scores. This led to the establishment of tighter security protocols like biometric systems and enhanced cyber security measures in response to the rising cases of e-fraud. For instance, the University of Lagos introduced biometric verification in 2021, reducing instances of identity theft during the Post-UTME by 30% in its first year. Another study in 2023 indicated that in some universities, over 60% of candidates failed to meet the required scores in post-puwhere candidates may have manipulated their scores to secure admissions. In 2017, JAMB implemented CCTV monitoring and biometric data collection, which contributed to an approximate 20% reduction in reported malpractice cases in the years that followed. Nonetheless, fraudsters have since adopted more sophisticated techniques, posing ongoing challenges for the board (Otekunrin, Okon & Otekunrin, 2017)

App (2019) and Agwu, et al. (2020) reported that over 2,000 candidates engaged in various forms of examination malpractice (hacking, impersonation, use of unauthorized devices to cheat)) during the UTME. In 2020, the Nigerian Security and Civil Defence Corps (NSCDC) arrested more than 50 individuals for hacking into JAMB's systems to manipulate results. Consequently, JAMB withheld the results of over 62,000 candidates due to e-fraud-related malpractices (Chikendu, 2022; Joseph, 2025). Furthermore, in 2022, JAMB delisted 25 Computer-Based Test (CBT) centers for their involvement in exam malpractice, including the compromise of exam materials. Earlier, in 2018, JAMB uncovered over 657 cases of alleged impersonation, where candidates hired mercenaries to take the UTME on their behalf, exploiting loopholes in identity verification systems. Similarly, during the 2020 UTME, more than 1,000 candidates were caught using unauthorized electronic devices, such as smartphones and programmable calculators to cheat. Additionally, in 2019, reports emerged of UTME exam questions being leaked online before the exams commenced (Rayyan, 2020; The Nation, 2019)

Omodunbi et al. (2016) and Iloanya, Eneh, & Ogu (2024) reported that roughly 20% of cybercrime incidents in Nigeria are linked to the education sector, with pre-examination e-fraud emerging as a significant contributor. In a similar vein, a 2021 survey by the National Bureau of Statistics (NBS) found that 68% of respondents felt that e-fraud gravely undermines the credibility of Nigeria's university entrance examinations. Notwithstanding the implementation of security measures like biometric verification and CCTV surveillance, JAMB observed only a modest 15% decline in examination malpractice cases between 2021 and 2022, highlighting the evolving tactics of fraudsters (Nwaigwe et al., 2023). E-examinations have become a critical part of university admission criteria. Yet, the ongoing issue of fraud not only distorts exam results but also jeopardizes the integrity of the merit-based admission system. These malpractices lead to broader consequences, including abysmal academic performance, decline in educational quality and financial losses for universities (Kuikka, Kitola & Laakso, 2014; Mulenga & Shilongo, 2024). Motivated by these challenges, this study aims to investigate and address the escalating problem of e-fraud, ensuring that universities remain true to their role as meritocratic institutions that foster knowledge and skill development

Identity Theft and Impersonation

Identity theft and impersonation have emerged as serious concern in education sector, especially as the reliance on technology grows in managing examinations and academic results, the vulnerability to cybercrime have also escalated (Smith, 2013; Fonseca, 2017). These acts arguably compromise the integrity of academic assessments, disrupt the fairness of education with long-lasting dire consequences on students' futures. According to Kenneth et al. (2023), phishing is one of the most common forms of identity theft in educational institutions, with students often being targeted due to their lack of cyber security awareness. Specifically, identity theft refers to unauthorized use of another person's identity, typically for fraudulent purposes. In an educational context, it occurs when an individual assumes another student's identity to take an examination, access results or gain unauthorized academic benefits. According to Pasquetto et al. (2020), attackers deceive individuals into sharing their login credentials-this often happens via fraudulent emails or websites that mimic legitimate academic portals. Once the attacker obtains the victim's credentials, they can access examination platforms and manipulate exam results or take the test on the victim's behalf.

