GENERATIVE AI ADOPTION: AN EXPLORATORY INNOVATIVE TOOL FOR CURBING ACCOUNTING FRAUDS IN THE NIGERIAN BANKING SECTOR DATA LAKE ANALYTICS

Emoarehi Eriki PhD
Department of Accounting,
Faculty of Management Science,
University of Benin, Benin City
emoarehi.eriki@uniben.edu/emoarehi11@gmail.com

Samuel Umanah PhD
Department of Accounting
Faculty of Management Science
University of Benin, Benin City.
samuel.umanah@uniben.edu

Corresponding Author: emoarehi.eriki@uniben.edu
DOI: https://doi.org/10.57233/ijamer.v2i3.022

Article History: Received: 19 August 2026 | **Revised:** 6 September 2026 | **Accepted:** 15 September 2026 | **Published:** 25 September 2026

How to Cite This Article :
Eriki, E., & Umanah, S. (2026). Generative AI adoption: An exploratory innovative tool for curbing accounting frauds in the Nigerian banking sector data lake analytics. *International Journal of Accounting, Management and Economic Review, 2*(3). https://doi.org/10.57233/ijamer.v2i3.022

Abstract
Accounting fraud remains a significant concern within the Nigerian banking sector, particularly as banking transactions become increasingly complex, digital and data-intensive. Traditional fraud detection approaches may face limitations in identifying variations of fraudulent behaviour that are not adequately represented in historical transaction records. This conceptual paper explores Generative Artificial Intelligence (Gen AI) as an innovative analytical tool for strengthening accounting fraud detection within Nigerian banking sector data lake environments. The paper adopts a conceptual and exploratory approach based on the synthesis of existing literature on Generative AI, accounting fraud detection, synthetic data generation, anomaly detection and banking data analytics. A conceptual framework is proposed linking banking data lakes, data preparation and governance, Generative AI applications, synthetic fraud data and fraud scenario generation, anomaly detection, human validation and accounting fraud prevention. In the framework, Generative Adversarial Networks (GANs) are proposed for generating synthetic fraud-related transaction patterns, while Large Language Models (LLMs) are proposed for generating and interpreting fraud scenarios. The paper argues conceptually that these capabilities may complement existing fraud detection systems by expanding the range of fraud scenarios available for analysis. However, the study recognizes important concerns relating to data privacy, bias, model reliability, security, regulatory compliance and the potential for inaccurate or unrealistic AI-generated outputs. Accordingly, Generative AI is positioned as a complementary tool requiring human oversight rather than a replacement for professional judgement. The paper concludes by recommending empirical pilot studies, regulatory collaboration, capacity building and appropriate AI governance to determine the practical effectiveness and responsible application of Generative AI in Nigerian banking fraud detection.

Keywords: Generative Artificial Intelligence, Accounting Fraud, Nigerian Banking Sector, Data Lake Analytics, Synthetic Data, Fraud Detection, Anomaly Detection

1.0 Introduction

Accounting fraud poses significant threats to the Nigerian banking sector, with potential consequences for financial losses, institutional reputation, customer confidence, and financial

system stability (Okoye & Gbegi, 2013; Owojori et al., 2011). The increasing volume, speed, and complexity of digital banking transactions have also created new opportunities for fraudulent activities, making effective fraud detection and prevention an important concern for financial institutions. Although Nigerian banks have increasingly adopted digital technologies and data-driven approaches to improve their operations, fraud detection practices continue to face challenges associated with the identification of emerging and increasingly sophisticated fraud patterns. Existing studies have examined the use of data analytics and other conventional techniques in detecting fraud in Nigerian banks, but there remains limited empirical evidence on the application of more advanced artificial intelligence approaches to accounting fraud detection (Owolabi & Ajayi, 2021; Onyia et al., 2021).

Traditional fraud detection approaches, including rule-based systems and conventional statistical or data-analytic techniques, can be useful for identifying previously known patterns of suspicious transactions. However, their effectiveness may be constrained when fraudsters adopt new methods that differ substantially from established patterns. This limitation creates a need to explore more adaptive analytical approaches capable of learning complex relationships, generating alternative fraud scenarios, and supporting the identification of previously unobserved patterns. Recent developments in data lake architectures provide an opportunity to integrate large volumes of structured, semi-structured, and unstructured information for advanced analytics. Nevertheless, the application of these capabilities to accounting fraud detection within the Nigerian banking environment remains insufficiently explored (Onyia et al., 2021).

Generative Artificial Intelligence (Gen AI), particularly techniques such as Generative Adversarial Networks (GANs) and Large Language Models (LLMs), presents a potentially innovative approach to addressing some of these limitations. GANs can generate synthetic data that resemble patterns contained in existing datasets, while LLMs can support the generation and interpretation of textual information and scenario-based narratives (Goodfellow et al., 2014; Brown et al., 2020). Previous research has demonstrated the potential of generative models for addressing data limitations and improving fraud-classification performance in other contexts (Esteban et al., 2017; Fiore et al., 2019). These capabilities suggest that Gen AI could complement existing fraud detection mechanisms by generating synthetic fraud scenarios, supporting anomaly detection, and improving the representation of rare fraud events.

