IOSR Journal of Multidisciplinary Research (IOSR -JMR)
ISSN: 3048-7439 Volume 3, Issue 3, Series 1, May. - June. (2026), PP 86-91
www.iosrjournals.org

Digital Forensic Accounting Dynamics And Detection Of Procurement Fraud In Kogi State Ministry Of Health, Nigeria

Iyadi Sadat Badanga
Department Of Accounting, Faculty Of Management Science, Federal University Lokoja

Emmanuel Eneche Onoja, PhD
Department Of Accounting, Faculty Of Management Sciences, Federal University Lokoja

Abstract
This study examines the effect of digital forensic accounting dynamics on procurement fraud detection in the Kogi State Ministry of Health, focusing on the Bureau of Public Procurement (BPP). Despite regulatory controls, procurement fraud persists due to increasingly complex digital procurement systems. A quantitative cross-sectional survey design was adopted, using data from staff involved in procurement oversight, audit, compliance, internal control, and ICT functions. Data were analysed using descriptive statistics and multiple regression. Findings show that both dimensions significantly enhance procurement fraud detection. Digital evidence collection improves data integrity and traceability, while forensic software strengthens anomaly detection, pattern recognition, and transaction reconstruction. The model explains 66% of the variation in procurement fraud detection ($R^2 = 0.660$). The study concludes that digital forensic accounting techniques are essential for effective fraud detection in digital procurement environments. It recommends increased investment in forensic technologies and stronger digital evidence management systems in public procurement institutions.

Keywords: *Digital Forensic Accounting, Procurement Fraud, Fraud Detection, Digital Evidence, Forensic Software, Public Sector.*

Date of Submission: 06-05-2026 Date of Acceptance: 16-05-2026

I. Introduction

Public procurement constitutes a significant component of government expenditure worldwide and plays a critical role in the delivery of public goods and services. Due to the scale of financial transactions, procedural complexity, and discretionary decision-making involved, procurement systems are widely recognised as highly vulnerable to corruption and fraud. Across both developed and developing economies, procurement-related irregularities such as bid rigging, contract inflation, collusion, and payment manipulation continue to undermine value for money, distort market competition, and erode public trust in governance (Organisation for Economic Co-operation and Development [OECD], 2024; World Bank, 2024). Although regulatory frameworks and oversight mechanisms have been strengthened in many jurisdictions, the effectiveness of fraud detection within procurement systems remains a persistent global concern.

The challenge is particularly acute in developing countries, where institutional capacity constraints, weak audit systems, and limited technological integration reduce the ability of public sector organisations to effectively identify and substantiate fraudulent activities. In such contexts, fraud detection is often hindered by fragmented audit trails, inadequate monitoring systems, and reliance on traditional investigative approaches that are ill-equipped to handle the complexity of modern, digitally mediated transactions (Kranacher et al., 2020; Singleton & Singleton, 2010). As public financial management systems increasingly transition to electronic and automated platforms, the nature of procurement fraud has evolved, becoming more sophisticated and difficult to detect using conventional methods.

In Nigeria, procurement fraud continues to pose a significant threat to accountability, transparency, and efficient resource utilisation within the public sector. Despite the existence of regulatory institutions such as the Bureau of Public Procurement and the presence of anti-corruption agencies tasked with oversight and enforcement, reported cases of procurement fraud persist. This persistence suggests that the problem extends beyond the existence of formal rules and regulations to the practical effectiveness of detection mechanisms (Bureau of Public Procurement [BPP], 2026; Independent Corrupt Practices Commission [ICPC], 2024). In particular, the growing digitisation of procurement processes has introduced new challenges, as fraudulent activities are increasingly embedded within complex electronic systems that require advanced analytical and investigative capabilities to uncover.

In response to these emerging challenges, digital forensic accounting techniques have gained prominence as a modern approach to strengthening fraud detection in public sector environments. These techniques involve the application of technology-driven procedures to identify, extract, analyse, and interpret financial and transactional data from digital systems.