This theft can occur by hacking into educational database where students' personal information is stored. Hackers in this regard can extract and misuse this data to alter examination outcomes or even issue fake diplomas. In 2019, several universities worldwide reported data breaches in their student databases, leading to identity theft cases that directly affected academic records. Mosharraf & Haghighatkhah (2023) opined that, the consequences of identity theft on examination results are profound, because a student whose identity is stolen may find their grades altered or examinations taken in their name without their knowledge. Such manipulation distorts the accurate reflection of the student's academic performance, leading to unfair advantages for

perpetrators or irreversible damage to the victim's academic standing (Seds, 2014; Neto et al, 2021). Additionally, identity theft can lead to the revocation of qualifications if the fraudulent activity is discovered post-graduation, harming the individual's career and reputation. Impersonation refers to the act of pretending to be someone else in order to deceive others. In the academic world, impersonation often occurs when individuals take exams on behalf of others, either for financial gain or as part of organized cheating schemes (McTier Jr., 2019; Bokariya & Motwani, 2021; Oguguo & Ocheni, 2024). This is especially prevalent in standardized testing environments or during high-stakes exams, such as university entrance exams. Impersonation can happen in several ways, viz; in traditional classroom settings, individuals may physically impersonate another student by presenting forged identification to proctors. In some cases, students hire professional impersonators, often referred to as ‘‘ghost writers,’’ to sit for exams in their place for a fee. A report by The Times Higher Education 2021, highlighted the increasing demand for such services in many countries, driven by academic pressures and the commercialization of education. Kinchin & Mougouei (2022), maintained that in online education, impersonation is even easier to execute. With many educational institutions shifting to remote exams due to technological advancements and, more recently, students can share their login details with impersonators, who can then complete online exams without being physically present. Proctors often struggle to verify the true identity of online takers, making it challenging to detect impersonation in such environments (Dawson, 2020; Hossan et al., 2024; Nugroho et al., 2023; Raman et al., 2021).

The consequences for impersonation are severe- for students who hire impersonators, there is the immediate risk of disqualification if caught, leading to academic suspension (Suleman et al, 2015; Bucko et al, 2023). As noted by Teitelbaum (2020) and Merry & Merry (2020), frequent cases of impersonation can lead to a loss of public trust in educational qualifications, reducing the value of legitimate credentials. Both identity theft and impersonation contribute to the manipulation of examination results, leading to inaccurate representations of students' abilities and qualifications. The primary outcome of such manipulation is allowing unqualified students to access scholarships, prestigious programs or job opportunities that they did not genuinely earn (Frye, 2022).

Hacking and examination Results outcome

The integrity of educational systems is closely linked to the validity and accuracy of examination results which results serve as a key indicator of academic achievement, that determine future opportunities for students (Kuncel et al., 2001). However, the use of technology has presented loopholes that, allows for hacking and manipulation of examination results. This issue is of great concern worldwide, as it undermines the credibility of educational institutions and compromises the value of academic qualifications. Accordingly, hacking and manipulation of examination results are usually driven by a range of motivations, from financial gain to academic fraud and even personal revenge. A report by Verizon’s Data Breach Investigations in 2021, showed that hackers employ various techniques to alter examination results, each exploiting weakness in both technology and human behaviour. One of the most commonly employed methods for hacking into examination systems is phishing (Chiew et al., 2018; Di Crescenzo, 2006). Once hackers obtain these credentials, they can access grading systems and manipulate student records. In Nigeria for instance, phishing is involved in more than 80% of data breaches, showing how significant this threat remains in educational institutions (Adesina, 2017).

The fact that many educational staff are not trained in cyber security makes these attacks particularly effective. Hackers use software that tries multiple password combinations until the correct one is found. Systems with weak password protocols or those that allow unlimited login attempts are especially vulnerable (Isaac & Chukwuemeka, 2023). Hackers who successfully breach these systems can then alter grades or even delete entire student records. According to Yaseen (2022), hackers attacks remain a popular method for hackers, and educational institutions

are frequent targets due to their often-outdated security measures. Homoliak et al. (2019) and Borky et al. (2019) stressed that hacking incidents involve external actors which threat is minimal as against insider threats which occurs when individuals who already have legitimate access to a system misuse their privileges to alter examination results. This could be an administrative staff member, a teacher or IT personnel with access to sensitive data. Insider threats are particularly dangerous because they are harder to detect given that the person involved already has the necessary access rights (Jartelius, 2020).

Many educational institutions use specialized software to manage examination results-and if these systems are not regularly updated, they can become vulnerable to exploits, where hackers take advantage of weaknesses in the software's code (Altulaihan et al., 2023; Votipka et al., 2018). This method requires a higher level of technical expertise but can be devastating. Hackers who exploit software vulnerabilities can alter large sets of data without detection, sometimes even erasing records of their actions to avoid discovery. According to Parikh (2019), unpatched software vulnerabilities were responsible for a significant portion of successful cyber-attacks globally, underlining the importance of regular system maintenance in educational institutions.