However, the potential application of Gen AI to accounting fraud detection in Nigerian banking data lake environments remains largely unexplored. Existing Nigerian studies have predominantly examined fraud detection through conventional data analytics, forensic accounting, and other established approaches, while limited attention has been given to the use of generative models for proactive fraud scenario generation and anomaly detection (Adebisi & Gbegi, 2015; Owolabi & Ajayi, 2021). Consequently, there is an important research opportunity to examine how Gen AI could be integrated into data lake analytics to strengthen the capacity of Nigerian banks to identify and respond to emerging accounting fraud patterns.

The Nigerian banking sector therefore provides a relevant context for exploring this emerging research area. Rather than assuming that Nigerian banks uniformly depend on outdated fraud detection technologies, this study recognises that banks operate with different levels of technological capability and analytical maturity. The concern is instead whether existing fraud detection arrangements are sufficiently adaptive to address evolving fraud techniques and whether Gen AI can provide additional capabilities beyond conventional approaches. Integrating

Gen AI with banking data lake analytics could potentially facilitate the generation of realistic fraud scenarios, enrichment of limited or imbalanced fraud datasets, and identification of complex anomalies that may not be readily detected through conventional approaches.

Against this background, this paper explores the potential of Generative AI as an innovative tool for curbing accounting fraud within Nigerian banking sector data lake analytics. The study particularly focuses on the potential contribution of GANs and LLMs to synthetic fraud-data generation, scenario simulation, anomaly detection, and human-in-the-loop fraud investigation. By positioning Gen AI as a complementary technology rather than assuming the inadequacy of all existing banking fraud systems, the study seeks to provide a more balanced and empirically defensible foundation for future research and practical implementation in the Nigerian banking sector.

2.0 Conceptual Review

Generative Artificial Intelligence (Gen AI)

Generative Artificial Intelligence (Gen AI) refers to a class of artificial intelligence models capable of generating new content or data by learning patterns and relationships from existing datasets. Important categories include Generative Adversarial Networks (GANs) and Transformer-based Large Language Models (LLMs). GANs consist broadly of a generator and discriminator that operate in an adversarial process to produce synthetic observations that resemble characteristics of the training data (Goodfellow et al., 2014). LLMs, on the other hand, are designed primarily for processing and generating human-like text and can support activities such as information extraction, summarisation, classification, and scenario generation (Brown et al., 2020).

Within accounting fraud detection, the relevance of Gen AI extends beyond its general ability to generate content. Its potential value lies particularly in addressing some of the data-related problems associated with fraud analytics. Fraudulent transactions are often relatively rare compared with legitimate transactions, which can result in highly imbalanced datasets. Historical fraud records may also contain missing observations, inconsistent classifications, or insufficient examples of newly emerging fraud techniques. Generative models may therefore be used to create synthetic observations that resemble selected characteristics of historical fraud cases and potentially improve the representation of minority fraud classes. Fiore et al. (2019), for example, examined the use of GANs to improve credit card fraud classification and demonstrated the potential of synthetic data generation to address classification challenges. However, evidence from credit card fraud environments should not automatically be generalised to accounting fraud in Nigerian banks because transaction structures, fraud typologies, institutional controls, and regulatory environments differ across contexts.

The potential application of Gen AI to banking fraud detection can therefore be understood through three related functions. First, generative models can support synthetic fraud-data generation, particularly where genuine fraudulent observations are limited. Second, they can support fraud scenario simulation, allowing investigators to examine hypothetical combinations of fraudulent activities that may not be sufficiently represented in historical records. Third, generated scenarios can potentially complement anomaly detection systems by exposing analytical models to a wider range of possible fraudulent patterns. These functions are particularly relevant to data lake environments because data lakes can integrate large volumes of structured, semi-structured, and unstructured information from multiple sources (Hai et al., 2016).

However, the potential benefits of Gen AI should not be interpreted as evidence that synthetic data automatically improves fraud detection. The quality of generated data is dependent on the quality and representativeness of the training data. If historical fraud records contain systematic biases, missing information, or inaccurate classifications, a generative model may reproduce or amplify those weaknesses. Similarly, synthetic transactions that appear statistically realistic may not necessarily represent genuine fraud mechanisms. Consequently, a fraud detection model trained partly on synthetic data could achieve apparently strong performance while performing poorly when exposed to actual fraudulent transactions. This creates an important distinction between synthetic-data realism and fraud-detection validity.

Another limitation concerns the detection of novel fraud. Gen AI learns from patterns contained in available data, meaning that it may still struggle to generate or identify fraud mechanisms that are substantially different from the information represented in its training environment. The ability to generate new scenarios should therefore not be equated with the ability to predict previously unknown fraud. In banking environments, where fraudulent behaviour can adapt in response to changes in controls, technology, customer behaviour, and regulatory requirements, continuous model validation is necessary.