Despite the growing relevance of digital forensic accounting, existing empirical studies reveal several limitations. A significant proportion of prior research has focused on general fraud detection, banking sector fraud, or private sector applications, with limited attention to procurement fraud within the public sector, particularly in developing countries such as Nigeria. Furthermore, digital forensic accounting has often been treated as a broad and undifferentiated construct, with insufficient emphasis on its specific functional components, such as digital evidence collection and forensic investigation software (Awwad, 2025; Bello et al., 2026). Methodologically, many studies rely heavily on perception-based survey data, with limited application of forensic or transactional evidence, thereby constraining the robustness and practical relevance of their findings (Eze et al., 2023; Lawal & Adeyemi, 2024).

Consequently, a clear gap exists in the literature regarding the role of discrete digital forensic accounting techniques in enhancing procurement fraud detection within Kogi State, Ministry of Health. This gap spans theoretical, methodological, and contextual dimensions, highlighting the need for a more focused and component-based investigation. Addressing this gap is essential not only for advancing academic understanding but also for improving practical fraud detection mechanisms in public procurement systems.

It is in view of the above gaps that this study examines the influence of digital forensic accounting techniques on the detection of procurement fraud in Kogi State, Ministry of Health. Specifically, the study focuses on digital evidence collection and preservation, and digital forensic investigation software as key dimensions of digital forensic accounting techniques. By adopting a structured and disaggregated approach, the study seeks to provide empirical evidence on how these techniques enhance fraud detection effectiveness, thereby contributing to improved transparency, accountability, and governance in Kogi state, ministry of health.

In order to address the problem of ineffective procurement fraud detection in Kogi state, ministry of health, this study seeks to answer the following research questions:

i. To what extent does digital evidence collection influence the detection of procurement fraud in Kogi State, Ministry of Health?
ii. How does digital forensic investigation software influence the detection of procurement fraud in Kogi State, Ministry of Health?

In line with the research questions, the specific objectives of this study are to:

i. Examine the influence of digital evidence collection on the detection of procurement fraud in Kogi State, Ministry of Health.
ii. Assess the influence of digital forensic investigation software on the detection of procurement fraud in Kogi State, Ministry of Health.

To empirically test the relationships between digital forensic accounting techniques and the detection of procurement fraud, the following null hypotheses are formulated:

H_{01}: Digital evidence collection has no significant influence on the detection of procurement fraud in Kogi State, Ministry of Health.

H_{02}: Digital forensic investigation software has no significant influence on the detection of procurement fraud in Kogi State, Ministry of Health.

This study will be significant theoretically by extending existing fraud theories to explain how digital forensic accounting techniques enhance procurement fraud detection, empirically by providing evidence on the effects of digital evidence collection and forensic investigation software on detection outcomes, and methodologically by demonstrating a more structured, proxy-based approach to studying digital forensic accounting. It will also be useful for policy formulation by informing the integration of digital forensic tools into procurement regulations, and for institutions such as the Bureau of Public Procurement and the Independent Corrupt Practices Commission in strengthening investigative capacity. Ultimately, the study will have societal relevance by promoting transparency, accountability, and improved management of public resources in Kogi state, ministry of health.

II. Literature Review

Conceptual Review

Digital Forensic Accounting Techniques

Aremu (2023) defines them as computer-assisted forensic procedures used to extract and analyse financial evidence from digital environments, while Sanusi et al. (2026) describe them as technology-driven methods for collecting, processing, and interpreting digital financial data to uncover fraud. These definitions emphasise data extraction, analysis, and evidential interpretation within digitised systems. With the increasing adoption of e-procurement and electronic financial systems, these techniques enhance audit trails, improve

traceability, and enable the detection of concealed fraud patterns that traditional methods may overlook. However, prior studies often treat the concept broadly without isolating its functional components. This study conceptualizes digital forensic accounting techniques as technology-enabled investigative procedures used to identify, extract, analyse, and interpret digital procurement data for fraud detection**,** operationalised through digital evidence collection and preservation, and digital forensic investigation software.