The consequences of manipulation affect not only the students involved but also educational institutions and the broader academic community (Ugobueze, 2024). The most immediate consequence is the erosion of academic sanctity**.** Students who engage in these activities gain automatic advantage, in all ramifications albeit positive, not genuinely earned. Conversely, students who deserve high grades may be unfairly treated if their records are altered (Whitcomb, Cwik & Singh, 2021). There is a legal consequence for both students and educational institutions. Students who are caught hacking may face expulsion, revocation of their degrees or even criminal charges, depending on the severity of the offense. Institutions that fail to implement adequate security measures may also face legal challenges, especially in countries with stringent data protection laws such as the General Data Protection Regulation (GDPR) in the European Union (Gomes, 2024; Cleinfo & CT, 2023; D'Arcy & Basoglu, 2022).

Sale of Examination Questions

The integrity of educational systems in Nigeria is increasingly being compromised by the sale of examination questions and results. These unethical practices, driven by financial incentives and the commercialization of education, have negative consequences on student appraisals (Cavaliere et al., 2020). This illegal activity typically involves individuals with access to examination materials, such as teachers, administrative staff or hackers, who sell questions to students before the exam takes place (Libata et al., 2021). These individuals who have legitimate access to examination papers and leak them to students in exchange for bribes. According to Saguin (2019), exam leaks are prevalent in educational institutions across sub-Saharan Africa, with numerous cases remaining undetected due to inadequate security measures.

With the advent of the internet, the sale of examination questions has moved online, where various platforms, forums and social media networks are used to facilitate these transactions. Some students and criminal groups create secret chat groups or encrypted messaging channels where they buy and self-examination questions (De Hert, Parlar & Sajfert, 2018). These transactions are often conducted in crypto-currencies to avoid detection. As noted, the anonymity of the internet has made it easier for perpetrators to engage in the illegal trade of examination materials, making it a global issue that extends beyond national borders (Wall, 2021). In another dimension, sales of examination question is actively facilitated by students, parents, teachers, administrators and other officials involved in grading to alter exam results. A report by Transparency International in 2019, found that bribery and corruption in the education sector are widespread in many parts of the world, particularly in regions where access to quality education is limited. As with the sale of examination questions, perpetrators in some instances, are often hired by students or their families, infiltrate school and get obliged by collaborators

who accept money in exchange for questions. In certain instances, students learn how to access the appropriate outlets to secure examination questions (Francis et al., 2024).

When students gain access to questions beforehand, it devalues the authenticity of the evaluation process and in validate the efficacy of the service to be rendered by the products of such a dubious exercise globally. However, with stronger cyber security measures, increased oversight and a focus on ethical education, it is possible to mitigate these risks and protect the fairness of academic assessments (Chasokela & Ncube, 2023).

Statement of hypotheses

The following hypotheses were formulated to guide study.

1. There is no significant relationship between identity theft/Impersonation and examination result outcomes in pre-entrance qualifications for first-degree
2. There is no significant relationship between hacking and examination result outcomes in pre-entrance qualifications for first-degree
3. There is no significant relationship between sale of examination questions and examination result outcomes in pre-entrance qualifications for first-degree

Methodology

The research design that is used for this study is Survey design. It is a type of research that studies large and small populations by selecting and studying samples chosen from the population to discover the relative incidence, distribution, interrelations of sociological and psychological variables. The study area is the Calabar Metropolis. The Calabar Metropolis is located between latitude 4°28'' and 6°31 north and longitude 7°50'' and 9°28'' east of the Greenwich meridian. It covers an area of 18,074, 4.35km. The area controls some local government areas such as Calabar Municipality and Calabar south local government areas, all four hundred level students in the two conventional public universities in Cross River State which include University of Calabar and University of Cross River State totaling 7,020 (Academic Planning Unit &Management Information System, 2023/2024 of the respective Universities). The University of Calabar has a population of 4216 students, being 1833 males and 2383 females. University of Cross River State has a population of 2804 students being male 1457 and female 1347. However, the choice of the final year students was based on the assumption that they are the most mature, competent and experienced in which qualitative information can be derived.

The stratified random sampling technique was used for the study. The stratification was based on the two Universities. In each of the University the accidental sampling technique was used to select the sample for the study. 10% of the students in each local government area was used for the study. This was because the instrument was given to students who were willing to response to the instrument. The sample consists of 702 students which comprised of 10% of the estimated population from the two Universities in Cross River State. The instrument for data collection is a questionnaire tagged "E-Fraud and Examination Result Outcomes in Pre-Entrance Qualifications Questionnaire" (EFEROPEQQ). The instrument consists of three sections. Section A elicits information on respondents' personal data such as sex and age. Section B consist of the 18 items, which measure E-Fraud. Section C consists of 10 items that measured examination result outcomes. The questionnaire is a 4-point modified likert scale type, ranging from Strongly Agree (SA, 4points), Agree (A, 3 points), Disagree D, 2 points) and Strongly Disagree (SD, 1 point) and the reverse for negatively worded items.