The use of Gen AI also introduces risks that are particularly important in accounting and banking. Financial and transaction data may contain confidential customer information and sensitive institutional records. Consequently, the development and training of generative models must incorporate appropriate data governance, access controls, anonymisation, security measures, and regulatory compliance. Ethical concerns also arise where models reproduce biases contained in historical data. Jobin et al. (2019) emphasise the importance of principles such as transparency, fairness, accountability, and privacy in the governance of artificial intelligence. These considerations are particularly important in fraud detection because false-positive classifications can subject legitimate customers or employees to unnecessary investigation, while false negatives may allow fraudulent activities to remain undetected.

LLMs present an additional set of limitations. Although they can assist with analysing textual information, generating fraud scenarios, and summarising investigation reports, their outputs may contain inaccurate or fabricated information. Such outputs cannot therefore be treated as independent evidence of fraudulent behaviour. In an accounting fraud environment, an LLM-generated explanation or scenario should serve as analytical support rather than as a substitute for transaction evidence, professional judgement, audit procedures, or human investigation. This reinforces the importance of a human-in-the-loop approach in which fraud investigators validate model-generated alerts and scenarios before decisions are taken.

Role of Gen AI in Accounting Fraud Detection

The role of Gen AI in accounting fraud detection should therefore be viewed as complementary rather than substitutive. Conventional fraud detection systems remain useful for identifying known patterns through predefined rules, statistical techniques, machine learning models, and established investigative procedures. Gen AI may extend these systems by generating additional scenarios, enriching training datasets, and supporting the interpretation of complex information. Its contribution is consequently not necessarily to replace existing fraud detection mechanisms but to improve their capacity to examine rare, complex, and evolving patterns.

In a Nigerian banking data lake environment, this complementary role could involve integrating transaction records, accounting information, audit trails, customer activity, digital banking

records, and other relevant data sources. A GAN-based component could generate synthetic examples of selected fraud patterns, while other analytical models could assess transactions for anomalous characteristics. LLM-based systems could subsequently assist investigators by summarising relevant evidence or generating structured descriptions of possible fraud scenarios. Importantly, generated outputs would require validation against authentic transaction records and expert assessments before being incorporated into fraud-related decisions.

The potential effectiveness of this approach is also dependent on the underlying data lake architecture. A data lake provides a repository for storing large volumes of structured, semi-structured, and unstructured data in their native formats, thereby supporting advanced analytics (Hai et al., 2016). However, the presence of a data lake alone does not guarantee effective fraud detection. Poor data quality, inadequate metadata, inconsistent data structures, weak access controls, and ineffective data governance can limit the usefulness of analytical models. Therefore, the integration of Gen AI should be accompanied by appropriate data preparation, governance, monitoring, and validation mechanisms.

Evidence from existing research provides some support for the potential of generative approaches, but the evidence base remains limited in relation to accounting fraud in Nigerian banking institutions. Fiore et al. (2019) found that GAN-based synthetic data generation could contribute to credit card fraud classification, while Esteban et al. (2017) demonstrated the broader potential of generative models for producing synthetic datasets. Nevertheless, these studies do not directly establish the effectiveness of Gen AI for accounting fraud detection in Nigerian banks. The differences in fraud typologies, accounting systems, transaction environments, data availability, and institutional and regulatory conditions mean that their findings should be regarded as indicative rather than conclusive.

Accordingly, the conceptual position of this study is that Gen AI represents a potentially useful augmentation technology for accounting fraud detection, rather than an established solution. Its contribution is expected to depend on the quality of available data, the realism and validity of synthetic fraud scenarios, the design of anomaly detection models, the quality of human validation, and the regulatory and ethical safeguards surrounding its deployment. This perspective provides a more balanced basis for investigating whether Gen AI can strengthen accounting fraud detection within Nigerian banking sector data lake analytics.

Critical Assessment of Generative AI for Fraud Detection

The conceptual review therefore identifies both opportunities and limitations. On the opportunity side, Gen AI can potentially address class imbalance, generate additional fraud scenarios, support analytical experimentation, and complement existing anomaly detection systems. On the limitation side, synthetic data may reproduce biases in historical data, generated scenarios may not accurately represent real fraud, models may fail to recognise genuinely novel fraud patterns, and LLM outputs may contain inaccurate or fabricated information. There are also significant concerns relating to privacy, security, explainability, accountability, and regulatory compliance.

These limitations are particularly significant in banking because fraud detection is a high-consequence activity. A model that incorrectly identifies legitimate transactions as fraudulent may impose financial and reputational costs on customers and institutions, while failure to identify genuine fraudulent activity may result in direct financial losses. Consequently, the success of Gen AI in this context should not be evaluated solely by its ability to generate realistic

synthetic data. Evaluation should also consider fraud-detection accuracy, false-positive and false-negative rates, generalisation to unseen fraud patterns, robustness across different datasets, explainability, and the consistency of expert validation.