Digital Evidence Collection and Preservation

Awwad (2025) defines digital evidence collection as the process of identifying and securing relevant electronic data while maintaining authenticity, whereas Yusuf et al. (2025) describe preservation as ensuring data integrity through chain-of-custody procedures and secure storage. These perspectives highlight the importance of authenticity, integrity, and continuity of evidence. In procurement systems, fraudulent activities leave digital footprints in transaction logs, emails, invoices, and metadata, making effective evidence handling essential for detection and prosecution. Empirical studies indicate that strong digital evidence systems improve investigative reliability and outcomes (Awwad, 2025). Within this study, digital evidence collection and preservation are conceptualised as the legally compliant processes of acquiring, authenticating, and safeguarding electronic procurement records to ensure reliable fraud detection**,** thereby enhancing evidential quality and traceability.

Digital Forensic Investigation Software

Sanusi et al. (2026) define it as advanced analytical tools for detecting anomalies and reconstructing financial events, while Bello et al. (2026) describe it as software that enables pattern recognition, data recovery, and relationship analysis within complex transactions. These tools facilitate automated analysis, anomaly detection, and linkage analysis, making them essential in modern procurement environments characterised by high data volume and complexity. They help identify irregular bidding patterns, inflated invoices, unauthorised payments, and collusive behaviour among actors. Empirical evidence suggests that forensic software enhances the speed, accuracy, and effectiveness of fraud investigations (Sanusi et al., 2026). For the purpose of this study, digital forensic investigation software is conceptualised as specialised analytical tools used to examine digital procurement data for anomaly detection, pattern recognition, and fraud case reconstruction**,** thereby improving detection effectiveness.

Procurement Fraud

Aremu (2023) defines it as the deliberate distortion of procurement procedures through activities such as bid rigging and contract inflation, while Okoye and Gbegi (2024) describe it as unlawful interference in the procurement cycle aimed at influencing outcomes or diverting resources. These definitions emphasise intentionality, deception, and financial gain. Procurement fraud undermines public financial management by increasing costs, reducing service quality, and eroding public trust, particularly in developing countries where institutional controls may be weak. Procurement fraud represents not only financial misconduct but also a systemic governance failure that undermines efficiency, distorts market mechanisms, and weakens institutional credibility. In this study, procurement fraud is conceptualised as the deliberate manipulation of public procurement processes through practices such as collusion, bid rigging, contract inflation, and payment irregularities for undue advantage**.**

Procurement Fraud Detection

Procurement fraud detection refers to the processes used to identify, uncover, and substantiate fraudulent activities within procurement systems. Ibrahim and Musa (2025) define it as the application of investigative techniques to detect hidden anomalies in procurement transactions, while Bello et al. (2026) describe it as the timely identification and substantiation of procurement misconduct through analysis of financial and transactional data. These definitions highlight timeliness, analytical procedures, and evidential substantiation. Traditional detection approaches have proven inadequate in addressing increasingly complex digital fraud schemes, thereby necessitating the use of technology-driven methods. In this study, procurement fraud detection is conceptualised as the technology-driven identification and substantiation of fraudulent activities in public procurement through the analysis of digital records and forensic evidence**,** serving as the dependent variable influenced by digital forensic accounting techniques.

Conceptual Linkage

Digital forensic accounting techniques, through digital evidence collection and preservation, and forensic investigation software, enhance procurement fraud detection by strengthening data integrity, improving audit trail traceability, and enabling advanced analytical procedures, thereby increasing the accuracy, timeliness, and reliability of fraud detection in Nigerian public sector procurement systems.

