International Journal of Entrepreneurial Research and Management
Volume 13 Issue 1, January-March
ISSN: 2995-4878
Impact Factor: 7.95
https://kloverjournals.org/index.php/em

TRANSFORMING FRAUD DETECTION THROUGH GENERATIVE ARTIFICIAL INTELLIGENCE

Nathaniel Chinedu Okafor
Department of Computer Science, University of Lagos, Lagos, Nigeria
DOI:https://doi.org/10.5281/zenodo.15480410

Abstract: As financial fraud schemes grow increasingly sophisticated, traditional detection models struggle to keep pace with the evolving threat landscape. Generative Artificial Intelligence (AI), particularly models like Generative Adversarial Networks (GANs) and Large Language Models (LLMs), are emerging as transformative tools in the realm of fraud detection. These models enable the creation of synthetic datasets, simulate fraudulent behaviors, and enhance the accuracy of anomaly detection systems. By generating realistic fraud scenarios, generative AI enhances predictive modeling and supports proactive risk mitigation strategies in financial institutions. However, the use of generative AI also raises critical concerns around data privacy, explainability, and potential misuse. This paper explores the current and future applications of generative AI in fraud detection, outlines the regulatory and ethical considerations, and offers forward-looking recommendations for integrating these tools into secure, transparent, and efficient fraud risk management frameworks.

Keywords: Generative AI, Fraud Detection, Synthetic Data, Anomaly Detection, Financial Crime Prevention, Large Language Models (LLMs), Generative Adversarial Networks (GANs), Natural Language Processing (NLP), Predictive Analytics, Risk Mitigation

INTRODUCTION

Financial fraud continues to be a significant threat to global economies, costing organizations billions of dollars annually and undermining public confidence in financial systems (Albrecht et al., 2018; Wells, 2019; Okafor, Naibe, Diala, & Akhuemonkhan, 2025). Traditional rulebased fraud detection systems, although widely adopted, often struggle to identify novel and adaptive fraudulent activities. As fraud schemes evolve in complexity and subtlety, there is an urgent need for advanced technologies that can predict, detect, and even simulate fraudulent behavior in real-time. Generative Artificial Intelligence (AI), particularly Generative Adversarial Networks (GANs) and Large Language Models (LLMs), has emerged as a transformative innovation in this domain. Unlike conventional machine learning models that rely on labeled data for classification, generative AI models learn to generate new data that mimics real-world patterns, enabling them to simulate realistic fraud scenarios and uncover hidden anomalies in large datasets (Bologna, Lindquist, & Warren, 2019; Singleton et al., 2014). Generative AI enhances fraud detection systems by augmenting scarce fraudulent data, creating synthetic yet realistic training datasets, and improving the performance of supervised learning models through adversarial training. In particular, GANs have shown promise in detecting anomalies in

financial transactions by modeling what ―normal‖ behavior looks like and flagging deviations from it (Ćirović & Marinković, 2021). Furthermore, the integration of generative AI into predictive analytics enables a more nuanced approach to risk profiling, allowing organizations to identify subtle fraud indicators that would be overlooked by static models (Akinbowale, Klingelhöfer, & Zerihun, 2023). Despite its benefits, the application of generative AI in fraud detection also raises important ethical and regulatory concerns. The ability to generate convincing fake data or deepfakes could be weaponized by bad actors, and the black-box nature of some AI systems may limit transparency and accountability (Njoku et al., 2025). Therefore, a comprehensive governance framework is necessary to ensure that generative AI tools are used responsibly, ethically, and in line with regulatory expectations. This paper critically examines the evolving role of generative AI in financial fraud detection, exploring both its opportunities and challenges. It highlights recent advancements, practical use cases in fraud detection frameworks, and discusses the ethical, technical, and regulatory implications of deploying generative AI models in high-stakes financial environments.