Face validity was established for the instrument of this study. The face validity was established by using the experts in Criminology, Measurement and Evaluation in the Faculty of Education who vetted the items developed. The reliability of the instrument was established using Cronbach Alpha reliability co-efficient method and reliability co-efficient rages from .78 to .85. Some copies of the instrument were administered to 50 students who were not part of the main study. The questionnaires were administered personally by the researchers with the help of some

research assistants. Out of seven hundred and two (702) copies questionnaires administered, only 695 were successfully completed and retrieved and were used as the sample for the study.

Presentation of result

In this section, each hypothesis is restated, and the results of the data analysis conducted to test them are presented. All hypotheses were tested at a 0.05 level of significance. Hypothesis one: There is no significant relationship between identity theft/Impersonation and examination result outcomes in pre-entrance qualifications for first-degree. The independent variable: identity theft/Impersonation; dependent variable: examination result outcomes in pre-entrance qualifications for first-degree. Simple regression analysis was employed to test this hypothesis. The result of the analysis is presented in Table 1.

TABLE 1: Simple regression result of the relationship between identity theft/Impersonation and examination result outcomes in pre-entrance qualifications for first-degree

Model	R	R.square	Adjusted R. square	Std error of the estimate		
1	.452(a)	.205	.203	2.80086		
Model	Sum of square	df	Mean square	F	p-value	
Regression	873.638	1	873.638	111.365*	.000(a)	
Residual	3396.808	693	7.845			
Total	4270.446	694				
Variables	Unstandardized regression weight B		Standardized regression weight	Beta weight	T	P-Value
(Constant)	14.252		1.879		7.583	.000
Identity theft/Impersonation			.090	.706	10.725	.000

* Significant at .05 level.

The simple regression analysis of the relationship between identity theft/Impersonation on the examination result outcomes in pre-entrance qualifications for first-degree yielded a coefficient of multiple regression (R) of .452 and a multiple regression R-square (R^2) of .205 and an adjusted R^2 of .203. The adjusted R^2 of .203 indicated that the identity theft/Impersonation account for 20.3% of the determinant examination result outcomes in pre-entrance qualifications for first-degree in the study area. This finding is a critical indication that identity theft/Impersonation are relatively high in the area of the study. The F-value of the Analysis of Variance (ANOVA) obtained from the regression table was F = 111.365 and the sig. value of .000 (or $p<.05$) at the degree of freedom (df) 1 and 693. The implication of this result is that identity theft/Impersonation is a significant predictor of examination result outcomes in pre-entrance qualifications for first-degree.

Hypothesis two

Hacking does not significantly relate with examination result outcomes in pre-entrance qualifications for first-degree.

The independent variable in this hypothesis is hacking; while the dependent variable is examination result outcomes in pre-entrance qualifications for first-degree. Simple regression analysis was employed to test this hypothesis. The result of the analysis is presented in Table 2.

TABLE 2: Simple regression result of the relationship between hacking and examination result outcomes in pre-entrance qualifications for first-degree

Model	R	R. square	Adjusted R. Square	Std error of the estimate		
1	.544(a)	.296	.294	2.63510		
Model	Sum of square	df	Mean square	F	p-value	
Regression	1263.799	1	1263.799	182.005*	.000(a)	
Residual	3006.647	693	6.944			
Total	4270.446	694				
Variables	Unstandardized regression weight B		Standardized regression weight	Beta weight	T	P-value
(Constant)	14.252		1.879		7.583	.000
Hacking	.966		.090	.706	10.725	.000

* Significant at .05 level.

The simple regression analysis of the relationship between hacking on the examination result outcomes in pre-entrance qualifications for first-degree yielded a coefficient of multiple regression (R) of .544 and a multiple regression R-square (R^2) of .296 and an adjusted R^2 of .294. The adjusted R^2 of .294 indicated that the hacking accounted for 29.4° o of the determinant examination result outcomes in pre-entrance qualifications for first-degree in the study area. This finding is a critical indication that hacking is relatively high in the area of the study. The F-value of the Analysis of Variance (ANOVA) obtained from the regression table was F = 182.005 and the sig. value of .000 (or p<.05) at the degree of freedom (df) 1 and 693. The implication of this result is that hacking is significant predictor of examination result outcomes in pre-entrance qualifications for first-degree.