Theoretical Review

This study builds its theoretical foundation by combining and extending the ideas of Donald Cressey's Fraud Triangle Theory and the Routine Activity Theory developed by Lawrence Cohen and Marcus Felson, but adapts them to reflect the realities of today's digital procurement systems. While the Fraud Triangle explains that fraud occurs due to pressure, opportunity, and rationalisation, this study goes further by arguing that "opportunity" in modern public procurement is no longer just about weak internal controls—it is increasingly shaped by poor digital visibility, fragmented data systems, and limited forensic capacity within electronic platforms. In the same vein, Routine Activity Theory's idea of "capable guardianship" is reinterpreted in practical, technology-driven terms. Here, digital forensic accounting techniques act as the "guardians": digital evidence collection and preservation help reduce opportunities for fraud by ensuring that records are complete, traceable, and difficult to manipulate, while forensic investigation software strengthens oversight by enabling faster detection of unusual patterns, hidden relationships, and suspicious transactions. By bringing these ideas together, the study contributes theoretically by showing that effective fraud detection today depends not just on controlling human behaviour, but on the strength of digital systems that can monitor, analyse, and expose irregularities in real time. In this way, the study shifts the focus from traditional, static explanations of why fraud occurs to a more practical and dynamic understanding of how it can be detected and limited in a technology-driven public sector environment.

Empirical Review

Sanusi et al. (2026) examined the effect of digital forensic accounting techniques on fraud detection in selected Nigerian public institutions using a quantitative survey design and multiple regression analysis. While the study reports a statistically significant relationship between forensic techniques and fraud detection effectiveness, its reliance on perceptual responses from audit personnel raises concerns about common method bias and subjective inflation of effectiveness, as respondents may overstate the impact of tools they are professionally associated with. More critically, the study treats digital forensic accounting as a composite construct, thereby obscuring the differential effects of its underlying components, which limits its explanatory precision and reduces its applicability to procurement-specific fraud contexts.

Bello et al. (2026) investigated the impact of forensic investigation software on fraud detection efficiency using a cross-sectional survey of audit personnel. Although the findings suggest that forensic software enhances detection speed and accuracy, the study adopts a generic fraud framework, failing to account for the unique structural and procedural complexities of procurement systems**,** such as multi-stage approvals and collusive bidding patterns. Furthermore, the cross-sectional design constrains causal inference, making it difficult to determine whether improved detection outcomes are attributable to the software itself or to pre-existing institutional capacity and technological maturity**.**

Awwad (2025) analysed the influence of digital evidence collection and preservation on fraud investigation outcomes using a mixed-method approach. While the study highlights the importance of chain-of-custody procedures and evidential integrity, its primary emphasis on investigative outcomes rather than detection processes limits its relevance to early-stage fraud identification. Additionally, the study does not sufficiently interrogate how digital evidence systems interact with large-scale transactional environments, such as procurement platforms, where data volume and complexity significantly affect detection capability.

Yusuf et al. (2025) explored the role of digital evidence systems in enhancing audit quality and fraud detection using survey and regression techniques. Although the study establishes a positive association between structured evidence systems and detection accuracy, its analytical focus remains at an aggregate system level, without examining how specific evidence-handling mechanisms influence distinct fraud detection outcomes. This aggregation introduces construct validity concerns, as improvements in audit quality may not directly translate to effective detection of procurement-related fraud, which often requires more specialised forensic analysis.

Ibrahim and Musa (2025) examined the effect of digital forensic analytics tools on fraud detection using a descriptive survey design. While the findings indicate that analytics tools improve anomaly detection and pattern recognition, the study is situated within a predominantly private-sector context, where governance structures, incentives, and data environments differ significantly from those of the public sector. This contextual mismatch limits the external validity of the findings, particularly in relation to public procurement systems characterised by bureaucratic complexity and weaker enforcement mechanisms.