Applications of Generative AI in Fraud Detection

Generative AI has introduced a paradigm shift in the approach to financial fraud detection by enabling systems to learn from data, simulate real-world fraud scenarios, and detect previously unidentifiable anomalies. Among the most impactful models are Generative Adversarial Networks (GANs), Variation Auto encoders (VAEs), and transformer-based architectures such as Large Language Models (LLMs), all of which are now being adapted to augment traditional and machine learning-driven fraud detection systems (Bologna, Rindova, & Suddaby, 2019; Njoku, Okafor, Akhuemonkhan, Naibe, & Diala, 2025). One of the most powerful applications of generative AI in fraud prevention is the generation of synthetic yet realistic transactional data. Fraudulent transactions are relatively rare in realworld datasets, making it difficult to train robust machine learning models. GANs can be employed to create diverse and realistic samples of fraudulent activity, thereby addressing the class imbalance problem common in fraud datasets (Aburumman et al., 2022). This synthetic data improves the learning process of supervised algorithms and enhances model generalization in real-world applications. Generative AI is also instrumental in modeling normal behavioral patterns in financial systems. By training models on large sets of legitimate transaction data, systems can learn to flag deviations as potential fraud with high precision (Ćirović & Marinković, 2021). VAEs and GANs are particularly effective in detecting subtle irregularities and uncovering hidden fraud rings, as they are able to capture complex, non-linear dependencies between features that rule-based systems miss (Akinbowale et al., 2023). Generative models are being used by fraud analysts and financial institutions to simulate "what-if" fraud scenarios. This allows for proactive stress testing of existing detection systems under a variety of threat models. For example, adversarial AI can create synthetic fraudulent behavior that challenges existing fraud models, leading to the development of more robust and adaptive systems (Golden, 2019). Large Language Models (LLMs) such as ChatGPT and BERT are increasingly being deployed in the detection of fraud involving textual data—such as financial reports, emails, invoices, and audit trails. These models can uncover suspicious language patterns and flag inconsistencies or unusual disclosures in regulatory filings (Pickett & Pickett, 2019). Combined with structured financial data, NLP-based

generative AI enhances the scope of fraud detection across both quantitative and qualitative dimensions. Unlike static rule-based systems, generative AI allows fraud detection systems to continuously learn and adapt to new patterns of fraud. These adaptive models can be deployed in real-time transaction monitoring environments to flag suspicious transactions as they occur, with minimal human intervention (Al Amosh & Khatib, 2021).

As financial fraud evolves, generative AI provides the tools to anticipate and prevent these crimes before they escalate. However, the effectiveness of these tools hinges on their proper training, ethical deployment, and continuous validation against real-world threats.

Challenges and Ethical Considerations in Applying Generative AI to Fraud Detection

As the financial industry increasingly adopts generative AI for fraud detection, several challenges and ethical considerations have emerged that must be addressed to ensure responsible and effective use. One of the primary concerns involves data privacy and security. Generative AI models rely on large volumes of sensitive financial data to function effectively. If not properly governed, the use of such data can lead to violations of privacy regulations and pose significant cyber security risks (Al Amosh & Khatib, 2021). Financial institutions must implement strict data protection protocols to ensure compliance with regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Another challenge is the issue of model transparency. Many generative AI systems, especially those based on deep learning architectures, operate as ―black boxes,‖ making it difficult to explain how they reach their conclusions. This lack of explain ability creates a barrier for regulators, auditors, and stakeholders who require clarity and accountability in fraud-related decisions (Abdulwahhab, Al-Dulaimi, & Alkfaajy, 2021). Developing AI systems with interpretable outputs is essential to gain trust and meet regulatory expectations. In addition, generative AI models are vulnerable to adversarial attacks, where malicious users manipulate input data to deceive detection algorithms. This can lead to undetected fraudulent transactions or false negatives in monitoring systems. Robust security frameworks and adversarial training techniques are necessary to protect these models from being exploited (Stanković, 2020). Bias and discrimination also present ethical dilemmas in AI-based fraud detection. If the training data contains historical biases or lacks diversity, the model may produce skewed results that disproportionately impact certain user groups or businesses. This highlights the importance of continuous monitoring, algorithm auditing, and ethical oversight throughout the model lifecycle (Njoku et al., 2025). Legal and regulatory uncertainty further complicates the integration of generative AI in fraud detection. As these technologies evolve faster than legislation, questions arise about accountability and liability in cases of AI-driven decision-making errors. There is an urgent need for updated policies and frameworks that define legal responsibilities, especially in critical areas like fraud prevention (Alshurafat, 2021). Finally, the use of synthetic data generated by AI introduces both benefits and risks. While synthetic data can be useful in training models and protecting real customer information, its misuse could compromise the integrity of financial audits and lead to fabricated reporting. Financial institutions must therefore develop ethical standards and governance mechanisms to guide the responsible use of synthetic data in fraud detection (Bologna, Lindquist, & Warren, 2019; Okafor, Naibe, Diala, & Akhuemonkhan, 2025).

Overall, addressing these ethical and operational challenges is crucial to leveraging the full potential of generative AI in a manner that promotes trust, security, and compliance within the financial ecosystem.

