JOURNAL OF BUSINESS MANAGEMENT AND ACCOUNTING
https://e-journal.uum.edu.my/index.php/jbma

How to cite this article:
Malik, M. S. & Ajape, M. K. (2026). Forensic accounting technologies and occupational fraud mitigation in the Nigerian maritime sector. *Journal of Business Management and Accounting*, *16*(2), 228-251. https://doi.org/10.32890/ jbma2026. 16.2.6

FORENSIC ACCOUNTING TECHNOLOGIES AND OCCUPATIONAL FRAUD MITIGATION IN THE NIGERIAN MARITIME SECTOR

[1]Muhammad Sidique Malik & [2]Mohammed Kayode Ajape
[1]Department of Accounting, University of Lagos, Nigeria
[2] Department of Accountancy, University of Johannesburg, Nigeria

Corresponding author: msodeeq@gmail.com

Received: 10/03/2026 Revised: 15/07/2026 Accepted: 22/07/2026 Published: 31/07/2026

ABSTRACT

This study examined how forensic accounting technologies influence the effectiveness of occupational fraud detection in the Nigerian maritime sector. Specifically, it investigated the effects of Artificial Intelligence-driven forensic analytics, blockchain-based transaction traceability, cybersecurity resilience, regulatory and audit enforcement, and organisational technology readiness on occupational fraud detection effectiveness. A quantitative research approach, grounded in the positivist paradigm, was adopted, using a cross-sectional survey design. The study conducted a census of 118 maritime organisations regulated by the Nigerian Maritime Administration and Safety Agency (NIMASA) and the Nigerian Shippers' Council, yielding 100 valid responses via a structured questionnaire. Data were analysed using descriptive statistics, Pearson Product-Moment Correlation, and multiple linear regression in SPSS at a 5% significance level. The findings revealed that all five dimensions of forensic accounting technologies had positive and statistically significant effects on occupational fraud detection effectiveness. Artificial intelligence-driven forensic analytics emerged as the strongest predictor ($\beta = 0.391$, $p < 0.001$), followed by blockchain-based transaction traceability, cybersecurity resilience, regulatory and audit enforcement, and organisational technology readiness. The regression model explained 63.0% of the variation in occupational fraud detection effectiveness ($R^2 = 0.630$). The study concludes that the integrated adoption of advanced forensic accounting technologies substantially strengthens fraud detection, transparency, accountability, and organisational governance within the Nigerian maritime sector.

The study contributes to knowledge by integrating the Fraud Diamond Theory and Agency Theory into a unified, technology-enabled framework and provides empirical evidence to support digital anti-fraud policies and governance reforms across the Nigerian maritime industry.

Keywords: Forensic accounting technologies, artificial intelligence, blockchain, occupational fraud detection, Nigerian maritime sector.

INTRODUCTION

Occupational fraud, defined by the Association of Certified Fraud Examiners as the use of deception to gain an unfair or unlawful advantage, is a pervasive global threat (Abdullahi & Mansor, 2018; Said et al., 2017). As digitalisation transforms financial systems, modern fraud schemes have become more complex and data-intensive, rendering traditional manual detection methods increasingly inadequate in digital contexts (Luka et al., 2025). The maritime industry is particularly exposed, owing to its complex documentation flows and multinational networks, making forensic accounting technologies a strategic priority.

Forensic accounting has increasingly evolved beyond its conventional litigation-support function into a strategic investigative discipline that integrates accounting, auditing, legal expertise, and digital analytical techniques to detect complex financial crimes, produce admissible evidence, and strengthen institutional accountability (Tijjani et al., 2023). The growing sophistication of financial misconduct has consequently elevated forensic accounting from a reactive investigative mechanism to a proactive governance tool that supports transparency and fraud prevention across both public and private organisations (Tijjani et al., 2023).

Globally, the adoption of forensic accounting technologies has accelerated across six interrelated pillars: artificial intelligence (AI), machine learning (ML), blockchain, cybersecurity, digital audit, and big data analytics (Daraojimba et al., 2023; Han et al., 2023). AI and ML techniques identify complex fraud patterns in historical data, enabling proactive, real-time transaction monitoring (Qader & Çek, 2024). Systematic reviews confirm that Naïve Bayes, Support Vector Machines, and Artificial Neural Networks are the most widely used ML algorithms for fraud detection (Ali et al., 2022). Blockchain reinforces these efforts through transparency, immutability, and tamper-resistant records, enabling real-time audit trails (Han et al., 2023; Qader & Çek, 2024). Cybersecurity safeguards fraud-prone processes against data breaches and ransomware during digital transformation (Saeed et al., 2023). Digital audit competencies strengthen fraud risk assessment, as information technology (IT) - skilled auditors detect unusual transactions more reliably (Razali et al., 2025). Big data analytics skills amplify forensic accounting knowledge, yielding superior fraud detection in digitised environments (Gao et al., 2024; Luka et al., 2025).

The maritime industry spans shipping, ports, logistics, marine transport, customs, cargo handling, and terminal operations, forming an interconnected ecosystem of counterparties, intermediaries, and cross-border financial flows. Structural weaknesses, poor segregation of duties, fragmented information systems, and geographically dispersed operations create fertile ground for occupational fraud (Lokanan & Maddhesia, 2024).

Consequently, occupational fraud in the maritime sector takes many forms: procurement fraud, payroll fraud, invoice manipulation, ghost workers, kickbacks, contract inflation, bribery, fuel theft, cargo diversion, and revenue leakages (Ali et al., 2022; Aros et al., 2024). Public procurement is particularly vulnerable: digital procurement systems enable transparency but generate vast datasets that fraudsters exploit, and most data-driven detection research focuses on collusion and favouritism (Santos et al., 2025). Traditional compliance-based audits cannot detect these schemes at scale.

Evidence from developing economies further shows that conventional auditing approaches are often inadequate for addressing sophisticated financial crimes, as they rely primarily on periodic compliance verification rather than continuous forensic investigation (Tijjani et al., 2023). As fraudulent schemes become increasingly technology-driven, organisations require investigative systems capable of detecting irregularities before they lead to substantial financial losses (Tijjani et al., 2023).

In Nigeria, the maritime sector remains highly vulnerable. Major agencies, including Nigerian Maritime Administration and Safety Agency (NIMASA), the Nigerian Shippers' Council, the Nigerian Ports Authority, the Nigeria Customs Service, terminal operators, and stevedoring companies, manage multibillion-naira contracts, tariffs, and concessions that are prone to manipulation (Adepoju, 2024; Iwuoha et al., 2022). Empirical studies of Nigerian public institutions indicate that forensic accounting techniques, such as data mining, trend analysis, and ratio analysis, are positively associated with fraud prevention and detection (Luka et al., 2025; Nelson et al., 2025).

Beyond technological capability alone, the successful deployment of forensic accounting depends on institutional conditions that foster the adoption of innovation. Conceptual evidence indicates that political commitment, adequate funding, enabling legislation, operational autonomy, competent personnel, and organisational capacity collectively determine whether investigative agencies adopt advanced forensic accounting practices (Umar et al., 2016).

These realities underscore the need for forensic accounting technologies grounded in AI, blockchain, cybersecurity, regulatory enforcement, and technology readiness. AI automates audit tasks and detects anomalies in real time, blockchain secures transaction records, cybersecurity protects digital audit trails, regulatory enforcement creates deterrents, and technology readiness determines how effectively maritime organisations operationalise these innovations (Luka et al., 2025; Qader & Çek, 2024; Saeed et al., 2023).

Institutional theory further suggests that organisations often adopt technological innovations not only to improve operational efficiency but also to meet regulatory expectations, strengthen organisational legitimacy, and respond to external governance pressures (Umar et al., 2016). Similarly, contingency theory holds that organisational characteristics, such as resource availability, managerial competence, and organisational size, influence the successful implementation of innovative fraud detection systems (Umar et al., 2016).