Adamu et al. (2024) investigated procurement fraud and internal control weaknesses in Nigerian public institutions using descriptive statistical analysis. The study identifies weak monitoring systems and poor transparency as key drivers of procurement fraud; however, its analytical approach remains diagnostic rather than solution-oriented, offering limited insight into how emerging digital tools can address these weaknesses. Moreover, the absence of inferential analysis restricts the study's ability to establish robust relationships between control deficiencies and fraud occurrence**.**

Collectively, the empirical literature suggests that that digital forensic accounting techniques enhance fraud detection through improved analytical capability, audit trail integrity, and anomaly detection. However, three critical limitations persist. First, there is an over-reliance on perception-based survey data, which constrains empirical objectivity and limits real-world applicability. Second, existing studies are largely generic, with insufficient focus on procurement fraud within Kogi state, ministry of health, where institutional weaknesses significantly shape fraud dynamics. Third, digital forensic accounting is often treated as a monolithic construct, with limited effort to disaggregate it into measurable components such as digital evidence collection and forensic investigation software. These limitations create significant conceptual, methodological, and contextual gaps, thereby justifying the need for a more structured and component-based investigation as undertaken in this study.

Gaps in the Literature

From the critical synthesis, the following gaps are identified:

i. Contextual Gap: Limited focus on procurement fraud detection in Kogi State, Ministry of Health.
ii. Conceptual Gap: Lack of disaggregation of digital forensic accounting into key components.
iii. Methodological Gap: Heavy reliance on perception-based data instead of forensic procurement records.
iv. Practical Gap: Limited integration of forensic tools within real public procurement systems.

III. Methodology

This study adopted a quantitative survey research design, a population of 130 staff of Kogi State, Ministry of Health, with a sample size of 98 using Yamene formula with a simple random sampling technique. This study used questionnaire in 5 Likert scale with the bio-data to gather all necessary information from the participants. The validity of the instrument was ensured through expert review by specialists in accounting, auditing, and forensic investigation, who assessed its content relevance and clarity. Reliability was tested using Cronbach's Alpha coefficient, and a threshold of 0.70 and above was adopted as evidence of acceptable internal consistency. The study uses multiple regression with the aid of SPSS 25 version to test the hypotheses. The model specification is:

$DPF = \beta_0 + \beta_1 DEC + \beta_2 DFE + \varepsilon$

Where: DPF = Detection of procurement fraud, DEC = Digital evidence collection, DFE = Digital forensic investigation software, β_0 = Constant, β_1 - β_2 = Coefficient, ε = Error term

Data collected were analysed using both descriptive and inferential statistical techniques. Descriptive statistics such as frequency distribution, percentages, mean, and standard deviation were used to summarise respondents' profiles and variable responses. Inferential analysis was conducted using multiple regression analysis to test the hypotheses.

IV. Results And Discussion

Hypothesis One (H_{01})

The result of the regression analysis is that the Digital Evidence Collection (DEC) Beta coefficient is 0.325 ($p < 0.05$) and the p-value is 0.000. We therefore reject H_{01}. DEC plays a significant role in fraud. This finding is in agreement with Awwad (2015), who postulated that "chain-of-custody" and "forensic integrity" are essential for investigations. For instance, in relation to the Fraud Triangle Theory, DEC removes the "Opportunity" to commit fraud by preserving the trail of all digital evidence.

Hypothesis Two (H_{02})

Digital Forensic Investigation Software (DFI) has a Beta coefficient of 0.341 and a p-value of 0.000 ($p < 0.05$). We therefore reject H_{02}. DFI is a significant predictor of fraud detection. This result agrees with Sanusi et al. (2026) and Bello et al. (2026) that software enhances detection efficiency and pattern recognition. Software is a "Capable Guardian" according to the Routine Activity theory, which provides the supervision required to detect complex collusion.

V. Conclusion And Recommendations

This study concludes that the Nigerian government needs digital forensic accounting; for instance, the Kogi State Ministry of Health's manual-to-digital approach to monitoring and control improves the ability to detect contract inflation and bid rigging. Young employees and effective software are promising, but the systematic capture of digital evidence is the "weak link".

This study recommends that:

i. The Ministry of Health should use blockchain or encrypted logs for transactions to enhance the "tamper-proof" score so that the administrative staff cannot alter the procurement documents after they have been

entered.

ii. Audit staff should be given priority training in Link Analysis to identify covert links between independent contractors.

iii. The Kogi State government should adopt a "Digital Chain-of-Custody" policy to enable digital evidence to be used in disciplinary and court proceedings.

iv. The Ministry should not do "Investigative Audits" but "Continuous Auditing" with forensic software to identify anomalies on a regular basis.