Recommendations for Future Applications and Ethical Considerations

As generative AI becomes more embedded in financial fraud detection systems, it is essential to balance technological advancement with ethical safeguards and policy frameworks. Institutions must prioritize transparency in how generative models are trained, ensuring that datasets are unbiased and representative to prevent skewed risk assessments (Al Amosh & Khatib, 2021). Clear auditing protocols should be established to monitor AI-generated decisions and reduce the likelihood of overfitting or producing misleading outputs, which can compromise financial investigations (Stanković, 2020). To maintain public trust, organizations must adhere to international data protection standards such as the GDPR and CCPA when deploying AI models that analyze personal financial information (Njoku et al., 2025). Establishing interdisciplinary oversight committees involving AI developers, forensic accountants, legal experts, and compliance officers can enhance accountability, flag algorithmic biases, and promote fair usage (Bologna, Lindquist, & Warren, 2019; Okafor, Naibe, Diala, & Akhuemonkhan, 2025). Furthermore, financial institutions and regulators should invest in workforce training programs to equip professionals with skills in AI auditing, model validation, and ethical AI governance (Alshurafat, 2021). Collaboration with academia and open-source communities can also facilitate knowledge-sharing and the development of best practices for secure and responsible implementation of generative AI in fraud detection (Abdulwahhab, Al-Dulaimi, & Alkfaajy, 2021). While the capabilities of generative AI are transformative, ethical foresight and robust governance mechanisms will determine its long-term success in strengthening fraud prevention and maintaining corporate transparency.

References

Abdulwahhab, M. T., Al-Dulaimi, A. A. K., & Alkfaajy, E. J. A. (2021). Using governance mechanisms to raise the efficiency of internal control performance to confront government corruption in Iraq: An empirical study. Webology, 18(2).

Aburumman, O. J., Omar, K., Al Shbail, M., & Aldoghan, M. (2022). How to deal with the results of PLS-SEM? In Explore Business, Technology Opportunities and Challenges after the COVID-19 Pandemic (1196–1206). Springer.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023). Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation. Cogent Economics and Finance, 11(1), 2153412.

Al Amosh, H., & Khatib, S. F. (2021). Ownership structure and environmental, social and governance performance disclosure: The moderating role of board independence. Journal of Business and Socio-Economic Development, 2(1), 49–66.

Al Amosh, H., & Khatib, S. F. (2021). Ownership structure and environmental, social and governance performance disclosure: The moderating role of board independence. Journal of Business and Socio-Economic Development, 2(1), 49–66.

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2018). Fraud Examination. Cengage Learning.

Alshurafat, H. (2021). Forensic accounting as a profession in Australia? A sociological perspective. Meditari Accountancy Research, 30(2), 395–423.

Bologna, G., Lindquist, R. J., & Warren Jr, D. E. (2019). Forensic Accounting and Fraud Examination. John Wiley & Sons.

Ćirović, M., & Marinković, V. (2021). The role of forensic accounting in uncovering financial fraud. Journal of Financial Crime, 28(3), 747-763.

Golden, T. W. (2019). Forensic Accounting and Fraud Examination. Cengage Learning.

Njoku, C., Okafor, G., Akhuemonkhan, E. E., Naibe, I., & Diala, A. K. (2025). Leveraging data analytics for fraud detection: The future of financial risk mitigation and regulatory compliance. Computer Science & IT Research Journal, 6(2), 86–93.

Njoku, C., Onwe, I., Onyeibor, C. I., Ekanem, C. E., & Diala, O. R. (2025). Integrating artificial intelligence and data analytics in imaging for early cancer detection: Optimizing workforce efficiency and healthcare resource allocation.

International Journal of Scientific Research Updates, 9(1), 17–21.

Okafor, G., Naibe, I., Diala, A. K., & Akhuemonkhan, E. E. (2025). The role of forensic auditing in strengthening corporate transparency and fraud prevention in financial institutions. Finance & Accounting Research Journal, 7(2), 126–132.

Okafor, G., Naibe, I., Diala, A. K., & Akhuemonkhan, E. E. (2025). Evaluating the effectiveness of risk-based auditing and SOX compliance in preventing financial fraud: A case study of multinational corporations. Finance & Accounting Research Journal, 7(2), 118–125.

Pickett, K. H., & Pickett, M. (2019). Forensic Accounting and Fraud Examination: Principles and Practice. Routledge.

Singleton, T. W., Singleton, A. J., Bologna, G. J., & Lindquist, R. J. (2014). Fraud Auditing and Forensic Accounting: New Tools and Techniques. John Wiley & Sons.

Stanković, M. (2020). The impact of blockchain technology on forensic accounting and auditing. Economic Themes, 58(1), 37–54.

Wells, J. T. (2019). Principles of Fraud Examination. John Wiley & Sons.