Despite growing scholarship, prior Nigerian studies have predominantly examined forensic accounting, internal control, audit quality, and corporate governance in isolation (Abrahams et al., 2024; Daraojimba et al., 2023; Odeyemi et al., 2024). Few studies have examined the integrated influence of AI, blockchain, cybersecurity, regulatory enforcement, and technology readiness on occupational fraud detection in Nigerian maritime organisations, revealing a clear empirical and contextual gap.

Furthermore, earlier Nigerian forensic accounting studies have concentrated primarily on taxpayer behaviour, tax compliance, public-sector accountability, and anti-corruption institutions, with relatively little empirical attention to technology-enabled fraud detection in the maritime industry. Likewise, conceptual studies on forensic accounting adoption have focused mainly on anti-corruption agencies rather than commercial maritime organisations, leaving an important sector-specific research gap that this study seeks to address (Tijjani et al., 2023; Umar et al., 2016).

This study examines the effectiveness of forensic accounting technologies in detecting occupational fraud in the Nigerian maritime sector. Specifically, it seeks to:

i. assess the influence of AI-driven forensic analytics on the effectiveness of occupational fraud detection within the Nigerian maritime sector.
ii. evaluate the contribution of blockchain-based transaction traceability to occupational fraud detection effectiveness within the Nigerian maritime sector.
iii. examine the influence of cybersecurity resilience on occupational fraud detection effectiveness within the Nigerian maritime sector.
iv. analyse the influence of regulatory and audit enforcement on occupational fraud detection effectiveness within the Nigerian maritime sector.
v. investigate the influence of organisational technology readiness on occupational fraud detection effectiveness within the Nigerian maritime sector.

The study extends forensic accounting theory into a sector-specific, technology-mediated context and provides practical guidance for maritime agencies deploying digital anti-fraud infrastructures.

LITERATURE REVIEW

Conceptual Review

The conceptual review that follows examines the core constructs underpinning forensic accounting technologies and the effectiveness of occupational fraud detection within the Nigerian maritime sector.

Forensic Accounting Technologies

Forensic accounting technologies are the integrated investigative tools and digital platforms used to detect, investigate, and prevent fraud in a legally admissible manner (Nelson et al., 2025). The discipline has evolved from manual, paper-based reconstructions to computer forensics, litigation support, and big-data analytics, driven by increasing fraud sophistication and the digitalisation of public finance in emerging economies such as Nigeria (Luka et al., 2025; Nelson et al., 2025). Its importance lies in producing evidence-based findings that deter unethical behaviour and strengthen accountability within fraud-prone institutions (Nelson et al., 2025).

Artificial Intelligence (AI) Driven Forensic

AI-driven forensic analytics applies machine learning and deep learning to large financial datasets to identify fraud patterns. Naïve Bayes, Support Vector Machines, and Artificial Neural Networks remain the most widely deployed algorithms across credit card, insurance, and financial statement fraud systems (Ali et al., 2022). Graph neural networks extend this capability by capturing relational patterns among transacting parties, significantly outperforming rule-based detection (Cheng et al., 2024). Benefits include automated continuous monitoring and reduced false positives (Qader & Çek, 2024), while challenges persist with imbalanced datasets, model interpretability, and data quality (Ali et al., 2022; Qader & Çek, 2024).

Blockchain-Based Transaction Traceability

Blockchain-based transaction traceability is a distributed-ledger technology in which validated transactions are hashed and appended to an immutable chain, producing tamper-resistant audit trails (Han et al., 2023). Its architecture integrates hash algorithms, public and private keys, decentralised nodes, and consensus protocols to ensure transparency and real-time visibility (Han et al., 2023). Smart contracts are self-executing agreements whose terms are encoded on the ledger, enabling automated compliance and faster transaction settlement (Han et al., 2023; Qader & Çek, 2024). The technology supports fraud minimisation, counter-party risk reduction, and improved regulatory efficiency (Han et al., 2023), while facilitating continuous, real-time monitoring for suspicious fund transfers (Qader & Çek, 2024).

Cybersecurity Resilience Framework

A cybersecurity resilience framework guides institutions in identifying, protecting, detecting, responding to, and recovering from cyber threats, and is anchored in global standards such as the NIST Cybersecurity Framework and ISO 27001 (Saeed et al., 2023). Maturity models guide organizations from ad hoc responses and basic controls to planned strategies and, ultimately, to optimised postures featuring continuous penetration testing and vulnerability monitoring (Saeed et al., 2023). In forensic accounting, such frameworks safeguard digital evidence through chain-of-custody documentation, write-blocking, and bit-stream imaging, ensuring its admissibility in court proceedings (Nelson et al., 2025).

Regulatory and Audit Enforcement

Regulatory and audit enforcement captures how internal audit, external audit, compliance regimes, whistleblowing channels, and sanctions collectively deter fraud (Bonrath & Eulerich, 2024). Internal audit ranks among the top three recipients of whistleblowing reports and serves as a core anti-fraud control, whereas external auditors' effectiveness may be hampered by their detachment from the audited entity (Bonrath & Eulerich, 2024). Effective whistleblowing systems signal organisational intolerance of fraud and increase the perceived risk of detection, while sanctions raise the expected cost of misconduct (Bonrath & Eulerich, 2024).

Organisational Technology Readiness

Organisational technology readiness reflects a firm's capacity to deploy digital forensic tools, encompassing management support, workforce training, IT infrastructure, and an innovation-supportive culture (Díaz-Arancibia et al., 2024). In many developing-country firms, knowledge and skills gaps remain the principal barrier to adoption (Díaz-Arancibia et al., 2024).

Occupational Fraud Detection Effectiveness

Occupational fraud detection effectiveness refers to an organisation's capability to uncover occupational fraud through structured detection, investigation, and prevention activities guided by fraud-risk indicators (Bonrath & Eulerich, 2024; Luka et al., 2025). Effectiveness is enhanced when big data analytics skills mediate forensic accounting knowledge, yielding timelier and more accurate investigative outputs in digitised financial environments (Luka et al., 2025).

Theoretical Review

The study is grounded in the Fraud Diamond Theory and the Agency Theory. The Fraud Diamond Theory explains the behavioural and organisational conditions that facilitate occupational fraud, while the Agency Theory illuminates the principal–agent relationship and the governance mechanisms that minimise information asymmetry. Together, they provide a robust framework for understanding how forensic accounting technologies enhance the effectiveness of occupational fraud detection in the Nigerian maritime sector.

Fraud Diamond Theory

Wolfe and Hermanson extended Cressey's Fraud Triangle by introducing the Fraud Diamond Theory, adding Capability, arguing that occupational fraud requires not only pressure, opportunity and rationalisation but also the knowledge, authority, and technical ability to bypass controls (Firdaus et al., 2022). The four components are Pressure (financial strain, performance pressure, personal obligations, lifestyle demands), Opportunity (weak controls, poor governance, monitoring gaps, information asymmetry), Rationalisation (culture-driven ethical justification), and Capability (technical expertise and positional authority) (Firdaus et al., 2022). In maritime organisations, these conditions manifest as procurement fraud, payroll fraud, contract inflation, cargo diversion, and billing manipulation. The theory maps onto the study's variables: AI-driven forensic analytics and blockchain traceability compress Opportunity, cybersecurity resilience constrains Capability, regulatory and audit enforcement weakens Rationalisation, and organisational technology readiness undermines concealment. Strengths include a comprehensive scope and compatibility with technology-enabled detection, limitations include a behavioural orientation and the absence of a principal–agent perspective, which are addressed by the Agency Theory.

Agency Theory

Jensen and Meckling formulated Agency Theory as a nexus of contracts model in which principals (owners) delegate authority to agents whose self-interested pursuit generates information asymmetry, moral hazard, and adverse selection, producing monitoring costs, bonding costs, and residual loss (Han et al., 2023). The theory has been applied in audit contexts to demonstrate how AI and blockchain reduce information asymmetry, mitigate agency conflicts, and enhance monitoring and accountability (Qader & Çek, 2024). In Nigerian maritime operations, where owners, managers, employees, contractors, stevedores, shipping agents, and terminal operators interact under regulated port concessions, these conflicts surface as vendor fraud, kickbacks, payroll fraud, revenue diversion, and asset misappropriation (Iwuoha et al., 2022). Forensic accounting technologies mitigate these agency problems: AI-driven forensic analytics enables continuous monitoring, blockchain produces immutable records that reduce information asymmetry, cybersecurity frameworks safeguard the integrity of audit evidence (Saeed et al., 2023), regulatory enforcement imposes sanctions, and organisational technology readiness provides the capability to operationalise these controls. Strengths include emphasis on governance and monitoring, critics note its assumption of self-interest, neglect of culture, and over-reliance on monitoring.