The conceptual review thus suggests that the most appropriate research position is neither to portray Gen AI as a guaranteed solution to accounting fraud nor to dismiss its potential because of its limitations. Instead, Gen AI should be investigated as an emerging analytical capability whose effectiveness must be empirically established within the specific institutional, technological, and regulatory context of Nigerian banking. This provides the basis for examining its integration with data lake analytics for synthetic fraud-data generation, fraud scenario simulation, anomaly detection, and human-supported fraud investigation.

3.0 Methodology

Research Approach

This paper adopts a conceptual and exploratory research approach to examine the potential application of Generative Artificial Intelligence (Gen AI) in curbing accounting fraud through data lake analytics in the Nigerian banking sector. The study is not an empirical investigation and does not involve the collection, estimation, or statistical analysis of primary or secondary banking data. Consequently, the paper does not formulate statistical hypotheses or report empirical model-performance results.

Instead, the study develops a conceptual framework based on existing literature on Generative AI, fraud detection, synthetic data generation, data lake architecture, accounting analytics, and banking fraud. The purpose is to explain how Gen AI technologies, particularly Generative Adversarial Networks (GANs) and Large Language Models (LLMs), could potentially be integrated into a banking data lake to strengthen existing accounting fraud detection mechanisms.

The conceptual approach is appropriate because the application of Gen AI to accounting fraud detection within Nigerian banking data lake environments remains insufficiently examined. The framework therefore provides a basis for understanding the possible relationships between data lake infrastructure, synthetic fraud-data generation, fraud scenario simulation, anomaly detection, human validation, and accounting fraud prevention.

Basis for the Proposed Framework

The proposed framework is developed through a synthesis of existing literature rather than through empirical testing. The literature reviewed covers four interconnected areas.

First, studies on accounting and banking fraud provide the basis for understanding the nature of fraudulent activities and the limitations associated with conventional fraud detection approaches. Second, literature on data analytics and data lakes provides the technological foundation for integrating large volumes of structured, semi-structured, and unstructured banking information. Third, research on Generative AI and synthetic data generation provides the basis for considering how GANs may generate additional fraud scenarios and synthetic observations. Fourth, literature on AI governance and human oversight provides the basis for incorporating validation, privacy, fairness, security, and accountability mechanisms.

The framework consequently represents a theoretical synthesis of these streams of literature rather than an empirically validated technological architecture.

Proposed Integration of Gen AI with Banking Data Lake Analytics

The proposed framework conceptualises the integration of Gen AI into a banking data lake as a multi-stage process.

Stage 1: Data Integration

The data lake serves as the central environment for integrating relevant banking information. This may include accounting records, transaction records, audit trails, customer activity, digital banking records, and other structured, semi-structured, or unstructured information relevant to fraud analysis. A data lake is particularly appropriate for this purpose because it can accommodate diverse forms of data and support advanced analytical applications (Hai et al., 2016).

Stage 2: Data Preparation and Governance

Before analytical processing, the data would be subjected to appropriate cleaning, standardisation, classification, anonymisation, access control, and data governance procedures. This stage is particularly important in banking because transaction and customer information is sensitive and must be protected from unauthorised access or misuse.

Stage 3: Synthetic Fraud-Data Generation

At this stage, GANs are proposed as a mechanism for generating synthetic observations based on patterns contained in appropriately anonymised historical fraud data. The purpose would be to supplement limited fraud observations and provide additional scenarios for analytical experimentation.

However, the framework does not assume that generated data are automatically valid. Synthetic observations would require statistical and domain-expert assessment before being considered suitable for model development. This distinction is important because synthetic data may reproduce weaknesses or biases contained in the original data.

Stage 4: Fraud Scenario Generation

LLMs are proposed as a complementary mechanism for generating structured descriptions of potential fraud scenarios. Based on established Nigerian banking fraud typologies and relevant transaction characteristics, an LLM could assist in developing hypothetical scenarios involving unusual transaction patterns, insider-related activities, fictitious transactions, manipulation of accounting records, or coordinated fraudulent behaviour.

The generated scenarios would serve as analytical and investigative aids rather than independent evidence of fraud.

Stage 5: Anomaly Detection

The synthetic observations and fraud scenarios generated through the Gen AI components could subsequently be incorporated into existing fraud detection and anomaly detection processes. The purpose would be to expose analytical models and investigators to a wider range of potential fraud patterns, including rare or underrepresented scenarios.

Importantly, the framework proposes Gen AI as a complement to existing fraud detection mechanisms rather than a replacement for conventional controls, audit procedures, or professional judgement.

Stage 6: Human-in-the-Loop Validation

Human expertise constitutes an important component of the proposed framework. Fraud investigators, auditors, accountants, and relevant banking professionals would be expected to review significant anomalies and generated fraud scenarios before any operational decision is taken.