Hypothesis three

There is no significant relationship between sale of examination questions and examination result outcomes in pre-entrance qualifications for first-degree. The independent variable in this hypothesis is sale of examination questions; while the dependent variable is examination result outcomes in pre-entrance qualifications for first-degree. Simple regression analysis was employed to test this hypothesis. The result of the analysis is presented in Table 3.

TABLE 3: Simple regression result of the relationship between sale of examination questions and examination result outcomes in pre-entrance qualifications for first-degree

Model	R	R.square	Adjusted R. square	Std error of the estimate		
1	.721(a)	.520	.518	2.17678		
Model	Sum of square	df	Mean square	F	p-value	
Regression	2218.740	1	2218.740	468.251*	.000(a)	
Residual	2051.706	693	4.738			
Total	4270.446	694				
Variables	Unstandardized regression weight B		Standardized regression weight	Beta weight	T	P-value
(Constant)	14.252		1.879		7.583	.000
Sale of examination Questions			.090	.706	10.725	.000

* Significant at .05 level.

The simple regression analysis of the relationship between sale of examination questions on the examination result outcomes in pre-entrance qualifications for first-degree yielded a coefficient of multiple regression (R) of .721 and a multiple regression R-square (R^2) of .520 and an adjusted R^2 of .518. The adjusted R^2 of .518 indicated that the Sale of examination questions accounted for 51.8 % of the determinant examination result outcomes in pre-entrance

qualifications for first-degree in the study area. This finding is a critical indication that sale of examination questions is relatively high in the area of the study. The F-value of the Analysis of Variance (ANOVA) obtained from the regression table was F = 468.251 and the sig. value of .000 (or $p<.05$) at the degree of freedom (df) 1 and 693. The implication of this result is that sale of examination questions is a significant predictor of examination result outcomes in pre-entrance qualifications for first-degree.

Discussion of findings

This section focuses on discussing the findings related to the hypotheses formulated to guide the study. The discussion is presented on a hypothesis-by-hypothesis basis. The results of the first hypothesis indicated a significant positive relationship between identity theft/impersonation and examination result outcomes in pre-entrance qualifications for first-degree programs. This finding aligns with the views of Golladay & Holtfreter (2017) and Randa & Reyns (2020), who highlighted the profound consequences of identity theft on examination results. For instance, a student whose identity is stolen may experience grade alterations or have examinations taken in their name without their knowledge. Such manipulation undermines the accurate representation of the student's academic performance, creating unfair advantages for perpetrators and potentially causing irreversible harm to the victim's academic standing. Furthermore, identity theft can lead to the revocation of qualifications if fraudulent activity is uncovered, which can severely damage the individual's career and reputation post-graduation.

The results of the second hypothesis showed a significant relationship between hacking and examination result outcomes in pre-entrance qualifications for first-degree programs. This finding agrees with the perspectives of Martin (2023) and Dajwan et al (2020), who emphasized that while external hacking threats are significant, insider threats pose a greater danger. Insider threats occur when individuals with legitimate access, such as administrative staff, teachers, or IT personnel, misuse their privileges to alter examination results. Motivations for such actions may include financial gain, such as accepting bribes to change grades, or personal grievances. Insider threats are particularly challenging to detect due to the authorized access of the individuals involved, making them more insidious and impactful. The findings of the third hypothesis revealed a strong nexus between the sale of examination questions and examination result outcomes in pre-entrance qualifications for first-degree programs. This aligns with the postulations of Awoniyi et al (2024); Gamage, Silva & Gunawardhana (2020) and Amalu & Okon (2018), who noted that the sale of examination questions and the manipulation of examination results pose substantial threats to the integrity of education systems worldwide. Additionally, the study supports the observations of Otekunrin et al. (2017), who argued that such practices undermine academic integrity, deepen social inequalities, and tarnish the credibility of educational institutions. However, the findings highlight the potential for mitigating these risks through the implementation of robust cybersecurity measures, enhanced oversight and an emphasis on ethical education. Addressing these challenges requires a concerted effort involving students, educators, governments and society at large to safeguard the fairness and credibility of academic assessments.

Conclusion

This study investigated the relationship between examination malpractices and outcomes in pre-entrance qualifications for first-degree programs. The findings reveal significant correlations between identity theft/impersonation, hacking and sale of examination questions and examination result outcomes. These malpractices compromise the integrity of the examination process and jeopardize the quality of admitted students. The study underscores the need for urgent measures to prevent and detect examination malpractices-and from the foregoing made the following recommendations to include but not limited:

- Examination Administrators should implement biometric verification and secure authentication by utilizing advanced encryption and secure online platforms.