Synthesis and Justification of the Underpinning Theory

The Fraud Diamond Theory underpins this study because it directly explains the behavioural conditions that facilitate occupational fraud and is particularly suited to examining how AI-driven forensic analytics, blockchain transaction traceability, cybersecurity resilience, regulatory and audit enforcement, and organisational technology readiness reduce fraud opportunities, constrain offenders' capabilities, and improve the effectiveness of occupational fraud detection in the Nigerian maritime sector. The Agency Theory complements this perspective by clarifying how these technologies strengthen monitoring, reduce information asymmetry, enhance accountability, and minimise principal–agent conflicts. Together, the two theories form a comprehensive framework for explaining the adoption of forensic accounting technologies and their contribution to the effectiveness of occupational fraud detection within the maritime industry in Nigeria.

Empirical Review

This section reviews empirical studies on forensic accounting technologies and the effectiveness of occupational fraud detection. It is organised around the study's specific objectives, namely AI-driven forensic analytics, blockchain-based transaction traceability, cybersecurity resilience, regulatory and audit enforcement, and organisational technology readiness. It synthesises findings, highlights methodological approaches, identifies inconsistencies, and establishes the research gaps addressed by the present study.

AI-Driven Forensic Analytics and Occupational Fraud Detection Effectiveness

Cheng et al. (2024) conducted a systematic literature review (SLR) and proposed a unified taxonomy to assess the effectiveness of Graph Neural Networks in financial fraud detection. While their findings suggest that GNNs outperform rule-based methods in relational fraud, the study lacks specific evidence from the maritime sector. Focusing on audit quality, Qader & Çek (2024) surveyed Turkish audit professionals and utilised partial least squares structural equation modelling to demonstrate that AI positively influences real-time anomaly detection. From a supply-chain perspective, Lokanan & Maddhesia (2024) employed thematic synthesis to conclude that machine learning and AI detect fraud patterns often invisible to manual reviews, though their work lacks direct maritime application. Similarly, Gao et al. (2024) applied a PRISMA-based review to highlight that bagging and boosting ensemble strategies enhance financial-estimating models, although they remain reliant on secondary sources. In the Nigerian context, Luka et al. (2025) utilised a cross-sectional survey of public-sector professionals to establish that big data analytics skills directly improve fraud-prevention performance, though the focus on the public sector limits broader private-sector inferences. Addressing algorithmic dominance, Ali et al. (2022) conducted a systematic literature review and found that Naïve Bayes, Support Vector Machines, and Artificial Neural Networks are the most prevalent algorithms, noting that imbalanced datasets can often impair model accuracy. Finally, Hernández-Aros et al. (2024) conducted a systematic literature review showing that while 56 per cent of global firms have experienced fraud, AI significantly accelerates detection speeds; however, their study lacks specific African evidence.

The reviewed literature consistently indicates that AI enhances anomaly detection, minimises false positives, and enables real-time transaction monitoring. While inconsistencies remain regarding accuracy under class imbalance, the collective findings suggest that Nigerian maritime firms could significantly leverage AI to address port transactions and invoicing irregularities. The following subsection examines how distributed-ledger technology reinforces these detection gains.

Blockchain-Based Transaction Traceability and Occupational Fraud Detection Effectiveness

Han et al. (2023) conducted a literature review on the impact of blockchain and AI on auditing, utilising thematic synthesis to demonstrate how blockchain facilitates continuous auditing and real-time assurance, though they noted a predominant theoretical emphasis in current research. Similarly, Qader & Çek (2024) utilised structural equation modelling to assess blockchain's effect on audit quality within Turkish audit firms, finding that transparency, immutability, and smart contracts effectively reduce fraud, although the study is limited by Turkey-specific context bias. Focusing on the Nigerian maritime sector, Iwuoha et al. (2022) employed qualitative content analysis to examine port-concession regulations, revealing that regulatory gaps in the Nigerian Ports Authority frameworks enable terminal-operator rent-seeking, albeit with limited quantitative evidence of fraud. Further examining regional constraints, Adepoju (2024) identified efficiency barriers in Nigerian seaport-hinterland logistics, highlighting how congestion, insecurity, piracy, and inefficient clearance compromise supply-chain integrity. Beyond specific sector studies, conceptual research by Dai & Vasarhelyi, cited in Han et al. (2023), underscores how blockchain models support automatic assurance and reliable audit trails, while Kokina and his co-authors, also cited in Han et al. (2023), emphasise the technology's capacity to reduce human error and improve operational efficiency.

The reviewed literature consistently indicates that blockchain improves audit-trail reliability, transparency, and the reduction of counterparty risk. Nevertheless, implementation challenges such as scalability, high costs, regulatory complexity, and skill gaps continue to hinder uptake in developing countries, where empirical evidence, particularly in the Nigerian maritime context, remains scarce. Notwithstanding these barriers, the technology's decentralised structure offers significant potential to mitigate fraud at port-concession interfaces, which aligns closely with the need for robust cyber-threat protection.

Cybersecurity Resilience and Occupational Fraud Detection Effectiveness

Saeed et al. (2023) conducted a PRISMA-based systematic literature review to examine the cybersecurity implications of digital transformation. Using thematic synthesis, they demonstrated that robust cybersecurity safeguards operational efficiency, prompting the proposal of a four-tier readiness framework; however, the study is limited by a lack of empirical evidence from the African continent. Similarly, Abrahams et al. (2024) employed an SLR to examine the intersection of regulatory compliance and cybersecurity in global accounting, finding that the convergence of these frameworks strengthens financial statement integrity, although their work remains primarily conceptual.

Focusing on the Nigerian context, Afrogha and his co-authors conducted a qualitative comparative review of forensic accounting practices, concluding that computer forensics and chain-of-custody protocols provide essential safeguards for digital evidence (Nelson et al., 2025). While this research offers granular detail on Nigerian forensic practices, it does not explicitly address the maritime context. In a United State (US) study, Daraojimba et al. (2023) conducted a conceptual review and concluded that ICT-based tools significantly accelerate detection speeds, though the findings remain U.S.-centric. Complementary literature supports these insights, Uddin and his co-authors, as cited in Saeed et al. (2023), highlighted how cyber-weaknesses impair banking operations, while Krutilla and his co-authors, also cited in Saeed et al. (2023), established that enhanced cost-benefit models improve cybersecurity investment decisions.

The reviewed literature shows that cybersecurity maturity, incident-response capability, and digital-evidence preservation are consistently associated with improved fraud detection. Although evidence from developing countries remains scarce, these findings establish that cybersecurity provides a necessary foundation for regulatory enforcement, as examined in the following subsection.

Regulatory and Audit Enforcement and Occupational Fraud Detection Effectiveness

Bonrath and Eulerich (2024) provide a theoretical-empirical analysis of the internal audit function, identifying it as a primary anti-fraud control and a top recipient of whistleblowing reports, though they note that external auditors' detachment can limit detection efficacy. Within the Nigerian public sector, Abdullahi & Mansor (2018) utilised structural equation modelling among 302 staff to confirm that pressure, opportunity, and rationalisation drive fraud, while Olaniyan and his co-authors, as cited in Nelson et al. (2025), further highlight that forensic accounting positively impacts fraud prevention. Regarding the impact of digital competence and ethical values, Razali et al. (2025) found that proficiency with digital tools significantly strengthens fraud-risk assessment among Malaysian auditors and Said et al. (2017) demonstrated that ethical values enhance fraud-detection effectiveness in the Malaysian banking sector. Furthermore, Ewa, as cited in Nelson et al. (2025), observed that data mining, trend, and ratio analyses are positive predictors of fraud prevention within Nigerian ministries, departments, and agencies.