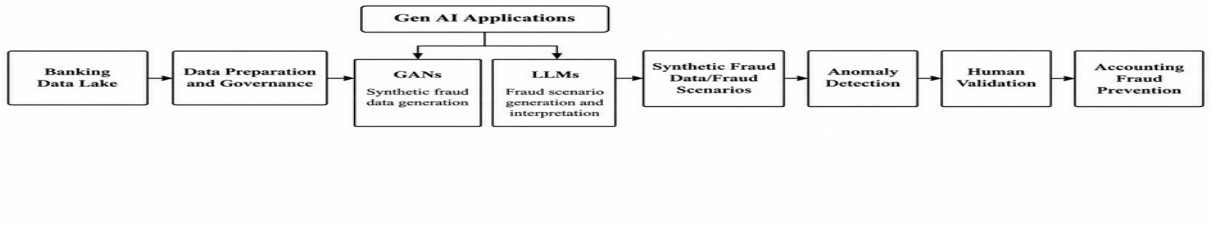
A structured assessment rubric could be used to evaluate the relevance, plausibility, consistency, and investigative usefulness of generated scenarios. Where multiple experts are involved, inter-rater agreement could be assessed using an appropriate measure such as Cohen's kappa (Cohen, 1960).

Conceptual Relationships

The framework proposes that banking data lake analytics provides the underlying data infrastructure, while Gen AI provides additional generative and scenario-based analytical capabilities.

Figure 1

Proposed Conceptual Framework for Generative AI-Enabled Accounting Fraud Detection in Nigerian Banking Sector Data Lake Analytics



Source: Author's Computation, 2026.

Within this relationship, Gen AI is conceptualised through two principal applications:

i. **GAN-based synthetic fraud-data generation**, which addresses the potential problem of limited or imbalanced fraud observations; and
ii. **LLM-based fraud scenario generation and interpretation**, which supports scenario development and human investigation.

The expected outcome is enhanced capacity for identifying and responding to accounting fraud, subject to appropriate validation, governance, and human oversight.

Evaluation of the Proposed Framework

Because this paper is conceptual, the framework is not empirically tested in the present study. Accordingly, no claims are made regarding actual improvements in fraud detection accuracy, precision, recall, or F1-score.

Nevertheless, these metrics are important for the future empirical validation of the framework. A subsequent experimental study could compare a conventional fraud detection model with a Gen AI-augmented model using an independent test dataset. Performance could then be evaluated using accuracy, precision, recall, F1-score, confusion matrices, and ROC-AUC.

Precision would be relevant for determining the proportion of transactions identified as fraudulent that are genuinely fraudulent, while recall would indicate the ability of the model to identify actual fraudulent transactions. The F1-score would provide a combined measure of precision and recall and may be particularly useful where fraud observations are highly imbalanced.These measures are therefore presented in this conceptual paper as proposed future evaluation criteria rather than findings of the current study.

Human and Ethical Considerations

The proposed framework recognises that the use of Gen AI in banking fraud detection introduces significant ethical, privacy, security, and governance considerations. Financial transaction data may contain confidential customer and institutional information, requiring appropriate anonymisation, encryption, access controls, and data governance procedures.

There is also a risk that generative models may reproduce biases contained in historical data. Similarly, generated information may appear plausible without accurately representing actual fraudulent behaviour. LLMs may also produce inaccurate or fabricated explanations. These limitations mean that Gen AI outputs should not be treated as conclusive evidence of fraud.

Human oversight is therefore incorporated into the proposed framework. Investigators and accounting professionals would remain responsible for validating significant alerts and determining whether further investigation is warranted. This approach is consistent with the broader principle that AI should support rather than completely replace professional judgement in high-consequence financial decisions.

Methodological Contribution

The methodological contribution of this paper lies in the development of a conceptual pathway for integrating Gen AI with data lake analytics for accounting fraud detection in Nigerian banks. Unlike an empirical study, the purpose is not to estimate the magnitude of an effect or establish statistical causality. Rather, the framework identifies the technological components, potential applications, evaluation requirements, and governance safeguards that would be necessary for future empirical investigation.

The framework therefore provides a foundation for subsequent pilot studies in which anonymised banking data could be used to determine whether GAN-generated synthetic observations and LLM-assisted fraud scenarios produce measurable improvements in fraud detection performance.

Scope and Limitation of the Methodological Approach

The conceptual nature of the study means that the proposed framework has not been empirically validated using Nigerian banking transaction data. Therefore, the paper cannot conclude that Gen AI will necessarily improve fraud detection performance in Nigerian banks. Its claims are limited to the identification of potential applications and a structured framework for future investigation.

The effectiveness of the proposed approach would ultimately depend on the quality and representativeness of available banking data, the ability of generative models to produce valid fraud scenarios, the quality of human validation, computational resources, institutional readiness, and regulatory requirements.