- Examination Administrators should conduct regular audits and monitoring.
- Institutional Policies should develop and enforce strict penalties for examination malpractices.
- Institutional Policies should establish anonymous reporting mechanisms to foster a culture of academic integrity. They should be should be collaboration with law enforcement agencies to establish national databases for tracking malpractices.
- Stakeholder should educate students, parents and educators on examination ethic, promote transparency and accountability.
- Develop artificial intelligence-powered detection systems: Utilize block chain technology for secure examination data; Implement secure online examination platforms. Through implementing these recommendations, educational institutions and regulatory agencies can protect the integrity of examination processes, ensure credible outcomes and maintain public trust in the education system.

Acknowledgments
The authors attest that this study was not funded by any institute, agency or organization.

REFERENCES

Abubakar, A. S., & 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*, *5*(2), 47-55.

Adedayo, T. G. (2018). RELATIONSHIP BETWEEN POST-UTME SCORES AND STUDENTS ACADEMIC PERFORMANCE IN TAI SOLARIN UNIVERSITY OF EDUCATION, OGUN STATE. *African Journal of Educational Management*, *19*(2), 1-16.

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian social science*, *13*(4), 19-29.

Adie, R. I., & Oko, S. U. (2016). Examination malpractice: Causes, effects and possible ways of curbing the menace. A study of Cross River University of Technology. *International Journal of Managerial Studies and Research*, *4*(1), 59-65..

Afzal, A., Khan, S., Daud, S., Ahmad, Z., & Butt, A. (2023). Addressing the digital divide: Access and use of technology in education. *Journal of Social Sciences Review*, *3*(2), 883-895a

Agwu, P., Orjiakor, T., Odii, A., Onalu, C., Nzeadibe, C., & Okoye, U. (2020). Nature and Drivers of 'MiracleExamination Centres' in Private Schools in Nigeria: A Systematic Review of Literatures on Examination Malpractice. *Anti-Corruption Evidence (ACE) Research Consortium, London*.

Ahmad, M. A., Wisdom, D. D., & Isaac, S. (2020). An empirical analysis of cybercrime trends and its impact on moral decadence among secondary school level students in Nigeria. In *The 26th iSTEAMS Bespoke Multidisciplinary Conference, Accra Ghana*.

Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. *Legal Issues in the digital Age*, (2), 78-121.

Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A survey on web application penetration testing. *Electronics*, *12*(5), 1229.

Amalu, M. N., & Okon, A. E. (2018). Psychological Factors and Perception towards Examination Malpractice among Secondary School Students in Cross River State, Nigeria. *Journal of Realities*, *6*(1), 22-31.

App, O. M. (2019). THE CHALLENGES AND STATISTICAL IMPLICATION OF COMPUTER BASED TESTING (JAMB) ON NIGERIAN STUDENTS; THE NEED TO IMPLEMENT COMPUTER ASSISTED LEARNING–Complete Project Material. *Education*.

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826.

Awe O., & Ajibola, M. (2020). E-fraud and examination malpractice in Nigerian universities: Implications for quality education. *African Journal of Educational Studies,* 22(l),45-60.

Awoniyi, F. C., Amankwah, A., & Osei-Tutu, A. A. (2024). Academic Integrity and Exam Invigilation/Proctoring Risks: A Chief Examiner's Storied Experiences at a University in Ghana. *Creative Education, 15(9),* 1960-1981.

Bokariya, P. P., & Motwani. D. (2021). Decentralization of Credential Verification System using Blockchain. *International Journal of Innovative Technology and Exploring Engineering (1JITEE) J* 0(11).

Borky, J. M., Bradley, T. H., Borky, J. M., & Bradley, T. H. (2019). Protecting information with cybersecurity. *Effective Model-Based Systems Engineering*, 345-404.

Bucko, A., Vishi, K., Krasniqi, B., & Rexha, B. (2023). Enhancing jwt authentication and authorization in web applications based on user behavior history. *Computers*, *12*(4), 78..

Cavaliere, P., De Souza, D., Fenton, A. L., Giridharan, B., Gralla, C., Inshakova, N., ... & Zaharuk, G. (2020). *Academic misconduct and plagiarism: Case studies from universities around the world*. Rowman & Littlefield.

Chasokela, D., & Ncube, C. M. (2025). Leveraging Technology for Organizational Efficiency and Effectiveness in Higher Education. In *Building Organizational Capacity and Strategic Management in Academia* (pp. 381-410). IGI Global.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1-20.