Regulatory enforcement, internal-audit rigour, and whistleblowing consistently reinforce fraud governance. Public-sector evidence dominates the literature, with maritime-specific Nigerian research remaining scarce. These frameworks necessitate organisational technology readiness to succeed.

Organisational Technology Readiness and Occupational Fraud Detection Effectiveness

Díaz-Arancibia et al. (2024) conducted an SLR on technology adoption among SMEs in developing countries, finding that although digital transformation is multidisciplinary, knowledge and skill gaps remain the most significant barriers. In this context, Lukongan and his co-authors, as cited in Díaz-Arancibia (2024), and Rahayu and his co-authors, as cited in Díaz-Arancibia et al. (2024), demonstrate that perceived usefulness, compatibility, and technology-organisation-environment factors are key drivers of adoption. Regarding professional capability, Razali et al. (2025)confirm that auditor competence and digital proficiency enhance fraud-risk assessment. Specifically, within Nigeria, Luka et al. (2025) observe that while digitised platforms increase data intensity, organisational readiness is the decisive factor for achieving performance gains. Conversely, Afrogha et al. (2025) highlight that institutional resistance and political interference often curtail the uptake of forensic accounting in the

Nigerian context. Collectively, these studies indicate that management support, infrastructure, competence, and a culture of innovation are fundamental to readiness, which underpins the successful implementation of forensic technology in maritime firms.

Comparative Analysis of Empirical Studies

Studies agree on AI's gains in anomaly detection (Ali et al., 2022; Cheng et al., 2024), blockchain's value for audit trails (Han et al., 2023; Qader & Çek, 2024), cybersecurity's protection of evidence (Nelson et al., 2025; Saeed et al., 2023), the compliance effect of regulatory enforcement (Abdullahi & Mansor, 2018; Bonrath & Eulerich, 2024), and readiness's moderating role (Díaz-Arancibia et al., 2024; Luka et al., 2025). Nigerian forensic accounting work highlights chain-of-custody protocols as essential to digital evidence integrity (Nelson et al., 2025), while broader digital transformation research confirms that tiered readiness frameworks enable secure financial data handling (Saeed et al., 2023).

Conflicting findings emerge along contextual and methodological lines. Geographic setting yields divergent magnitudes: the Turkish PLS-SEM study reports stronger AI-audit-quality coefficients (Qader & Çek, 2024), whereas Nigerian cross-sectional MDA work using ordinary least squares (OLS) reports comparatively modest effects (Abdullahi & Mansor, 2018; Nelson et al., 2025). Sectoral orientation further differentiates results; Malaysian external-auditor SEM evidence (Razali et al., 2025) contrasts with Nigerian public-sector forensic accounting studies (Nelson et al., 2025) and with global systematic literature reviews dominated by Naïve Bayes, SVM, and ANN benchmarks (Ali et al., 2022). Sample composition also varies: Malaysian auditors (n = 150) (Razali et al., 2025) versus Nigerian MDA personnel (Abdullahi & Mansor, 2018) versus broader bibliometric samples (Ali et al., 2022). Cross-sectional surveys dominate (Abdullahi & Mansor, 2018; Razali et al., 2025), whereas longitudinal or archival fraud-detection evidence remains scarce. Internal-audit function research emphasises whistleblowing prevalence as a global anti-fraud control (Bonrath & Eulerich, 2024), whereas Nigerian studies foreground institutional and political interference as constraining factors (Nelson et al., 2025). Analytical preferences favour covariance-based SEM (Qader & Çek, 2024; Razali et al., 2025) rather than deep-learning evaluations of maritime fraud data (Cheng et al., 2024). Methodologically, surveys dominate (Abdullahi & Mansor, 2018; Razali et al., 2025), whereas longitudinal or archival datasets are rare. These differences confirm that integrated maritime-Nigerian empirical evidence on AI, blockchain, cybersecurity, regulation, and readiness remains thin, motivating the present study.

Research Gap

Despite the growing body of literature on forensic accounting technologies and fraud detection, several important gaps remain. Methodologically, existing studies have relied predominantly on cross-sectional survey designs, limiting the ability to examine how the effectiveness of forensic accounting technologies evolves over time. For example, Abdullahi and Mansor employed Structural Equation Modelling (SEM) using data collected from 302 respondents in Kano State Ministries, Departments and Agencies (MDAs) at a single point in time, while Razali and his co-authors utilised Partial Least Squares Structural Equation Modelling (PLS-SEM) with 150 Malaysian auditors, without incorporating longitudinal evidence. Consequently, advanced analytical approaches such as hierarchical regression, panel data analysis and longitudinal modelling remain largely unexplored within maritime fraud research (Abdullahi & Mansor, 2018; Razali et al., 2025).

From a contextual perspective, previous empirical studies have focused primarily on the banking, insurance and public-sector MDA environments, with relatively little attention devoted to the Nigerian maritime industry. While studies have highlighted operational challenges such as seaport congestion, logistics inefficiencies and port-concession governance, stevedoring companies, terminal operators and shipyards have received limited empirical investigation as occupational fraud environments (Abdullahi & Mansor, 2018; Adepoju, 2024; Iwuoha et al., 2022; Nelson et al., 2025; Said et al., 2017). Theoretically, prior research has largely examined fraud using either the Fraud Triangle Theory or the Technology Acceptance Model (TAM) independently, with little attempt to integrate the complementary insights of the Fraud Diamond Theory and Agency Theory to explain technology-enabled detection of occupational fraud (Abdullahi & Mansor, 2018; Díaz-Arancibia et al., 2024).

Furthermore, a significant variable gap exists because no previous Nigerian maritime study has examined the combined effects of AI-driven forensic analytics, blockchain-based transaction traceability, cybersecurity resilience, regulatory and audit enforcement, and organisational technology readiness within a unified analytical framework. Empirically, the literature also reports inconsistent findings on the effectiveness of forensic accounting technologies. For instance, studies conducted in Turkey reported stronger effects of artificial intelligence on audit quality, whereas Nigerian public-sector studies found comparatively weaker relationships, indicating the need for additional empirical evidence within the maritime context (Abdullahi & Mansor, 2018; Nelson et al., 2025; Qader & Çek, 2024). Finally, existing policy recommendations remain largely generic and seldom provide sector-specific guidance for key maritime stakeholders such as the Nigerian Maritime Administration and Safety Agency (NIMASA), the Nigerian Shippers' Council (NSC), terminal operators, shipyards and stevedoring companies. These methodological, contextual, theoretical, variable, empirical and policy gaps collectively justify the need for the present study.

Contribution of the Present Study to Existing Literature

By integrating Fraud Diamond Theory and Agency Theory into a multivariate Nigerian maritime model, this study provides original empirical evidence on AI analytics, blockchain traceability, cybersecurity resilience, regulatory enforcement, and organisational readiness, offering policy-actionable guidance for NIMASA, the Nigerian Shippers' Council, terminal operators, and stevedoring firms.

METHODOLOGY

This section presents the research methodology adopted for this study. It outlines the research design, population, sampling procedure, data collection methods, validity and reliability procedures, operationalisation of variables, data analysis methods, model specification, and limitations of the research methods.

The study adopted a quantitative research approach within the positivist philosophical paradigm and employed deductive reasoning because the hypotheses were derived from the Fraud Diamond Theory and Agency Theory and subjected to empirical testing. A cross-sectional survey design was considered appropriate because data were collected from respondents at a single point in time using a structured questionnaire. The design incorporated descriptive, correlational and explanatory components, thereby enabling the study to describe respondents' perceptions, examine relationships among variables and determine the influence of forensic accounting technologies on the effectiveness of occupational fraud detection.

The target population comprised 118 maritime companies regulated by the NIMASA and the Nigerian Shippers' Council (Anagor-Ewuzie, 2023; NIMASA, 2025). These organisations were selected because they handle high-value transactions and operate sophisticated digital financial systems vulnerable to occupational fraud. The unit of analysis was the organisation, represented by a knowledgeable senior officer in Finance, Accounting, Internal Audit, Compliance, Risk Management, Operations, or Information Technology.