Future empirical research should therefore test the proposed framework using appropriately anonymised banking datasets and established fraud-detection performance measures.

4.0 Discussion of Conceptual Insights and Implications

As a conceptual study, this paper does not report empirical results or claim that Generative AI has been experimentally validated for accounting fraud detection in Nigerian banks. Instead, the discussion focuses on the conceptual insights derived from the proposed framework and their implications for the application of Generative AI within banking data lake analytics. The framework suggests that Generative AI can potentially complement existing fraud detection approaches by expanding the range of fraud scenarios available for analysis and supporting the development of more dynamic fraud detection capabilities.

Conceptual Insights

A major conceptual insight of the proposed framework is the potential for Generative AI to support the development of dynamic fraud libraries. Conventional fraud detection approaches may depend substantially on previously observed fraud patterns and historical transaction records. The proposed framework extends this approach by introducing the generation of synthetic fraud data and fraud scenarios that can represent variations of known fraudulent activities. In this context, Generative Adversarial Networks (GANs) are proposed as a mechanism for generating synthetic transaction patterns, while Large Language Models (LLMs) can support the generation and interpretation of textual fraud scenarios.

The integration of these capabilities within a banking data lake provides a conceptual pathway through which diverse banking information can be prepared, analysed and used to support fraud detection. Rather than replacing existing fraud detection systems, Generative AI is conceptualised as a complementary analytical capability that can provide additional scenarios and patterns for anomaly detection.

A second conceptual insight concerns the potential use of synthetic fraud data in fraud detection model development. Where genuine fraudulent transactions are limited because of their rarity, confidentiality or security implications, carefully generated synthetic observations may provide additional training scenarios. However, the usefulness of such data depends on whether the generated observations adequately reflect meaningful characteristics of real-world fraudulent activities. Consequently, synthetic data should not automatically be regarded as equivalent to actual fraud observations. Domain experts and fraud investigators would be required to assess its relevance and plausibility before it is incorporated into operational fraud detection processes.

A third insight is the importance of human validation. Although Generative AI can generate synthetic data, scenarios and analytical outputs, its outputs may contain inaccuracies, biases or unrealistic representations of fraud. The proposed framework therefore places human validation after anomaly detection. Fraud investigators, auditors and compliance professionals would review relevant outputs before decisions are made. This human-in-the-loop approach recognises that Generative AI should support professional judgement rather than independently determine whether a banking transaction constitutes fraud.

Implications for Accounting Fraud Detection in Nigerian Banking

The proposed framework has implications for accounting fraud detection in the Nigerian banking sector. Its principal implication is that banking institutions could potentially move towards a more scenario-oriented approach to fraud analytics, where the analysis is not restricted to previously documented fraud patterns. The generation of alternative fraud scenarios may provide opportunities for banks to examine how emerging or modified fraudulent behaviours could appear within transaction data.

The framework also suggests that banking data lakes can provide an appropriate conceptual environment for integrating heterogeneous banking information with advanced analytical tools. When combined with appropriate data preparation, governance and security mechanisms, such an environment could support the application of Generative AI to fraud-related analytics.

However, these implications should be interpreted cautiously. The present study does not demonstrate that Generative AI improves fraud detection accuracy, reduces fraud losses or outperforms existing banking fraud detection systems in Nigeria. Such claims require empirical investigation using appropriate banking data and established fraud detection evaluation measures. Therefore, the contribution of this paper is the development of a conceptual pathway that can subsequently be subjected to empirical validation.

Challenges and Ethical Considerations

Despite its potential, the proposed integration of Generative AI into banking fraud analytics presents important challenges. Data privacy and regulatory compliance represent major concerns because banking transaction information may contain confidential and sensitive information. Even when synthetic data are used, appropriate safeguards are required to prevent the reconstruction, disclosure or misuse of information associated with real customers and transactions.

Another concern is bias. Generative models may reproduce or amplify biases present in their training data. If such biases are incorporated into fraud detection systems, some transaction patterns, customer groups or banking activities could be disproportionately classified as suspicious. Consequently, fairness assessment and appropriate bias-mitigation mechanisms should form part of any future implementation.

The reliability of generated information is also an important consideration. GAN-generated synthetic transactions may appear statistically realistic without necessarily representing genuine fraudulent behaviour. Similarly, LLMs may produce plausible but inaccurate fraud scenarios or interpretations. These limitations make human oversight essential and reinforce the need for systematic validation before generated outputs are used in fraud detection decisions.

Security and governance are further challenges. Synthetic fraud datasets should be appropriately labelled, encrypted and restricted to authorised users and controlled environments. Model outputs should also be subject to regular auditing, while access controls and governance procedures should be established to reduce the possibility of misuse. Collaboration between banking institutions and relevant financial regulators, including the Central Bank of Nigeria, would be important in developing appropriate governance arrangements for the responsible application of Generative AI in banking fraud analytics.