Contribution to Knowledge

i. Unlike other studies (Sanusi et al., 2026; Okoye & Gbegi, 2024) that have used forensic accounting as a whole, this study disaggregated it into Collection and Software, and found that software has a slight marginal impact.

ii. It has applied the Routine Activity Theory to the digital world, demonstrating that "guardianship" in modern procurement is digital.

iii. It provides the first forensic evidence in the Kogi State Ministry of Health, thus filling a geographical and sectoral gap in Nigeria's forensic accounting literature.

References

[1]. Aremu, O. A. (2023). Digital Forensic Accounting And Fraud Detection In Public Sector Organisations. *Journal Of Forensic Accounting And Fraud Investigation, 8*(2), 45–62.

[2]. Adamu, Y., Bello, M., & Sani, A. (2024). Public Procurement Fraud And Internal Control Weaknesses In Nigerian Institutions. *African Journal Of Public Sector Management, 12*(1), 88–104.

[3]. Awwad, B. A. (2025). Digital Evidence Collection And Preservation In Fraud Investigations: Implications For Forensic Accounting. *International Journal Of Digital Accounting Research, 15*(1), 101–119.

[4]. Bello, S. A., Ibrahim, U., & Lawal, K. A. (2026). Forensic Investigation Software And Fraud Detection Efficiency In Public Organisations. *Journal Of Accounting And Digital Innovation, 10*(3), 77–95.

[5]. Bureau Of Public Procurement. (2026). *Annual Procurement Compliance Report*. Abuja, Nigeria: Author.

[6]. Eze, C. N., Okeke, M. N., & Ugwu, J. I. (2023). Digital Systems And Fraud Detection In Nigeria's Public Sector. *Nigerian Journal Of Accounting Research, 19*(2), 120–138.

[7]. Ibrahim, M. A., & Musa, S. (2025). Digital Forensic Analytics And Fraud Detection In Emerging Economies. *Journal Of Financial Crime And Compliance, 13*(2), 55–73.

[8]. Independent Corrupt Practices Commission. (2024). *Annual Anti-Corruption Report*. Abuja, Nigeria: Author.

[9]. Kranacher, M. J., Riley, R. A., & Wells, J. T. (2020). *Forensic Accounting And Fraud Examination* (2nd Ed.). Wiley.

[10]. Lawal, A. I., & Adeyemi, T. O. (2024). Digital Systems Integration And Procurement Fraud Detection In Developing Economies. *Journal Of Public Financial Management, 14*(1), 33–50.

[11]. Nwankwo, P. O., & Okafor, G. C. (2025). Fraud Detection Mechanisms In Public Procurement Systems: Evidence From Nigeria. *International Journal Of Government Auditing, 9*(2), 66–84.

[12]. Organisation For Economic Co-Operation And Development. (2024). *Public Procurement And Corruption Risk Report*. OECD Publishing.

[13]. Okoye, E. I., & Gbegi, D. O. (2024). Forensic Accounting Practices And Fraud Detection In The Public Sector. *Journal Of Accounting And Governance, 11*(2), 90–108.

[14]. Sanusi, L. S., Ahmed, R., & Bello, A. (2026). Digital Forensic Accounting Techniques And Fraud Detection In Public Institutions. *Journal Of Emerging Accounting Technologies, 7*(1), 21–40.

[15]. Singleton, T. W., & Singleton, A. J. (2010). *Fraud Auditing And Forensic Accounting* (4th Ed.). Wiley.

[16]. World Bank. (2024). *Enhancing Public Procurement Transparency In Developing Economies*. World Bank.

[17]. Yusuf, H. M., Abdullahi, S., & Garba, A. (2025). Digital Evidence Systems And Audit Quality In The Public Sector. *African Journal Of Accounting And Financial Studies, 18*(3), 140–158.