Table 1

Population Table

Category	**Number**
Stevedoring Companies	65
Terminal/Jetty Operators	26
Shipyards	27
Total	118

Source: NIMASA (2025)

A census approach was adopted to eliminate sampling error by covering the entire study population. Purposive sampling was then used to select one senior officer from each organisation with adequate knowledge of fraud risk management and forensic accounting technologies. A total of 118 questionnaires were administered, of which 100 were correctly completed and returned, yielding a response rate of 84.75 per cent.

Primary data were collected using a self-administered, structured questionnaire distributed both in person and electronically between June and September 2025. Participation was voluntary, and respondents were assured of confidentiality and anonymity. The instrument, divided into 8 sections (A-H), consisted exclusively of questions measured on a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

Content and face validity of the instrument were established through expert review, and reliability was assessed using a pilot study and Cronbach's alpha. All constructs exceeded the acceptable threshold of $\alpha \geq 0.70$, indicating satisfactory internal consistency as contained in Table 2. The measurement instrument demonstrated strong reliability and satisfactory construct validity. Cronbach's alpha coefficients ranged from 0.833 to 0.890, exceeding the recommended threshold of 0.70 and confirming excellent internal consistency across all constructs. Construct validity was supported by a KMO value of 0.848, a statistically significant Bartlett's Test of Sphericity ($\chi^2 = 1731.041$, df = 435, $p < 0.001$).

Table 2

Reliability Measurement

Variable	Items	α	KMO	Bartlett's χ^2	D.F	P-value
AIFA (C1-C5)	5	0.890	0.848	1731.041	435	<0.001
BBTT (D1-D5)	5	0.873				
CSRF (E1-E5)	5	0.857				
RAES (F1-F5)	5	0.850				
OTR (G1-G5)	5	0.833				
OFDE (H1-H5)	5	0.868				
Overall Reliability	30	0.862				

Source: Researchers (2026)

Composite mean scores were computed for each construct from the respective Likert-scale items, with higher scores indicating stronger agreement. The operationalisation of the study's variables is presented in Table 3.

Table 3

Operationalisation of Study Variable

Variable	Type	Proxy	Construct Domain	Measurement
Occupational Fraud Detection Effectiveness	Dependent	OFDE	Timely detection, investigation, continuous monitoring, whistleblowing and post-incident learning	5-item Likert (H1–H5); composite mean
AI-Driven Forensic Analytics Adoption	Independent	AIFA	Automated anomaly detection, analytics-driven audit, full-population testing, operational analytics and triage workflow	5-item Likert (C1–C5); composite mean
Blockchain-Based Transaction Traceability	Independent	BBTT	Tamper-resistant approvals, traceability, audit evidence retrieval, reconciliation and rule-based controls	5-item Likert (D1–D5); composite mean
Cybersecurity Resilience Frameworks	Independent	CSRF	Asset inventory, authentication, encryption, monitoring and incident response	5-item Likert (E1–E5); composite mean
Regulatory and Audit Enforcement Strength	Independent	RAES	Audit independence, management follow-up, policy enforcement, oversight and sanctions	5-item Likert (F1–F5); composite mean
Organisational Technology Readiness	Independent	OTR	Skills, training, infrastructure, management support and change capability	5-item Likert (G1–G5); composite mean

Source: Researchers (2026)

The completed questionnaires were coded, cleaned and analysed using the Statistical Package for the Social Sciences (SPSS). Preliminary analyses included data screening, assessment of missing values and outlier detection. Descriptive statistics summarised respondent characteristics and study variables, while Pearson Product-Moment Correlation examined relationships among variables and assessed potential multicollinearity. Multiple linear regression was used to evaluate the influence of the five independent variables on occupational fraud detection effectiveness. Statistical decisions were made at the 5 per cent level of significance ($p < 0.05$).

Model Specification

The study employed a multiple linear regression model specified as:

$$OFDE = \beta_0 + \beta_1 AIFA + \beta_2 BBTT + \beta_3 CSRF + \beta_4 RAES + \beta_5 OTR + \varepsilon$$

Where OFDE denotes Occupational Fraud Detection Effectiveness, AIFA denotes AI-Driven Forensic Analytics, BBTT denotes Blockchain-Based Transaction Traceability, CSRF denotes Cybersecurity Resilience Frameworks, RAES denotes Regulatory and Audit Enforcement Strength, OTR denotes Organisational Technology Readiness, β_0 is the constant term, β_1–β_5 are the regression coefficients, and ε represents the stochastic error term.

The a priori expectation is:

$$\beta_1, \beta_2, \beta_3, \beta_4, \beta_5 > 0$$

Based on the empirical regression results, the estimated model is:

$$OFDE = -0.710 + 0.391AIFA + 0.268BBTT + 0.207CSRF + 0.171RAES + 0.143OTR + \varepsilon$$

The estimated model indicates that all explanatory variables exert positive effects on occupational fraud detection effectiveness, thereby confirming the study's a priori expectations.

Limitations of the Research Methods

Although the methodology was appropriate for achieving the study’s objectives, certain limitations should be acknowledged. The cross-sectional design limits causal inference because data were collected at a single point in time. The reliance on self-reported responses introduces the possibility of social desirability and common method bias. Furthermore, one respondent per organisation implies that some organisational perspectives may not have been fully captured. The focus on stevedoring companies, terminal operators and shipyards limits the generalisability of the findings to other maritime subsectors. Finally, although the response rate of 84.75 per cent was considered high, the possibility of non-response bias arising from the eighteen unreturned questionnaires cannot be completely eliminated.

DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS

This section presents the study's empirical findings, based on respondents' perceptions of the effectiveness of occupational fraud detection rather than on objectively reported fraud cases. It also provides the demographic profile of respondents, who were purposively selected from finance, audit, compliance, operations, and information technology functions due to their direct involvement in fraud risk management and forensic accounting technologies.

Table 4

Summary of Respondent Characteristics

Characteristic	Category	Frequency	Percentage (%)
Gender	Male	75	75.0
	Female	25	25.0
Role	Finance	18	18.0
	Accounting	17	17.0
	Internal Audit/Compliance/Risk	25	25.0
	Operations	25	25.0
	Information Technology	15	15.0
Years of Experience in Maritime	Less than 2 years	8	8.0
	2–5 years	16	16.0
	6–10 years	37	37.0
	11–15 years	18	18.0
	Above 15 years	21	21.0
Years of Experience in Current Employment	Less than 2 years	14	14.0
	2–5 years	24	24.0
	6–10 years	32	32.0
	11–15 years	16	16.0
	Above 15 years	14	14.0
Educational Qualification	SSCE	16	16.0
	OND/NCE	37	37.0
	HND/B.Sc.	14	14.0
	MBA/M.Sc.	5	5.0
	Professional/PhD	28	28.0
Fraud Risk Management Involvement	Not involved	2	2.0
	Low	11	11.0
	Moderate	28	28.0
	High	34	34.0
	Final decision authority	25	25.0
Technology Decision Involvement	Not involved	7	7.0
	Low	14	14.0
	Moderate	25	25.0
	High	38	38.0
	Final authority	16	16.0

Source: Researchers (2026)

Table 4 shows that respondents were predominantly male (75%) and were drawn from key functional areas, including Finance, Accounting, Internal Audit/Compliance/Risk, Operations, and Information Technology. Most respondents had substantial industry experience, with 37% having 6–10 years of maritime experience and 32% having 6–10 years in their current employment. In terms of educational attainment, the majority held OND/NCE (37%) or Professional/PhD (28%) qualifications. Furthermore, a significant proportion of respondents reported high or final decision-making involvement in both fraud risk management (59%) and technology decisions (54%). Overall, respondents possess the relevant expertise, experience, and organisational responsibilities required to provide reliable information for the study.