Implications for Future Empirical Research

Since this paper is conceptual, the proposed framework requires empirical validation before its effectiveness can be established. Future studies could examine whether the incorporation of synthetic fraud data and generated fraud scenarios improves the ability of banking fraud detection systems to identify fraudulent transactions.

Such empirical investigations could compare conventional fraud detection models with models enhanced using Generative AI. Established evaluation measures, including accuracy, precision, recall, F1-score, confusion matrices and receiver operating characteristic area under the curve

(ROC-AUC), could be used to assess model performance. These measures are therefore proposed as future evaluation criteria and should not be interpreted as findings of the present conceptual study.

Future research could also investigate the quality and realism of GAN-generated fraud data, the reliability of LLM-generated fraud scenarios, the extent to which human investigators agree with AI-generated classifications, and the ethical and regulatory implications of deploying such systems within Nigerian banks.

5.0 Conclusion

This conceptual paper examined Generative AI as an emerging analytical approach for addressing accounting fraud within Nigerian banking sector data lake environments. Rather than presenting empirical findings, the study developed a conceptual framework linking banking data lakes, data preparation and governance, Generative AI applications, synthetic fraud data and fraud scenarios, anomaly detection, human validation and accounting fraud prevention.

The framework suggests that GANs could support the generation of synthetic fraud data, while LLMs could assist in developing and interpreting fraud scenarios. These capabilities may potentially complement existing fraud detection mechanisms by expanding the range of fraud patterns and scenarios considered during fraud analytics. However, the framework does not establish that Generative AI improves fraud detection performance because no empirical testing was conducted.

The responsible application of Generative AI would also require attention to data privacy, bias, security, output reliability, regulatory compliance and human oversight. Consequently, Generative AI should be viewed as a complementary tool rather than a replacement for fraud investigators, auditors, compliance officers or existing fraud detection systems.

A phased approach is therefore recommended for future implementation. Pilot studies could first be undertaken in collaboration with selected Nigerian banks and relevant regulators within controlled environments such as regulatory sandboxes. Such studies would provide an opportunity to assess the technical feasibility, fraud detection performance, ethical implications and organisational readiness associated with Generative AI.

Recommendations

Based on the conceptual insights developed in this paper, the following recommendations are made:

i. **Empirical validation:** Nigerian banks and researchers should undertake pilot studies to empirically evaluate the effectiveness of Generative AI in accounting fraud detection using appropriate and anonymised banking data.
ii. **Regulatory collaboration:** Banking institutions should collaborate with the Central Bank of Nigeria and other relevant financial regulators in developing appropriate governance frameworks for the responsible use of Generative AI in fraud detection.
iii. **AI-enabled fraud guidelines:** Existing banking fraud management guidelines should progressively incorporate considerations relating to AI oversight, synthetic fraud data, scenario-based fraud simulation, model accountability and human supervision.
iv. **Data protection and security:** Banks should establish strong data governance, encryption, access control and sandboxing mechanisms to ensure that synthetic and real banking information is not misused.

v. **Human oversight:** Generative AI outputs should be reviewed by appropriately trained auditors, fraud investigators, compliance officers and other relevant professionals before being used to support significant fraud-related decisions.
vi. **Capacity building:** Banks should provide continuous training and retraining for managers, supervisors, auditors, compliance personnel and operational staff to improve their understanding of Generative AI, its applications and its limitations.
vii. **Further research:** Future researchers should investigate the performance, reliability, fairness and regulatory implications of integrating GANs, LLMs and other Generative AI technologies into Nigerian banking data lake analytics.

References

Adebisi, J. F., & Gbegi, D. O. (2015a). Fraud and forensic accounting services in Nigerian banks. *Journal of Accounting and Management, 5*(1), 1-14.

Adebisi, J. F., & Gbegi, D. O. (2015b). Fraud management in Nigerian banking sector. *European Journal of Business and Management, 7*(1), 61-67.

Adeyemi, S. B., & Fagbemi, T. O. (2011). The perception of ethics in the Nigerian accounting profession. *Journal of Accounting and Taxation, 3*(7), 146-152. https://doi.org/10.5897/JAT11.008

Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile* (NIST AI 600-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., ... Amodei, D. (2020). Language models are few-shot learners. *Advances in Neural Information Processing Systems, 33*, 1877-1901. https://proceedings.neurips.cc/paper/2020/hash/1457c0d6bfcb4967418bfb8ac142f64a-Paper.pdf

Caltech Science Exchange. (n.d.). *What is generative AI?* California Institute of Technology. https://scienceexchange.caltech.edu/topics/artificial-intelligence-research/generative-ai

Central Bank of Nigeria. (2020a). *Framework for regulatory sandbox operations*. https://www.cbn.gov.ng/Out/2020/CCD/CBN%20Regulatory%20Sandbox%20Framework.pdf

Central Bank of Nigeria. (2020b). *Revised fraud management framework for banks and other financial institutions*. https://www.cbn.gov.ng