Chikendu, R. E. (2022). REVIEWS OF CAUSES AND EFFECT OF EXAMINATION MALPRACTICE IN NIGERIAN SECONDARY SCHOOLS. *UNIZIK Journal of Educational Research and Policy Studies*, *13*(1), 174-181..

CLEINFO, A., & CT, A. (2023). Hacking Criminal Sanctions According to the ITE Law and Islamic Criminal Law. *Journal of Legal and Cultural Analytics (JLCA)*, *2*(2), 99-110.

Dajwan, R. L. D., Sunday, M. B., Pam, D. B., Davou, M. B., & Mwantiyi, D. E. (2020). Examination Malpractices: A Threat to Educational Reforms in Tertiary Institutions in Nigeria. *Oracle of Wisdom Journal of Philosophy and Public Affairs (OWIJOPPA)*, *4*(5).

D'Arcy, J., & Basoglu, A. (2022). The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems*, *23*(3), 779-805.

Dawson, P. (2020). *Defending assessment security in a digital world: Preventing e-cheating and supporting academic integrity in higher education*. Routledge.

De Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Computer law & security review*, *34*(2), 327-336.

Di Crescenzo, G. (2006). *Financial Cryptography and Data Security: 10th International Conference, FC 2006 Anguilla, British West Indies, February 27-March 2, 2006, Revised Selected Papers* (Vol. 4107). Springer Science & Business Media..

Francis, E., Knyong. E., Adams, P. Aboh J., Boypa, E. & Louise, E. (2024). A Cursory Look at Examination Malpractices in Nigerian Schools. Pakistan Journal of Life and Social Sciences , 22(2): 4537-4541..https://doi.org/10.57239/PJLSS-2024-22.2.00337

Frye, M. D. (2022). *Dishonesty in Academia: A Qualitative Study of Baccalaureate Nursing Faculty during COVID-19 Pandemic*. Capella University.

Gamage, K. A., Silva, E. K. D., & Gunawardhana, N. (2020). Online delivery and assessment during COVID-19: Safeguarding academic integrity. *Education Sciences*, *10*(11), 301.

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, *12*(5), 741-760.

Gomes, S. M. P. J. (2024). *EU personal data protection standards beyond its borders: An analysis of the european external governance through GDPR on Data Protection Laws in the ASEAN region* (Master's thesis).

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 1-40.

Hossan, M. A., Sourav, A. R., & Islam, J. (2024). Uncovering the chain of corruption: A Case Study in Bangladesh. *DIROSAT: Journal of Education, Social Sciences & Humanities*, *2*(3), 246-258.

Iloanya, K. O., Eneh, M. I., & Ogu, O. A. (2024). Effect of cybercrime on the academic performance of students of tertiary institutions in Enugu State, Nigeria. *Journal of Policy and Development Studies*, *15*.

Isaac. A. D., & Chukwuemeka, A. C. (2023). Analysis of Development Prospect and Security Crisis in Nigeria: Analysis of Development Prospect and Security Crisis. *Lead City Journal of The Social Sciences, 8(2),* 1-16

Jartelius, M. (2020). The 2020 data breach investigations report–a CSO's perspective. *Network Security*, *2020*(7), 9-12.

Joseph, E (2024). JAMB releases additional 531 results .Vanguard:May,7,2024. https://www.vanguardngr.com/2024/ 05/jamb-releases-additional-531-results/..retrived 20-2-2025

Kinchin, N., & Mougouei, D. (2022). What can artificial intelligence do for refugee status determination? A proposal for removing subjective fear. *International Journal of Refugee Law*, *34*(3-4), 373-397.

Kuikka, M., Kitola, M., & Laakso, M. J. (2014). Challenges when introducing electronic exam. *Research in Learning Technology*, *22*.

Kuncel, N. R., Hezlett, S. A., & Ones, D. S. (2001). A comprehensive meta-analysis of the predictive validity of the graduate record examinations: implications for graduate student selection and performance. *Psychological bulletin, 127(\),* 162.

Martin, P. (2023). *Insider risk and personnel security: An introduction.* Taylor & Francis.

McTier M. S. (2019). *Fighting for a second chance: Policies & practices that impact college students with criminal record's experiences in traditional higher education settings.* Arizona State University.

Merry, M. S., & Merry, M. S. (2020). Educational Justice and Citizenship. *Educational Justice: Liberal Ideals, Persistent Inequality, and the Constructive Uses of Critique*, 89-121.

Mosharraf, M., & Haghighatkhah, F. H. (2023). Exploring Identity Theft: Motives, Techniques, and Consequents on Different Age Groups. *Journal of Innovations in Computer Science and Engineering (JICSE)*, *1*(1), 63-74.