Table 5

Summary of Organisational Characteristics

Characteristic	Category	Frequency	Percentage (%)
Organisation Type	Stevedoring Company	58	58.0
	Terminal/Jetty Operator	20	20.0
	Shipyard	22	22.0
Ownership	Private Nigerian	57	57.0
	Foreign-owned	9	9.0
	Joint Venture	17	17.0
	Government-linked	13	13.0
	Others	4	4.0
Firm Size	1–49 employees	24	24.0
	50–199 employees	37	37.0
	200–499 employees	22	22.0
	500–999 employees	13	13.0
	1,000+ employees	4	4.0
Location	Lagos Axis	46	46.0
	South-South	33	33.0
	South-West	7	7.0
	South-East	5	5.0
	Others	9	9.0
Digitalisation Level	Very Low	8	8.0
	Low	11	11.0
	Moderate	22	22.0
	High	30	30.0
	Very High	29	29.0
Internal Audit Structure	Fully In-house	54	54.0
	Co-sourced	14	14.0
	Outsourced	18	18.0
	Ad-hoc	12	12.0
	None	2	2.0

Source: Researchers (2026)

Table 5 shows that the majority of respondents were from Stevedoring Companies (58%), with most organisations being privately Nigerian owned (57%). The largest proportion of firms employed 50–199 staff (37%) and were located within the Lagos Axis (46%). Furthermore, most organisations reported high or very high levels of digitalisation (59%), while 54% maintained a fully in-house internal audit structure. Overall, the findings indicate that the participating organisations possess the operational, technological, and governance characteristics necessary to provide reliable information for assessing the influence of forensic accounting technologies on the effectiveness of occupational fraud detection in the Nigerian maritime industry.

Table 6

Descriptive Statistics of Study Variables

Variable	Mean	SD	Minimum	Maximum	Rank
AIFA	4.026	0.869	1.40	5.00	2
BBTT	4.028	0.840	1.60	5.00	1
CSRF	4.018	0.842	1.40	5.00	4
RAES	4.024	0.868	1.00	5.00	3
OTR	4.010	0.839	1.40	5.00	5
OFDE	4.042	0.862	1.20	5.00	—

Source: Researchers (2026)

Following preliminary data screening, the dataset was found to be suitable for inferential analysis. Missing responses were negligible, yielding 100 valid observations. Diagnostic tests based on standardised residuals, Mahalanobis distance, and Cook's distance identified no influential outliers. In addition, the skewness values (−0.896 to −1.146) and kurtosis values (0.246 to 0.997) (Table 7) were within the recommended thresholds, indicating that the data were approximately normally distributed. Also, the extraction of six components together explained 67.474% of the total variance, exceeding the recommended 60% benchmark. Furthermore, the questionnaire items generally exhibited strong factor loadings on their respective constructs, providing evidence of good convergent validity. Although one OFDE item showed a relatively low factor loading, its acceptable communality and a stronger Structure Matrix loading justified its retention. Overall, the findings confirm that the research instrument is reliable, valid, and suitable for subsequent correlation and multiple regression analyses. Consequently, the normality assumption was satisfied, confirming the dataset's suitability for parametric analyses, including Pearson correlation and multiple linear regression.

Table 7

Normality Statistics

Variable	Skewness	Kurtosis	Eigenvalue	% Variance	Cumulative %	Factor Loading Range
AIFA	-0.896	0.246	9.337	31.124	31.124	0.672–0.971
BBTT	-0.989	0.455	3.002	10.008	41.132	0.727–0.887
CSRF	-1.050	0.663	2.604	8.680	49.812	0.623–0.894
RAES	-1.137	0.901	2.381	7.936	57.748	0.642–0.833
OTR	-1.096	0.787	1.851	6.169	63.917	0.733–0.831
OFDE	-1.146	0.997	1.067	3.558	67.474	0.351–0.856

Source: Researchers (2026)

Table 8 presents the results of Harman's Single-Factor Test, conducted to assess common method bias (CMB) in the study. The analysis included 30 measurement items, from which six factors with eigenvalues greater than one were extracted. The first factor accounted for 31.124% of the total variance, well below the recommended threshold of 50%. This indicates that no single factor dominates the variance in the data, suggesting that common method bias is not a significant concern. Therefore, the relationships among the study variables are unlikely to have been materially influenced using a common measurement method, and the data are considered suitable for subsequent correlation and regression analyses.

Table 8

Harman's Single-Factor Test

Statistic	Value
Number of Measurement Items	30
Number of Factors Extracted	6
Variance Explained by First Factor	31.124%
Recommended Threshold	<50%
Decision	No Serious Common Method Bias

Source: Researchers (2026)

Table 9 shows that all independent variables are positively and significantly associated with Occupational Fraud Detection Effectiveness. Artificial Intelligence Analytics (AIFA) exhibits the strongest association ($r = 0.664$, $p < 0.01$), followed by Blockchain-Based Traceability Technologies (BBTT) ($r = 0.557$, $p < 0.01$), Cybersecurity Resilience Framework (CSRF) ($r = 0.486$, $p < 0.01$), Organisational Technology Readiness (OTR) ($r = 0.440$, $p < 0.01$), and Regulatory and Audit Enforcement Systems (RAES) ($r = 0.364$, $p < 0.01$). The moderate intercorrelations among the independent variables indicate the absence of serious multicollinearity, suggesting that the variables are suitable for subsequent multiple regression analysis.

Table 9

Pearson Correlation Matrix

Variables	AIFA	BBTT	CSRF	RAES	OTR	OFDE
AIFA	1.000					
BBTT	0.442**	1.000				
CSRF	0.303**	0.339**	1.000			
RAES	0.217*	0.124	0.227*	1.000		
OTR	0.396**	0.223*	0.257**	0.198*	1.000	
OFDE	0.664**	0.557**	0.486**	0.364**	0.440**	1.000

Correlation is significant at $p < 0.01$
Source: Researchers (2026)

Table 10 indicates that the assumptions underlying multiple linear regression were met. The tolerance values (0.691–0.915) and VIF values (1.093–1.446) confirm the absence of multicollinearity, while the Durbin-Watson statistic of 1.936 indicates no significant autocorrelation among the residuals. Furthermore, the histogram, Normal P–P plot, residual scatterplots, and partial regression plots confirm the assumptions of normality, homoscedasticity, and linearity. Overall, these diagnostic results demonstrate that the OLS regression model is appropriate and that the estimated coefficients are reliable and unbiased.

Table 10

Multicollinearity Diagnostics

Variable	**Tolerance**	**VIF**	Durbin-Watson
AI-Driven Forensic Analytics	0.691	1.446	
Blockchain-Based Transaction Traceability	0.758	1.320	
Cybersecurity Resilience Framework	0.817	1.224	1.936
Regulatory and Audit Enforcement Strength	0.915	1.093	
Organisational Technology Readiness	0.814	1.229	

Source: Researchers (2026)

Following confirmation that the regression assumptions were met, multiple linear regression was conducted in SPSS using the Enter Method. The model showed a strong positive relationship between the explanatory variables and Occupational Fraud Detection Effectiveness ($R = 0.794$). The coefficient of determination ($R^2 = 0.630$) indicates that the five forensic accounting technology dimensions jointly explained 63.0% of the variation in Occupational Fraud Detection Effectiveness, while the Adjusted R^2 of 0.610 confirms substantial explanatory power after accounting for the number of predictors. The Standard Error of the Estimate (0.538) indicates good predictive accuracy, and the Durbin-Watson statistic (1.936) confirms the absence of autocorrelation. Overall, the regression model exhibited strong explanatory power and was considered suitable for hypothesis testing.

Table 11

Model Summary

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of Estimate**	**Durbin-Watson**
1	0.794	0.630	0.610	0.538	1.936

Source: Researchers (2026)

Table 12 presents the ANOVA results for the multiple regression model. The model is statistically significant ($F(5,94) = 32.013$, $p < 0.001$), indicating that the combined effects of Artificial Intelligence Analytics, Blockchain-Based Transaction Traceability, Cybersecurity Resilience Framework, Regulatory and Audit Enforcement, and Organisational Technology Readiness significantly explain variation in Occupational Fraud Detection Effectiveness. The regression sum of squares (46.334) is considerably greater than the residual sum of squares (27.210), demonstrating that the model explains a substantial proportion of the variation in the dependent variable. Therefore, the overall regression model is appropriate for testing the study hypotheses.