Chen, M., Kang, J., & Fu, Y. (2022). Generative adversarial networks for anomaly detection in cyber-physical systems. *IEEE Access, 10*, 41310-41320. https://doi.org/10.1109/ACCESS.2022.3166583

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and Psychological Measurement, 20*(1), 37-46. https://doi.org/10.1177/001316446002000104

Deloitte. (2023, December 18). *Generative AI in accounting: Opportunities and risks to assess today*. https://www2.deloitte.com/us/en/blog/accounting-finance-blog/2023/generative-ai-auditing.html

Deloitte. (2024, April 8). *Generative AI in financial reporting and accounting*. https://www2.deloitte.com/us/en/blog/accounting-finance-blog/2024/generative-ai-in-financial-reporting.html

Esteban, C., Hyland, S. L., & Rätsch, G. (2017). Real-valued (medical) time series generation with recurrent conditional GANs. *arXiv*. https://doi.org/10.48550/arXiv.1706.02633

Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences, 479*, 448-455. https://doi.org/10.1016/j.ins.2018.02.060

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems, 27*, 2672–2680. https://papers.nips.cc/paper_files/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf

Hai, R., Geisler, S., & Quix, C. (2016). Constance: An intelligent data lake system. In *Proceedings of the 2016 International Conference on Management of Data* (pp. 2097–2100). Association for Computing Machinery. https://doi.org/10.1145/2882903.2899389

Institute of Chartered Accountants in England and Wales. (2023, September 26). *ICAEW guide: Generative AI's role in accounting*. https://www.icaew.com/insights/viewpoints-on-the-news/2023/sep-2023/icaew-guide-generative-ais-role-in-accounting/

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence, 1*(9), 389-399. https://doi.org/10.1038/s42256-019-0088-2

McMahon, A., Buyx, A., & Prainsack, B. (2021). Big data governance needs more collective responsibility: The role of harm mitigation in the governance of data use in medicine and beyond. *Medical Law Review, 29*(1), 159-180. https://doi.org/10.1093/medlaw/fwaa028

McMahon, R., Whittingham, L., Tapsell, P., & Moore, R. (2021). AI and Indigenous data: The need for a balanced approach. *AI & Society, 36*, 1115-1125. https://doi.org/10.1007/s00146-021-01161-7

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Nigeria Data Protection Commission. (2023). *Nigeria Data Protection Act, 2023*. https://www.ndpc.gov.ng/resources/

Nigeria Data Protection Commission. (2025). *General Application and Implementation Directive (GAID) 2025*. https://ndpc.gov.ng

Okoye, E. I., & Gbegi, D. O. (2013a). An evaluation of forensic accountants to planning management fraud risk detection procedures. *Global Journal of Management and Business Research, 13*(1), 1-15.

Okoye, E. I., & Gbegi, D. O. (2013b). An evaluation of the effect of fraud and related financial crimes on the Nigerian economy. *Kuwait Chapter of Arabian Journal of Business and Management Review, 2*(7), 110-129.

Onyia, C. O., Okezie, M. A., &Agbatogun, K. (2021). Big data analytics in Nigerian banks: Challenges and opportunities. *International Journal of Financial Research, 12*(1), 63-73. https://doi.org/10.5430/ijfr.v12n1p63

Onyia, U., Ezenwoke, A. A., & Odukoya, J. (2021). A review of data lake architecture for intelligent data analytics. *Nigerian Journal of Technology, 40*(4), 670–680. https://doi.org/10.4314/njt.v40i4.11

Owolabi, S. A., & Ajayi, B. O. (2021). Fraud detection using data analytics in Nigerian banks. *Journal of Accounting and Management, 11*(3), 53–65.

Owolabi, S. A., & Ajayi, F. A. (2021). Effectiveness of forensic accounting in detecting fraud in Nigerian banks. *International Journal of Accounting Research, 8*(1), 21-30.

Owojori, A. A., Akintoye, I. R., & Adidu, F. A. (2011a). The challenge of accounting fraud in the Nigerian banking sector. *Research Journal of Finance and Accounting, 2*(4), 1-10.

Owojori, A. A., Akintoye, I. R., & Adidu, F. A. (2011b). The challenge of risk management in Nigerian banks in the post-consolidation era. *Journal of Accounting and Taxation, 3*(2), 23-31.

Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

The Verge. (2024, August 25). *AI is confusing: Here's your cheat sheet*. https://www.theverge.com/24201441/ai-terminology-explained-humans

Xero. (2024, January). *Future focus: Xero's AI guide for accountants and bookkeepers*. https://accounting.h5mag.com/iab_supplement_jan24/how_generative_ai_will_alter_the_role_of_the_accountant

Zhang, B. H., Lemoine, B., & Mitchell, M. (2018). Mitigating unwanted biases with adversarial learning. In *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 335-340). Association for Computing Machinery. https://doi.org/10.1145/3278721.3278779