Mulenga, R., & Shilongo, H. (2024). Academic integrity in higher education: Understanding and addressing plagiarism. *Acta Pedagogia Asiana*, *3*(1), 30-43.

Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality (JDIQ)*, *13*(1), 1-33.

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

Nugroho, M. A., Abdurohman, M., Erfianto, B., & Sulistiyo, M. D. (2023, August). Client-side virtual camera impersonation attacks detection on automatic proctoring exam. In *2023 11th International Conference on Information and Communication Technology (ICoICT)* (pp. 74-79). IEEE..

Oguguo, B. C., & Ocheni, C. A. (2024). Cybersecurity: a tool for curbing examination breaches and improvement of the quality of large-scale educational assessments. *Information Security Journal: A Global Perspective*, *33*(4), 359-373.

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *FUOYE Journal of Engineering and Technology*, *1*(1), 37-42.

Otekunrin, O., Okon, E., & Otekunrin, O. (2017). Analysis of Candidates' Performance in Unified Tertiary Matriculation Examinations (UTME) and Post-UTME in the University of Ibadan, Nigeria. *J Sci Res Reports*, *14*(5), 1-8.

Parikh, A. (2019). *Cloud security and platform thinking: an analysis of Cisco Umbrella, a cloud-delivered enterprise security* (Doctoral dissertation, Massachusetts Institute of Technology).

Pasquetto, I. V., Swire-Thompson, B., Amazeen, M. A., Benevenuto, F., Brashier, N. M., Bond, R. M., ... & Yang, K. C. (2020). Tackling misinformation: What researchers could do with social media data. *The Harvard Kennedy School Misinformation Review*.

Raman, R., Vachharajani, H., & Nedungadi, P. (2021). Adoption of online proctored examinations by university students during COVID-19: Innovation diffusion study. *Education and information technologies*, *26*(6), 7339-7358.

Randa, R., & Reyns, B. W. (2020). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey. *Deviant Behavior*, *41*(10), 1290-1304.

Saguin, K. I. (2019). Designing effective governance of education. *Policy design and practice*, *2*(2), 182-197.

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, *2*, 100034.

Seda, L. (2014). Identity theft and university students: do they know, do they care?. *Journal of Financial Crime*, *21*(4), 461-483.

Suleman, Q., Gul, R., Ambrin, S., & Kamran, F. (2015). Factors contributing to examination malpractices at secondary school level in Kohat Division, Pakistan. *Journal of Education and Learning*, *9*(2), 165-182.

Teitelbaum, K. (2020). *Critical issues in democratic schooling: Curriculum, teaching, and socio-political realities*. Routledge.

The Nation (2019, April 15). *JAMB releases results of 2019 mock UTME .April 2,2019.* https://thenationonlineng. net/breaking-jamb-releases-results-of-2019-mock-utme/.retrieved *4-2-25*.

Tunde, O. (2025).jamb blacklist six CBT officials for exam malpractice.Punch,10th, February ,2025.https://punchng.com/jamb-blacklists-six-cbt-officials-for-exam-malpractice/.retrieved 5-2-25

Ugobueze, A. N. (2024). Factors contributing to examination malpractice and its impact on educational standards in Nigeria. *Pakistan Journal of Educational Research*, *7*(2), 261-272.

Vanguard News. (2021, June 25). *JAMB Withholds Results of 62,000 Candidates Over Malpractice.* Retrieved from Vanguard News ,3-2-25

Votipka, D., Stevens, R., Redmiles, E., Hu, J., & Mazurek, M. (2018, May). Hackers vs. testers: A comparison of software vulnerability discovery processes. In *2018 IEEE Symposium on Security and Privacy (SP)"* (pp. 374-391). IEEE.

Wall, D. S. (2021). Cybercrime as a transnational organized criminal activity. In *Routledge handbook of transnational organized crime* (pp. 318-336). Routledge.

Whitcomb, K. M., Cwik, S., & Singh, C. (2021). Not all disadvantages are equal: Racial/ethnic minority students have largest disadvantage among demographic groups in both STEM and non-STEM GPA. *Aera Open*, *7*, 23328584211059823.

Williams, A. (2024). JAMB uncovers fraudulent admission practices by universities ,issues warning. Daily Post, Published on August 4, 2024 https://dailypost.ng/2024/08/04/iamb-uncovers-fraudulent-admission-practices-by-universities-issues-warning/.retrieved 2-2-25

Yaseen, K. A. Y. (2022). Digital education: The cybersecurity challenges in the online classroom (2019-2020). *Asian Journal of Computer Science and Technology*, *11*(2), 33-38.