Table 12

ANOVA Results

Source	**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Regression	46.334	5	9.267	32.013	0.000
Residual	27.210	94	0.289		
Total	73.544	99			

Source: Researchers (2026)

Table 13 presents the regression coefficients for the predictor variables. The findings indicate that all five independent variables have positive and statistically significant effects on Occupational Fraud Detection Effectiveness. Artificial Intelligence Analytics exerts the strongest influence ($\beta = 0.394$, $t = 5.226$, $p < 0.001$), followed by Blockchain-Based Transaction Traceability ($\beta = 0.262$, $t = 3.632$, $p < 0.001$), Cybersecurity Resilience Framework ($\beta = 0.202$, $t = 2.916$, $p = 0.004$), Regulatory and Audit Enforcement Strength ($\beta = 0.173$, $t = 2.632$, $p = 0.010$), and Organisational Technology Readiness ($\beta = 0.139$, $t = 2.001$, $p = 0.048$). As all p-values are below 0.05, each predictor makes a significant positive contribution to improving occupational fraud detection effectiveness. Furthermore, the tolerance and VIF values confirm the absence of multicollinearity, indicating that the regression coefficients are stable and reliable.

Table 13

Multiple Regression Coefficients

Variable	B	Std. Error	β	t-value	Sig.
Constant	-0.710	0.403	—	-1.760	0.082
AI-Driven Forensic Analytics	0.391	0.075	0.394	5.226	0.000
Blockchain-Based Transaction Traceability	0.268	0.074	0.262	3.632	0.000
Cybersecurity Resilience Framework	0.207	0.071	0.202	2.916	0.004
Regulatory and Audit Enforcement Strength	0.171	0.065	0.173	2.632	0.010
Organisational Technology Readiness	0.143	0.071	0.139	2.001	0.048

Dependent Variable: Occupational Fraud Detection Effectiveness (OFDE)
Source: Researchers (2026)

Test of Research Hypotheses

Table 14 summarises the results of the hypothesis tests. The findings indicate that all five null hypotheses (H01–H05) are rejected, as their respective p-values are below the 5% significance level. Specifically, Artificial Intelligence Analytics ($\beta = 0.394$, $t = 5.226$, $p < 0.001$) has the strongest positive effect on Occupational Fraud Detection Effectiveness, followed by Blockchain-Based Transaction Traceability ($\beta = 0.262$, $t = 3.632$, $p < 0.001$), Cybersecurity Resilience Framework ($\beta = 0.202$, $t = 2.916$, $p = 0.004$), Regulatory and Audit Enforcement Strength ($\beta = 0.173$, $t = 2.632$, $p = 0.010$), and Organisational Technology Readiness ($\beta = 0.139$, $t = 2.001$, $p = 0.048$). These results provide empirical evidence that each forensic accounting technology significantly enhances occupational fraud detection effectiveness in the Nigerian maritime industry, with Artificial Intelligence Analytics emerging as the most influential predictor.

Table 14

Summary of Hypothesis Testing

Hypothesis	Predictor Variable	β	t-value	p-value	Decision
H_{01}	AI-Driven Forensic Analytics	0.394	5.226	<0.001	Rejected
H_{02}	Blockchain-Based Transaction Traceability	0.262	3.632	<0.001	Rejected
H_{03}	Cybersecurity Resilience Framework	0.202	2.916	0.004	Rejected
H_{04}	Regulatory and Audit Enforcement Strength	0.173	2.632	0.010	Rejected
H_{05}	Organisational Technology Readiness	0.139	2.001	0.048	Rejected

Source: Researchers' Computation (2026)

Discussion of Findings

The findings indicate that all five dimensions of forensic accounting technologies have positive, statistically significant effects on the effectiveness of occupational fraud detection within Nigerian maritime organisations. AI-Driven Forensic Analytics emerged as the strongest predictor ($\beta = 0.394$, $t = 5.226$, $p < 0.001$), corroborating the findings of Qader and Çek (2024), Ali et al. (2022), and Luka et al. (2025) that artificial intelligence enhances fraud detection, audit quality and financial oversight.

Blockchain-Based Transaction Traceability also showed a significant positive effect ($\beta = 0.262$, $t = 3.632$, $p < 0.001$), supporting the studies of Han et al. (2023) and Qader and Çek (2024), which demonstrated that blockchain improves transparency and audit integrity through immutable transaction records.

Cybersecurity Resilience Frameworks significantly enhanced the effectiveness of fraud detection ($\beta = 0.202$, $t = 2.916$, $p = 0.004$), consistent with the findings of Saeed et al. (2023) and Nelson et al. (2025) that robust cybersecurity strengthens digital risk management and the preservation of forensic evidence. Likewise, Regulatory and Audit Enforcement Strength positively influenced occupational fraud detection ($\beta = 0.173$, $t = 2.632$, $p = 0.010$), confirming the empirical evidence of Bonrath and Eulerich (2024), Razali et al. (2025), and Abdullahi and Mansor (2018) on the importance of governance, compliance and internal audit effectiveness.

Finally, Organisational Technology Readiness exerted a significant positive influence ($\beta = 0.139$, $t = 2.001$, $p = 0.048$), supporting Díaz-Arancibia et al. (2024) and Luka et al. (2025), who identified technological capability and organisational preparedness as critical drivers of digital forensic accounting adoption. Collectively, the findings provide empirical support for the Fraud Diamond Theory and Agency Theory, demonstrating that the integrated adoption of AI, blockchain, cybersecurity resilience, regulatory and audit enforcement, and organisational technology readiness substantially enhances the effectiveness of occupational fraud detection in the Nigerian maritime sector.

CONCLUSION, RECOMMENDATIONS AND SUGGESTIONS FOR FUTURE STUDY

This study concludes that forensic accounting technologies significantly enhance the effectiveness of occupational fraud detection in regulated Nigerian maritime organisations. The findings show that AI-Driven Forensic Analytics, Blockchain-Based Transaction Traceability, Cybersecurity Resilience Frameworks, Regulatory and Audit Enforcement Strength, and Organisational Technology Readiness all have positive and statistically significant effects on occupational fraud detection, with AI-Driven Forensic Analytics emerging as the strongest predictor. The results provide empirical support for the Fraud Diamond Theory and Agency Theory, demonstrating that advanced forensic accounting technologies strengthen monitoring, improve transparency, reduce opportunities for fraud, minimise information asymmetry, and enhance organisational accountability. Consequently, the study concludes that sustainable occupational fraud detection is best achieved through the integrated adoption of artificial intelligence, blockchain technology, cybersecurity resilience, effective regulatory and audit enforcement, and organisational technology readiness, supported by robust corporate governance and regulatory oversight.

Based on the findings, the study recommends that maritime organisations prioritise investment in AI-driven forensic accounting systems, including continuous transaction monitoring, predictive analytics and anomaly detection, while strengthening staff competencies through regular training. Organisations should also adopt blockchain-enabled audit trails, immutable transaction records and smart-contract technologies to improve traceability across procurement, billing and payment processes. To enhance cybersecurity resilience, organisations should strengthen multi-factor authentication, data encryption, continuous security monitoring, incident response capabilities and the preservation of digital forensic evidence.

Furthermore, regulatory and audit enforcement should be reinforced through stronger internal audit independence, effective whistleblowing systems, consistent sanctions, regulatory collaboration and periodic fraud risk assessments. Organisations should also improve technology readiness by investing in digital infrastructure, staff development, data governance and change management. At the policy level, the NIMASA and the Nigerian Shippers' Council (NSC) should establish sector-wide digital fraud control standards, promote the adoption of forensic accounting technologies, strengthen technology-based audit requirements, enhance cybersecurity compliance, support industry-wide capacity building and foster collaboration among regulators, maritime operators and technology providers to improve fraud governance across the Nigerian maritime sector.

This study contributes to knowledge by extending the Fraud Diamond Theory and Agency Theory, demonstrating that advanced forensic accounting technologies strengthen fraud detection, organisational monitoring and accountability. Empirically, it enriches the limited literature on forensic accounting technologies in the Nigerian maritime sector by integrating Artificial Intelligence-Driven Forensic Analytics, Blockchain-Based Transaction Traceability, Cybersecurity Resilience, Regulatory and Audit Enforcement, and Organisational Technology Readiness within a unified analytical framework. Methodologically, the study adopted a census approach and employed validated measurement scales, conducted reliability and construct validity tests, assessed common method bias, performed comprehensive regression diagnostics and carried out SPSS-based statistical analyses. Practically, the findings provide valuable evidence for maritime organisations, regulators and policymakers to strengthen technology-enabled governance, fraud prevention and digital risk management across the Nigerian maritime industry.

Future research should conduct longitudinal studies to assess changes in the effectiveness of occupational fraud detection after the adoption of forensic accounting technologies. Comparative investigations across other maritime subsectors and African maritime jurisdictions are also recommended to assess contextual variations in technology adoption and fraud governance. In addition, future studies should employ mixed methods designs and advanced analytical techniques, including Structural Equation Modelling (AMOS), SmartPLS, and multilevel modelling, to explore more complex causal relationships. Researchers should further examine the mediating or moderating effects of ethical organisational culture, leadership commitment, digital innovation capability, forensic accounting competence, organisational resilience, regulatory quality, and artificial intelligence maturity on the effectiveness of occupational fraud detection.

ACKNOWLEDGEMENT

This research was not funded by any grant.

AUTHOR DECLARATION ON THE USE OF GENERATIVE AI

"During the preparation of this manuscript, generative AI tools (Jenni and Grammarly) were used solely to improve the language and readability of the text. No AI-generated content contributed to the intellectual or analytical aspects of the research, including conceptual development, data interpretation, or the formation of conclusions. The final content was reviewed and approved by the authors, who take full responsibility for the accuracy and integrity of the work."

REFERENCES

Abdullahi, R. B., & Mansor, N. (2018). Fraud prevention initiatives in the Nigerian public sector. *Journal of Financial Crime*, *25*(2), 527–544. https://doi.org/10.1108/jfc-02-2015-0008

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: A comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, *5*(1), 120–140. https://doi.org/10.51594/csitrj.v5i1.709

Adepoju, O. O. (2024). Analysis of constraints against efficiency of seaport-hinterland logistics in Nigeria. *Periodica Polytechnica Transportation Engineering*, *52*(2), 199–208. https:// doi.org/10.3311/pptr.23287

Ali, A., Razak, S. A., Othman, S., Eisa, T., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences, 12*(19), 9637. https://doi.org/10.3390/app12199637

Amaka Anagor-Ewuzie. (2023, August 30). *Job creation: NIMASA puts 11,956 Nigerian seafarers on Cabotage vessels*. *BusinessDay*. https://businessday.ng/maritime/article/job-creation-nimasa-puts-11956-nigerian-seafarers-on-cabotage-vessels/

Aros, L. H., Molano, L. X. B., Gutierrez-Portela, F., Hernandez, J. J. M., & Barrero, M. S. R. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, 11, 1130. https:// doi.org/ 10.1057/s41599-024-03606-0

Bonrath, A., & Eulerich, M. (2024). Internal auditing's role in preventing and detecting fraud: An empirical analysis. *International Journal of Auditing*, *28*(4), 615-631. https://doi.org/10.1111/ijau.12342

Cheng, D., Zou, Y., Xiang, S., & Jiang, C. (2024). Graph neural networks for financial fraud detection: A review. *Frontiers of Computer Science*, *19*, 1-17. https://doi.org/10.1007/s11704-024-40474-y

Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2023). Forensic accounting in the digital age: A U.S. perspective: Scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal*, *5*(11), 342–360. https://doi.org/10.51594/farj.v5i11.614

Díaz-Arancibia, J., Hochstetter-Diez, J., Bustamante-Mora, A., Sepúlveda-Cuevas, S., Albayay, I., & Arango-López, J. (2024). Navigating digital transformation and technology adoption: A literature review from small and medium-sized enterprises in developing countries. *Sustainability*. *16*(14), 5946. https://doi.org/10.3390/su16145946

Firdaus, R., Xue, Y., Gang, L., & Ali, M. S. e. (2022). Artificial intelligence and human psychology in online transaction fraud. *Frontiers in Psychology*, *13*, 947234–947234. https:// doi.org/10.3389/fpsyg.2022.947234

Gao, H., Kou, G., Liang, H., Zhang, H., Chao, X., Li, C., & Dong, Y. (2024). Machine learning in business and finance: A literature review and research opportunities. *Financial Innovation, 10*(86), 1-35. https://doi.org/10.1186/s40854-024-00629-z

Han, H., Shiwakoti, R., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information System*, *48*, 100598. https://doi.org/10.1016/j.accinf.2022.100598

Iwuoha, V. C., Okafor, N. I., & Ifeadike, E. (2022). State regulation of Nigeria's maritime ports: Exploring the impact of port concession on both the regulator and the operators. *Politics & Policy*, *50*(5), 1032–1052. https://doi.org/10.1111/polp.12495

Lokanan, M., & Maddhesia, V. (2024). Supply chain fraud prediction with machine learning and artificial intelligence. *International Journal of Production Research*, *63*, 286–313. https://doi.org/10.1080/00207543.2024.2361434

Luka, J. K., Muse, O., Popoola, J., & Abidin, S. (2025). From forensic knowledge to fraud detection performance: Mediating role of big data analytics skills in the public sector. *International Journal of Applied Mathematics*, *38*(4s),880-902. https://doi.org/10.12732/ijam.v38i4s.277

Nelson, A., Lucky, O., Bukola, A. U., & Afrogha, O. (2025). Forensic accounting practice and fraud management in Nigeria public sector entities. *Journal of Information Systems Engineering and Management*, *10*(48s), 1239-1255. https://doi.org/10.52783/jisem.v10i48s.9754

Nigerian Maritime Administration and Safety Agency. (2025). *List of registered and licensed shipyards*. https://nimasa.gov.ng/nimasa-accredits-27-registered-shipyards-for-operation-in-nigeria/

Odeyemi, O., Ibeh, C. V., Mhlongo, N. Z., Asuzu, O. F., Awonuga, K. F., & Olatoye, F. O. (2024). Forensic accounting and fraud detection: A review of techniques in the digital age. *Finance & Accounting Research Journal*, *6*(2), 202–214. https://doi.org/10.51594/farj.v6i2.788

Qader, K., & Çek, K. (2024). Influence of blockchain and artificial intelligence on audit quality: Evidence from Turkey. *Heliyon*, 10,(9), e3016. https://doi.org/10.1016/j.heliyon.2024.e30166

Razali, F. M., Sulaiman, N., Manan, D. I. A., & Said, J. (2025). Sustainability of audit profession in digital technology era: The role of competencies and digital technology capabilities to detect fraud risk. *SAGE Open*, *15*,(1), 1-12. https://doi.org/10.1177/21582440241304974

Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E., & Alabbad, D. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors (Basel, Switzerland)*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Said, J., Alam, Md. M., Ramli, M., & Rafidi, M. (2017). Integrating ethical values into fraud triangle theory in assessing employee fraud: Evidence from the Malaysian banking industry. *Journal of International Studies*, *10*(2), 170–184. https://doi.org/10.14254/2071-8330.2017/10-2/13

Santos, E. S. D., Santos, M. M. D., Castro, M., & Carvalho, J. T. (2025). Detection of fraud in public procurement using data-driven methods: A systematic mapping study. *EPJ Data Science, 14*(52), 1-46. https://doi.org/10.1140/epjds/s13688-025-00569-3

Tijjani, H., Ibrahim A. S., Ardo, A. M., & Yusuf, A. U. (2023). The impact of forensicaccounting on tax payer attitude and compliance towards tax evasion within SMEs in the North East Nigeria. *Journal of Business Management and Accounting, 13*(1) January, 79-105. https:// doi.org/ 10.32890/jbma2023.13.1.4

Umar, I., Samsudin, R. S., & Mohamed, M. (2016). The influence of institutional and contingency factors on the adoption of forensic accounting by anti-corruption agencies: A proposed framework. *Journal of Business Management and Accounting, 6*(2), 1–10.